INL/EXT-15-37287

Concept for Cyber-Physical Consequence Process

January 2015

Idaho National Laboratory

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-15-37287

Concept for Cyber-Physical Consequence Process

January 2015

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Concept for Cyber-Physical Consequence Process

January 2015

Approved by:

1/27/15	
Craig Rieger	**Date**
Principal Investigator, Idaho National Laboratory	
2/3/2015	
Ronald Fisher	**Date**
Program Director, Idaho National Laboratory	
2/25/2015	
Robert Schmidt	**Date**
IT Cyber (INFOSEC), Office of Cyber and Infrastructure Analysis (OCIA)	
2/25/2015	
Richard Moore	**Date**
Office of Cyber and Infrastructure Analysis (OCIA) Cyber-Physical Analysis Chief	

EXECUTIVE SUMMARY

The Department of Homeland Security's Office of Cyber and Infrastructure Analysis (DHS/OCIA)[1] has a mission and vision that promotes innovation as central to expanding the organization's capability to conduct consequence analysis. To pursue such innovation, OCIA is sponsoring a seedling effort with Idaho National Laboratory (INL) to leverage data from the proposed Automated Vulnerability Assessment (AVA) capability, which the DHS Science and Technology (S&T) Directorate is developing through a separate INL effort.

The first phase of this effort is to develop a process by which recognized vulnerabilities can be scored relative to importance, reflected primarily in the ability to initiate high consequence and potentially cascading events. This report documents a cyber-physical metrics process (CPMP) to tie physical impact to the malicious exploitation of cyber vulnerabilities in industrial control systems (ICS) with the potential for initiating consequence in the critical infrastructure. The scale of achieving any particular physical consequence is dependent upon the ICS **C**omponent the vulnerability exists on, the **L**evel of **A**ccess that the exploit would allow to component function and the **P**hysical **I**mpact (CLAPI) to the power system that the component is tied. A modified common vulnerability scoring system (CVSS) was detailed and demonstrated for the power sector with three case studies associated with a recognized vulnerability, with significant consequence detail provided to apply the process across the power sector. A detailed table that provides background on the power system components, ICS-enabled monitoring and control, potential consequence effects, and CVSS scoring is provided. To demonstrate the applicability of the CPMP, tables are provided as examples for other sectors that include chemical, water/wastewater and oil/gas.

While the recognized vulnerabilities for the case studies all have a CVSS high severity base metric, the results affirmed that this condition does necessarily equate to a high severity environmental impact. Concluded from this effort are the following:

- As with any metrics system, an understanding of the significance of the attributes considered is important. In the case of the CPMP and the use of the CVSS, what appears to be a vulnerability of grave concern based on its base score, may not lead to a severe impact even if exploited. For example, the Target Distribution attribute of the environmental metric represents the vulnerability's prevalence, and has a great effect on the metric calculation and, consequently, on the final severity rating. Within the context of the case studies in this report, the identified vulnerabilities are not expected to lead to high consequence impacts and potential cascading failures, and thus their final ratings of medium and low severity seem reasonable.
- Detailed prevalence understanding on the level of use for a particular ICS component requires vendor sales/service information, which is known at a higher level from sources such as Newton-Evans. Additional analysis from subject matter experts and regional installation specifics will provide the proper context of the vulnerability's impact. To provide greater granularity in the determination of the environmental metric, a detailed evaluation of prevalence is proposed in the second phase of this effort.
- The CVSS system is useable for ICS, but requires some modification to specifically reflect the application to critical infrastructure. Consideration of other variables that relate to the current environment of ever increasing threat, such as the ability of an adversary to chain vulnerabilities, is important for making an improved assessment of a vulnerability's severity. Chained vulnerabilities

[1] In February 2014, the DHS National Protection and Programs Directorate (NPPD) created the Office of Cyber and Infrastructure Analysis by integrating analytic resources from across NPPD, including the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the National Infrastructure Simulation and Analysis Center (NISAC).

are expected to be partially addressed in CVSS 3.0, which is expected to be released soon. Phase 2 of this effort will look to take advantage of CVSS 3.0 enhancements and other related metrics work to provide insight into new useful variables to incorporate into the Environmental metric for ICS.

- To illustrate the benefit of the approach, examples of similar consequence detail is provided for the chemical, water and wastewater and oil/gas sectors. It is clear from these tables, provided in Appendix E, that the CPMP process can be applied cross-sector based upon the development of similar consequence-related information and scoring.

A scope of work that is based upon prior discussions with OCIA and the conclusions of this first phase have been provided. This effort will provide a more granular evaluation of metrics correlating cyber vulnerability to consequence. This look will include ICS market data collection, chaining of vulnerabilities, and potential modification of the scoring system (including CVSS 3.0, if released). This effort will also take a first look at correlating potential threat actors and avenues for exploitation, including physical failure, which would result in the consequence scenario initiation. Finally, as the AVA project progresses in parallel, this effort will align with one asset owner and vendor to vet the overall CPMP.

CONTENTS

FIGURES

TABLES

ACRONYMS

ACORN	Automated Construction Of Realistic Networks
AVA	Automated Vulnerability Assessment
CDP	collateral damage potential
CLAPI	**C**omponent of interest, **L**evel of **A**ccess, **P**hysical **I**mpact
CPMP	cyber-physical metrics process
CVSS	Common Vulnerability Scoring System
DCS	distributed control system
DHS	Department of Homeland Security
DMS	distribution management systems
EMS	energy management system
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HMI	human-machine interface
ICS	industrial control system
ICS-CERT	Industrial Control Systems-Cyber Emergency Response Team
IT	Information Technology
INL	Idaho National Laboratory
MSC	INL Mission Support Center
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OCIA	Office of Cyber and Infrastructure Analysis
PLC	programmable logic controllers
POC	proof of concept
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SME	subject matter expert
S&T	Science and Technology Directorate (DHS)
TD	target distribution

INTRODUCTION

Purpose

The Department of Homeland Security's Office of Cyber and Infrastructure Analysis (DHS/OCIA) has a mission and vision that promotes innovation as central to expanding the organization's capability to conduct consequence analysis. To pursue such innovation, OCIA is sponsoring a seedling effort with Idaho National Laboratory (INL) to leverage data from the proposed Automated Vulnerability Assessment (AVA) capability, which the DHS Science and Technology (S&T) Directorate is developing through a separate INL effort.

In 2013, OCIA developed and tested a proof-of-concept methodology for conducting cyber-physical site assessments. The assessments involved collecting and evaluating vulnerability information manually (i.e., through phone and in-person discussions focused on each site's network diagrams, firewall rules, and other considerations) to inform follow-on consequence modeling efforts. OCIA had extensive planning, scheduling, and in-person engagement to develop each site assessment individually. Although OCIA demonstrated the effectiveness of that approach, the approach does not scale quickly or broadly, and OCIA is exploring new methods to increase scalability and efficacy. If S&T and OCIA's efforts related to the AVA project succeed, these will help OCIA extend beyond a one-site-at-a-time approach to cyber-physical analysis. In addition, the project positions OCIA to leverage other DHS capabilities through coordination and collaboration with other DHS elements.

The AVA project is intended to provide scalable processes to assess the classes of cybersecurity vulnerabilities for any asset owner site. The scalable methodology, by design, minimizes hands-on labor associated with manual vulnerability assessment processes. Understanding vulnerabilities only provides one piece of the risk equation, though. Assessing vulnerabilities and related consequences provides a fuller picture of the risk equation. By engaging with S&T and INL at the ground stage of this process, OCIA has an opportunity to ensure requirements that would promote adaptation of follow-on consequence analysis into the AVA construct. Although consequence analysis cannot be automated similarly, the AVA can provide broad sets of readily available vulnerability data that OCIA can leverage to more quickly identify potential consequences.

OCIA's effort has two phases, each with distinct outcomes for what DHS S&T plans to receive. The next section provides an overview of the first phase of this effort.

Objectives

While this effort is planning for the eventuality of having vulnerability data from the AVA construct, as described in Appendix A, the process itself is standalone and applicable to other sources of vulnerability data. The resulting objectives are structured to ensure the successful development of a cyber-physical metrics process (CPMP) for associating consequence to vulnerability, provide an actionable metric on cyber-physical impact, and provide a process that can be applied consistently. To focus this particular effort, as each sector has its own set of consequences, the OCIA chose the power sector as the primary infrastructure under initial study. This will allow leveraging the asset owner (and vendor) engagements that AVA is developing in support of that effort. The resulting outcomes for this phase therefore address the development of a CPMP process for the power sector. Two primary attributes of the CPMP have been developed, which are identified in the list below.

- A documented process for conducting consequence analysis using vulnerabilities from AVA, or other sources. This process will leverage the AVA requirements for information on the power sector, type of industrial control systems (ICS) component, and physical function to provide:

  - Criteria for determining which AVA vulnerabilities have most potential to lead to consequences
  - Relevant cyber scenarios based upon an exploited vulnerability
  - Relevant physical factors that influence exploiting consequence scenarios.
- A table that identifies the high-impact consequence scenarios for the power sector.

OCIA developed a scoring process based upon the Common Vulnerability Scoring System (CVSS), provided in detail in Appendix B, which addresses the points above in that it provides a weighting to address impact, different vectors to attack (demonstrated through case study selection) and physical factors that influence consequence. The process includes modifications that provide relevance to the CVSS application to ICS. Secondly, a table of high-impact consequence power sector scenarios, and a range of actual possibilities, is provided in its entirety in Appendix C of this report. This process is designed for direct application to any vulnerability identified by AVA, or other source, but can be further refined for more exact application depending on sources of data that will be discussed in other sections.

Team

A multidisciplinary team was formed to support this effort and capture the cyber-physical aspects as well as the sector-specific focus. The point of recognizing these aspects of the project is to understand that all cyber-physical challenges are complex. As a result, a suitable team is required to optimize the potential for a holistic solution. The list below divides the individual contributions to this effort:

- Cyber Vulnerabilities and Attacks
  - Taxonomies
  - Attack scenarios
  - Methodology
- Cyber Security Measures and Models
- Physical (Critical Infrastructure) and ICS lead
- Power Generation, Transmission and Distribution
  - Generic plant and control system
  - Physical safety mechanisms
  - Analysis of potential consequences.

CPMP Background

Generic ICS Architectures

Supervisory control and data acquisition (SCADA) and distributed control system (DCS) are the two overarching types of control system architectures commonly referenced. Understanding vendor implementations can vary, so Figure 1 and Figure 2 provide notional references for DCS and SCADA architectures taken from the National Institute of Standards and Technology (NIST)[2]. DCS and SCADA architectures possess the same functionality, in general, when it comes to data acquisition, display, and control action. Programmable logic controllers (PLC) can be included in either architecture, as an originating set of technologies introduced and adopted with transition from digital to analog control. However, remote terminal units (RTU) have become the normal interface to field devices within the

[2] NIST Guide 800-82, "Guide to Industrial Control Systems Security."

SCADA architecture. RTUs provide the same capability for monitoring and control but not necessarily the same ability to program logic as with a PLC.

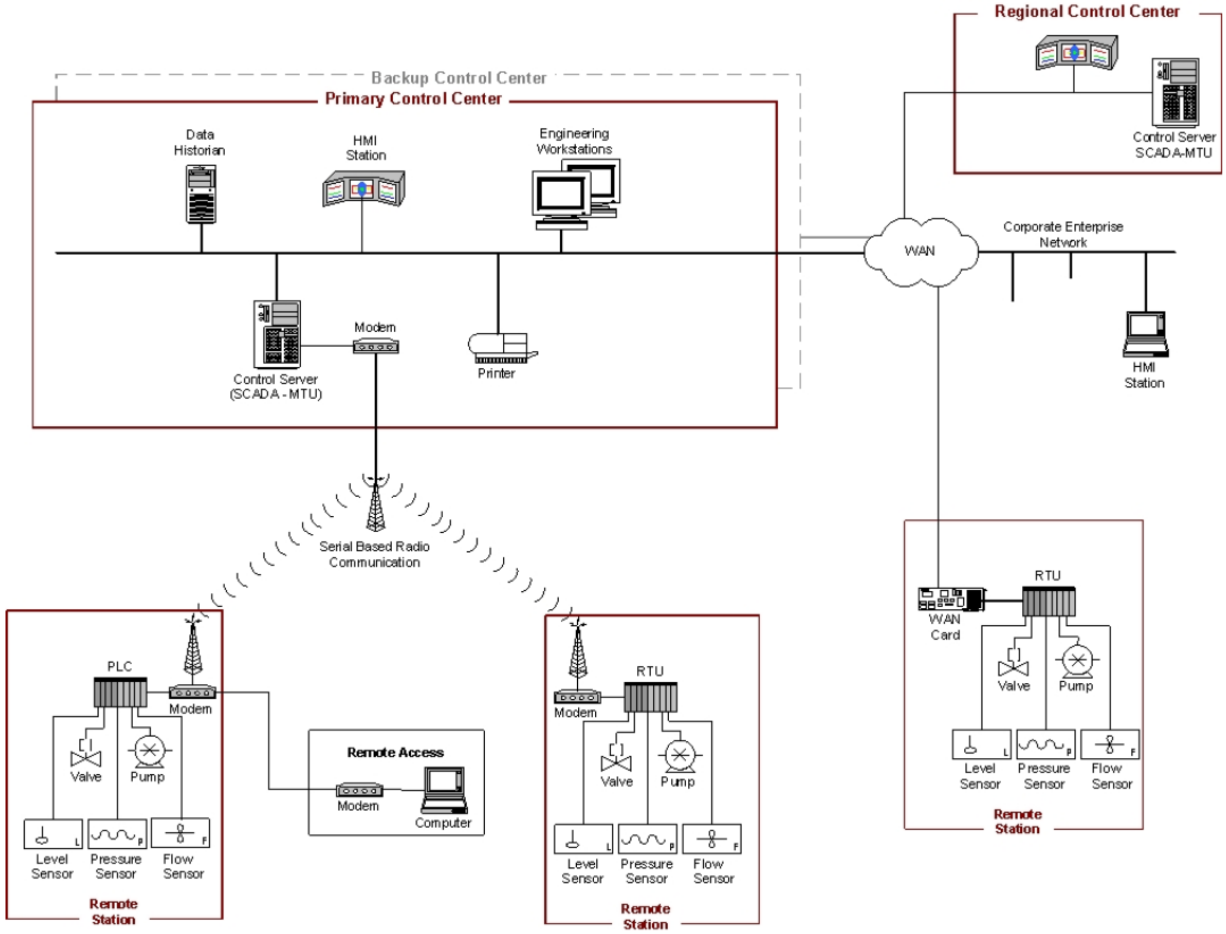


Figure 1. Generic SCADA Architecture from NIST 800-82

However, within vendor implementations and the system evolution, these architectures have the following common and differing attributes:

- Similarities:
  - Utilizes similar sensor signal types, with some variation in digital fieldbus standards practices
  - Common migration from proprietary to industry standard operating systems and protocols
  - Possess some common architectural nodes such as a human-machine interface (HMI) for operator or dispatcher interaction, an engineering workstation for configuring the ICS, a historian for long term data collection, etc.
- Differences
  - SCADA
  - “Intelligence” exists within the relays and decision support applications
  - Focused on event-based controls

– Focused on Wide Area controls

– DCS

– "Intelligence" exists in the controllers

– Focused on variable process feedback controls

– Focused on fixed infrastructure (i.e., generation plant).

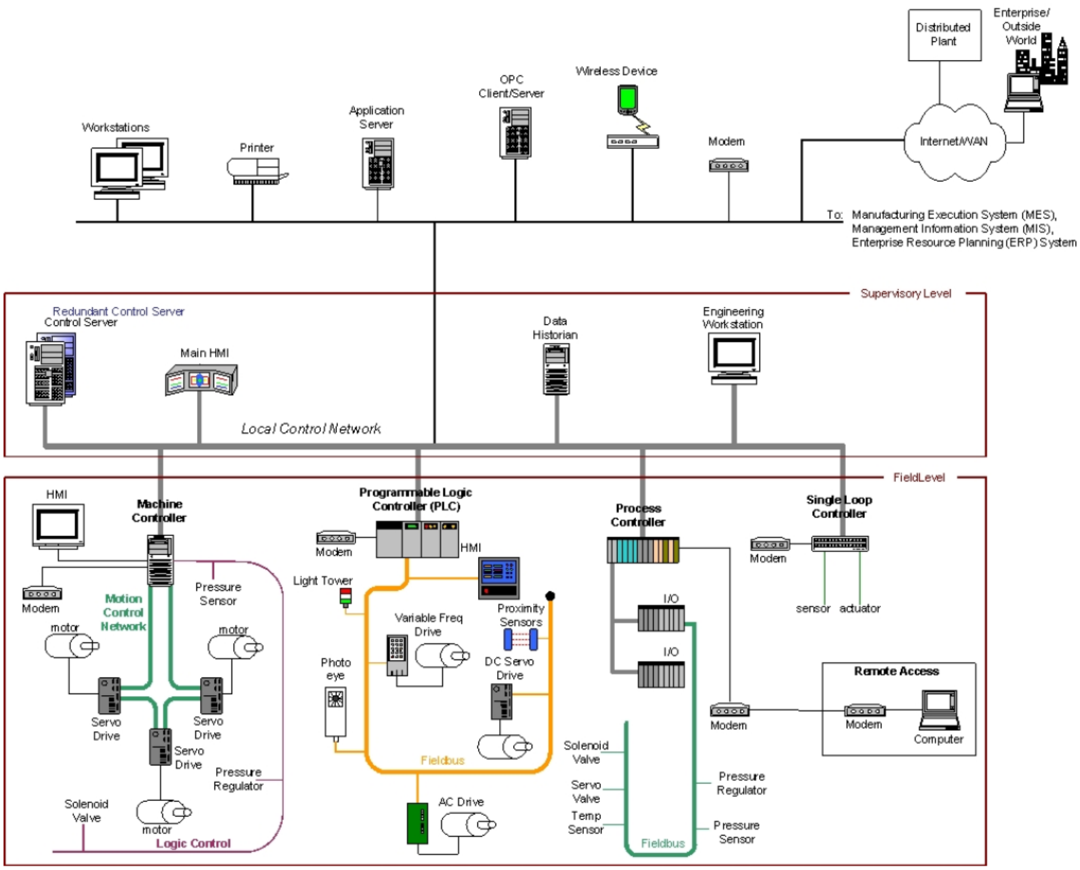


Figure 2. Generic DCS Architecture from NIST 800-82

Referring to Figure 1 and Figure 2, several of the components on the control system network are essentially standard Information Technology (IT) appliances, such as the firewall and intrusion detection system. However, specific components described by red text are the focus of specific interactions with the vendors. In some cases, subcomponents will also be necessary to adequately describe the design. SCADA applications servers can host specialty decision support and supervisory control applications, call energy management system (EMS) and distribution management systems (DMS) when applied in particular to the energy sector.

CVSS Scoring Basis

When a vulnerability is discovered and reported, it is important to assess the potential impact of the vulnerability. The Common Vulnerability Scoring System (CVSS)[3] was developed to provide a relatively uniform method for making this assessment for each vulnerability within IT systems. The CVSS consists

[3] Peter Mell, Karen Scarfone, and Sasha Romansky, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," hxxp://www.first.org/cvss/cvss-guide.pdf, June 2007, date last accessed February 18, 2010.

of three major groupings of attributes, or metric groups: Base, Temporal, and Environmental; each consisting of a set of metrics, as shown in Figure 3. Further background on CVSS is provided in Appendix B.

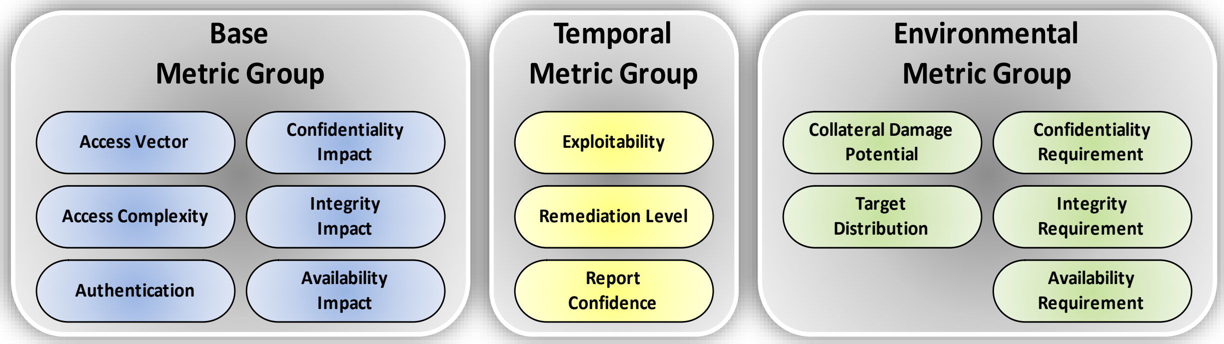


Figure 3. CVSS metric groups

The base group and score reflect attributes of the vulnerability itself, independent of any context. The temporal group and score attempts to take into account those external attributes related to the ease of exploiting a vulnerability that change over time. This includes factors such as the availability of exploit code and whether official patches are available. The temporal factor reflects, to some degree, the changing nature of the external vulnerability eco-system. The environmental group and score are intended to provide a context to the vulnerability that will vary by each system and facility in which it exists. The environment includes attributes such as the potential for loss of life if the vulnerability is “successfully” exploited and the percent of devices within a facility that could be impacted by the vulnerability.

In IT, CVSS has gained acceptance over time due to its standardization of scoring and its modular nature. The base score can, and is, calculated without need for the temporal or environmental factors. Individual facilities may then choose to add temporal factors and environmental factors based on their own assessments and knowledge of their particular systems (i.e., based on the context of the vulnerability in their particular facility).

The potential issues for applying CVSS to assess vulnerabilities in many critical infrastructures is that CVSS was not designed with ICS in mind, nor was its focus on assessing the importance of a vulnerability based on a national security perspective. However, because of the general acceptance of the value that CVSS provides and an initial assessment that CVSS could be enhanced to assess a vulnerability’s importance from a national security perspective, CVSS was chosen CVSS as the foundation for the CPMP in assessing an ICS vulnerability’s potential impact to the nation’s critical infrastructure.

In using CVSS as the foundation in assessment of an ICS vulnerability, the source of the vulnerability information would normally be the source of the vulnerability’s base score. That is, AVA is intended in its initial development to recognize existing vulnerabilities, such as those documented with a base score calculated by the Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT). The CPMP will allow, as the situation dictates, the temporal score of a vulnerability based on threat-related input from the ICS-CERT program. Ideally, the environmental score, from a national perspective, would be calculated and provided by ICS-CERT as well, but this is currently unlikely due to the lack of installed base and installation specifics providing more contexts. Consequently, the focus of this effort is on enhancing the CVSS environmental attribute group to better reflect the potential for high-impact events.

Power Sector Consequence and Environmental Metric Basis

Each critical infrastructure sector has its own unique dependencies and complexities, as well as subsystems. For the power sector, the top-level subsystems are generation, transmission, and distribution. Within each are additional subsystem breakdowns and components. How these interrelate and describe the dependencies and complexities of the power sector are provided in Appendix C. Figure 4 below diagrams the use of this information, starting with the determination of the individual subsystem and/or component of interest.

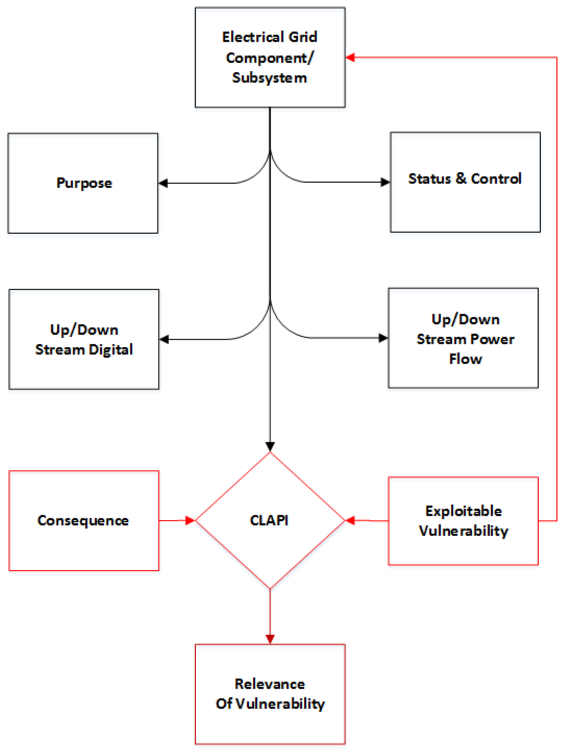


Figure 4. CPMP Flow

For each subsystem or component, the purpose of each subsystem or component is defined, along with other cyber and physical characteristics. These include what the subsystem or component monitors and controls in the physical environment, how the control system on the subsystem level might be affected by adjacent ICS, and physical subsystems. To indicate a consequence, a scale of high-impact events are mentioned, and in the case of this effort, reflect power grid outages and equipment damage. The table in Appendix C then provides a scoring relative to the assumptions provided for an individual vulnerability exposure.

This effort considers models of ICS used in a chosen critical infrastructure, as provided in Figure 1 and Figure 2. The different generic devices used within the control system are then identified within the architecture, i.e., SCADA and DCS, and their ability to cause potential physical damage is assessed. The scale of achieving any particular consequence is dependent upon the ICS **C**omponent the vulnerability exists on, the **L**evel of **A**ccess that the exploit would allow to component function, and the **P**hysical **I**mpact (CLAPI) to the power system that the component is tied. For the Environment Factor, if the potential for damage through compromise of a device is great, then the enhanced environmental score for a vulnerability on that device will increase.

IMPACT EVALUATION AND SCENARIOS

To illustrate the spectrum of potential impacts and the resulting scoring, scenarios are presented below as the basis for case studies. The case study will be based upon pre-existing vulnerabilities affecting power sector ICS available from ICS-CERT, in some cases modified for improved illustration. The focus on the single vulnerability impact to the complex systems on systems architectures in power grid and other critical control systems is narrow. Most malware contains exploits using multiple vulnerabilities. These vulnerabilities were selected based upon the impact that may be generated through compromise of different ICS devices, and are provided in full in Appendix D. The result of each scenario is the assignment of the environmental factors included with the CVSS scoring.

Scenario 1

A Siemens webserver vulnerability has been recognized by a vulnerability assessment and could be exploited within a coal-fired generation station ICS, as described in Appendix D. Following the process of Figure 4 and referring to the table in Appendix C for a "Generation Station" under the "Generation" category, the purpose and status/control are provided below in Figure 5. These two columns provide an overview of the overall system and subsystems within a generation station. Under status and control, it is noted that architecture is primarily DCS. Further information on DCSs is provided in the "Applications on Control Centers and Specialized Equipment" category in Appendix C.

Electric Grid Component / Subsystem	Purpose	Status & Control
Generation Station – Balance of Plant  	Converts fuels or nuclear reaction to electric power. Generation stations are similar to any complex manufacturing plant with many subsystems to support the conversion of raw materials into a finished product.	Power plants contain many industrial control and instrumentation systems. Primary plant controls • Fuel supply system • Fire/burner control • Feed water pumps • Steam valve motors • Chill water pumps • Oiling system • Water chemistry system • Temperature and pressure monitoring system

Figure 5. Generation Purpose and Status/Control

This webserver vulnerability is to an HMI, referring to Figure 2, and allows full access to HMI functions. With full access, the operation of the generator can be modified in any way the attacker chooses. Referring to Figure 6, several potential impacts may occur within the generation facility and to the neighboring grid with which it is tied. For instance, the balance of plant systems that include the boiler and turbine loop can be shut down or inappropriate settings placed as if a facility operator had done so. Externally, variations within the facility can impact the ability of the transmission EMS to predict operation of this generator and prevent the EMS from accurately predicting the expected power flow from the facility.

Digital Flows	Load/Utility Power Flow
Energy Management Systems with digital and analog input/output, Human Machine Interfaces (HMI), status and control • Generation Dispatch Control • Voltage Regulation Control • Automatic Generation Control (AGC) Plant Operation Systems • Programmable Logic Controllers (PLC), Intelligent End Devices (IED), Remote Terminal Units (RTU) • HMI • Motor VSD, starters • Monitoring systems • Cooling • Balance of Plant Systems • Emergency Generation for shutdown or startup • Generation Substations • Step Up for Transmission	Utility Upstream – Energy Management Systems • Generation Dispatch Control • Voltage Regulation Control • Fuel Consumption / Fuel Costs Downstream – Plant Operation Systems • PLC • Motor VSD, starters • Monitoring systems

Figure 6. Generation Digital and Power Flows

The consequence column in Figure 7 for the generator indicates several impactful potential effects that an exploited HMI may lead to. Any cycling can cause instability within the facility and externally, causing a transmission dispatcher to take this generator offline. If not caught quickly enough, it could lead to cascading effects. If associated damage is created within any of the transmission systems due to malicious operation, loss of this generator from the grid can also be the result. If facility equipment damage is associated with a long-lead item such as a turbine, it could lead to an extended loss of the generator.

Referring to Appendix B, which provides a modification to the CVSS to better reflect ICS, the environmental factors are developed and provided in Figure 8. While the collateral damage potential (CDP) is high for this type of HMI vulnerability, the target distribution (TD) is considered low. This metrics assignment reflects the fact that numerous vendors supply HMI systems. With data on the implementation of the affected HMI, this assignment may change. Confidentiality in the operations of the generator is not a large concern, but both the integrity and availability are rated at a medium as these have greater importance. Grid operations can withstand one generator being lost from service. However, any impact to accurate data will be reflected in abnormal operation from the facility operator and potentially equipment damage from improper operator actions. One further point should be made regarding the consequence factors. If the vulnerability within the HMI had not full access, the base metric would have also changed.

Consequence
Monetary - Operating outside of EPA and other regulatory requirements Physical Damage - Physical damage to parts and equipment in balance of plant; Damage to core reactor highly unlikely; Collateral damage to balance of plant systems likely, limited target distribution due to isolation of systems and boundary protections Loss of Confidence - is low since time sensitive information Loss of Integrity – Balance of plant subsystems likely Loss of Availability - Nuisance failures and shut downs of subsystems Reputation - Radiological release highly unlikely; if unstable generation

Figure 7. Generation Consequence

Environmental Factors						
CDP	Collateral Damage Potential					
	N	L	LM	MH	H	ND
TD	Target Distribution					
	Component: Generator					
	Subsystem: Generation Station					
	% in Subsystem 20% nuclear- 60% Fossil/hydro					
	N	L	M	H	ND	
CR	System Confidentiality Requirement					
	L	M	H	ND		
IR	System Integrity Requirement					
	L	M	H	ND		
AR	System Availability Requirement					
	L	M	H	ND		

Figure 8. Scenario Environmental Factors for CVSS

Scenario 2

A Rockwell PLC vulnerability has been recognized by a vulnerability assessment and could be exploited within both a gas-fired generator and adjacent transmission system substation. The vulnerability, as described in Appendix D-1, will lead to multiple impacts. Referring to the table in Appendix C for a "Transmission Network" under the "Transmission Substation" category, it is noted in Figure 9 the purpose and status/control and the primary ICS architecture as SCADA. Further information on PLCs is also provided in this category. Information for a generator is shown in Figure 5, noting that DCS architecture is prevalent in generation facilities. In addition, as noted before, DCS and SCADA architectures both may have PLCs integrated, as in this scenario. Further information on PLCs is provided in the "Applications on Control Centers and Specialized Equipment" category in Appendix C.

The PLC vulnerability provides potential to cause a controller fault, denial of service, a man-in-the-middle attack or replay attack. Loss of access to the PLC, as the first two effects indicate, effectively prevents the operator/dispatcher from monitoring the substation. Figure 10 indicates that this loss of access to control the substation would prevent a dispatcher from making any needed set point changes to substation devices, such as relays and breakers. While this is an operational issue, especially in parallel with any transient power flow disturbances that may be occurring, it does not directly lead to a grid failure. The substation devices will remain in the last state operated so long as the conditions are steady-state. Referring to Figure 11, it would be unlikely, over a short duration in time, to achieve the maximum consequence.

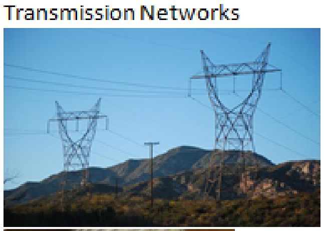
Electric Grid Component / Subsystem	**Purpose**	**Status & Control**
Transmission Networks  	The transmission network consists of a number of transmission line circuits that connect generation stations to distribution substations. The mesh network serves as a bulk power delivery system to cities, rural areas, and industrial complexes. The primary components of the transmission network are the transmission lines and substations. Transmission lines are passive devices with practically no control points. Historically, any instrumentation of the transmission lines was associated at the substations. Common transmission network voltages: 138kV, 230kV, 345kV, 500kV and 765kV	The transmission lines are passive devices for transporting power. Instrumentation: • Conductor sagging monitors • Conductor temperature monitors • Weather condition monitoring • Current / Power flows Line fault protection system: • Short-circuit fault protection • Out-of-step / power swing detection and blocking / tripping

Figure 9. Transmission Purpose and Status/Control

A similar level of impact would be expected in the generation facility. However, in this case there are normally more control actions necessary to ensure the facility operates properly. In addition, if the PLC happens to be the ICS device controlling the turbine or other critical controls, a loss of operation could occur immediately depending upon the failure mode during a controller fault. Therefore, the physical impact resulting from the loss of state awareness in generation is considered more critical to the operation. However, not unlike with transmission, the consequence listed in Figure 7 is unlikely to be reached.

Referring to Figure 12, the CDP for the transmission effect is low-medium, reflecting the limited impact expected in direct cost and/or physical impact to the transmission system. In light of the impact to the control actions within a generation, however, the affect is much greater reflecting a high score. As the PLCs are common, the TD is considered medium. As with the prior scenario, the integrity and availability are important attributes to ICS operation, as contrasted to confidentiality, and are therefore ranked as a medium.

For a worst-case scenario, as indicated in Appendix C, note that the CDP could be high if greater access to control the operation were provided by exploit of the vulnerability. Confidentiality could be elevated to a medium, if customer data were available within the distribution system ICS. Integrity and availability could also be elevated, as less redundancy exists if a compromise were to disable power to certain critical loads.

Digital Flows	**Load/Utility Power Flow**
Electro-Mechanical: Instrumentation transformers (CTs & PTs) and thermal / mechanical transducers; Control signals to switches most non-digital Digital: • IED, PLC, RTU monitoring devices and systems with HMI • SCADA data input channels • Protective relaying inputs	Transmission from large generation Transmission to distribution centers Transmission to central power grid Transmission to major load industrial centers

Figure 10. Transmission Digital and Power Flows

Consequence
Monetary: if physical damage or loss of efficiency (i. e. wrong line rating)
Physical Damage: Failure of the conductors; Damaged insulators Reduction of operational life; Sagging conductors beyond elasticity point
Loss of Confidentiality: Market estimate of transmission capacity
Loss of Integrity: If spoofed line ratings
Loss of Availability: Power Outage - localized or if coordinated and networked wide spread; Transfer of power flow to other transmission circuits; Increasing the susceptibility to cascading power outage
Reputation: inefficient transmission

Figure 11. Transmission Consequence

Environmental Factors						
CDP	Collateral Damage Potential					
	N	L	**LM**	MH	H	ND
TD	Target Distribution					
	Component: Transmission Lines					
	Subsystem: Transmission					
	% in Subsystem: 100%					
	N	L	**M**	H	ND	
CR	System Confidentiality Requirement					
	L	M	H	ND		
IR	System Integrity Requirement					
	L	**M**	H	ND		
AR	System Availability Requirement					
	L	**M**	H	ND		

Environmental Factors						
CDP	Collateral Damage Potential					
	N	L	LM	MH	**H**	ND
TD	Target Distribution					
	Component: Generator					
	Subsystem: Generation Station					
	% in Subsystem 20% nuclear-60% Fossil/hydro					
	N	**L**	M	H	ND	
CR	System Confidentiality Requirement					
	L	M	H	ND		
IR	System Integrity Requirement					
	L	**M**	H	ND		
AR	System Availability Requirement					
	L	**M**	H	ND		

Figure 12. Transmission & Generation Environmental Metrics

Scenario 3

A Telegyr RTU vulnerability has been recognized by a vulnerability assessment and could be exploited within distribution system substation. The vulnerability, as described in Appendix D-1, will lead to multiple impacts. Referring to the table in Appendix C for a “Distribution Network” under the “Distribution Substation” category, it is noted in Figure 9 the purpose and status/control and the primary ICS architecture as SCADA. Further information on RTUs is provided in the “Applications on Control Centers and Specialized Equipment” category in Appendix C.

The RTU vulnerability provides potential to cause a denial of service. Loss of access to the RTU effectively prevents the operator/dispatcher from monitoring the substation. Figure 10 indicates that this loss of access to control the substation would prevent a dispatcher from making any needed set point changes to substation devices, such as breakers. While this is an operational issue, especially in parallel with any transient power flow disturbances that may be occurring, the effects are primarily to the downstream loads for the substation. The substation devices will remain in the last state operated, which is normal for radial distribution networks. In addition, unlike transmission, the impact would be minimized to an area of a city and not a region. Referring to Figure 15, it would be unlikely over a short duration in time to achieve the maximum consequence.

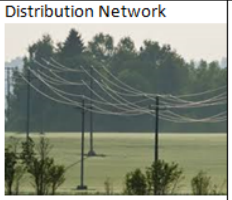
Electric Grid Component / Subsystem	Purpose	Status & Control
Distribution Network 	The distribution network consists of a number of feeder circuits that connect the bulk transmission system to end-users/customers. The radial network serves as a distribution power delivery system to homes, business, and small industry. The primary components of the distribution network are the feeder lines coming out of the distribution substations and the step-down pole-top and pad-mount transformers. Most distribution lines are passive devices with some control points such as reclosers, sectionalizers, switched capacitor banks, and voltage regulators. Distribution is the focus from most newer applications such as demand response, microgrids, fault isolation, reclosing, islanding, distributed generation, outage management, customer information, pricing signals, net metering – which is changing distribution to be less passive and more digital control with data from the end load user. Common distribution network voltages: 4.8kV, 12.47kV, 13.8kV, 24.5kV and 34.5kV Many applications from municipality to rural	The distribution lines are mainly passive devices for delivering power locally. Emerging applications for reclosing and fault isolation and outage management systems provide more connectivity. Instrumentation: • Voltage magnitude monitors • Power flow monitors and meters Line fault protection system: • Short-circuit fault protection Status: of distribution network, outage management systems, dispatch control centers, load balance applications, potential for connectivity into energy markets, demand response applications, time of use and islanding. Control: connect and disconnect of load areas, isolation of faults, load shedding

Figure 13. Distribution Purpose and Status/Control

Referring to Figure 16, the CDP is low-medium, reflecting the limited impact expected in direct cost and/or physical impact to the distribution system. As the RTUs are common, the TD is considered medium. As with the prior scenario, the integrity and availability are important attributes to ICS operation, as contrasted to confidentiality, and are therefore ranked as a medium.

For a worst-case scenario, as indicated in Appendix C, note that the CDP could be high if greater access to operation control were provided by exploit of the vulnerability. Confidentiality could be elevated to a medium, if customer data were available within the distribution system ICS. Integrity and availability could also be elevated, as less redundancy exists if a compromise were to disable power to certain critical loads.

Up/Down Stream Digital	**Load/Utility Power Flow**
Up: DCS, substation controls, SCADA systems that function as Dispatch center, outage management systems, meter data management system, customer information system, energy market Down: many communications paths to 'last mile' to residence or load center for connect, disconnect, islanding, time of use, market signal transactive data, distributed generation, net metering.	Load side: major load center, industrial complexes, residential areas Utility side: Dispatch centers, DCS, SCADA, Substation controls; generation and transmission

Figure 14. Distribution Digital and Power Flows

Consequence
Monetary: Outage costs; dispatch linemen crew to troubleshoot failed isolation, safety issue potential; outage can range from residential area to large load center Physical Damage: safety and impact to load center and residences Loss of Confidentiality: state based data limited value unless large distribution network or critical load center; if connected to customer information systems (i.e. meter data management systems) potential for customer privacy concerns Loss of Integrity: if reclose signal spoofed indication of breaker setting resulting in localized outage or safety issue Loss of Availability: Indication spoofing less likely due to other sensing and protection mechanisms Reputation: outage recover times or safety incident

Figure 15. Distribution Consequence

Environmental Factors	
CDP	Collateral Damage Potential
	N | L | LM | MH | H | ND
TD	Target Distribution
	Component: Transmission Lines
	Subsystem: Transmission
	% in Subsystem: 100%
	N | L | M | H | ND
CR	System Confidentiality Requirement
	L | M | H | ND
IR	System Integrity Requirement
	L | M | H | ND
AR	System Availability Requirement
	L | M | H | ND

Figure 16. Distribution Environmental Metrics

Other Infrastructures

Similar tables to Appendix D have been provided in an abbreviated form for other infrastructures in Appendix E. While the flow diagram and components may be different, the ICS architectures are the same and a similar breakdown of supporting information and consequence is provided for each.

SCORING

Introduction

The AVA program will emulate select control systems, software, and devices found within portions of the critical infrastructure. Various forms of automated software vulnerability assessments will then be executed as part of the AVA process to identify one or more unidentified system vulnerabilities within the emulated system, devices, and software. As vulnerabilities within the emulated system are identified, an AVA team will quickly begin assessing the potential importance of the vulnerabilities to the critical infrastructure sector of most interest, assign initial importance scores both to individual vulnerabilities and sets of vulnerabilities, and then report the vulnerabilities and their assessed importance score through appropriate channels.

For this project, a scoring process was selected and developed on singular software vulnerabilities, with the intent that the process be a foundation that could eventually be built upon to accommodate evaluation and scoring of sets of intertwined software vulnerabilities, individual or sets of devices, and even other system level vulnerabilities (e.g., limited communication bandwidth). What follows is an overview of the well-defined scoring process selected and enhanced to score the importance of individual software vulnerabilities found within critical infrastructure control systems. After the overview, three vulnerability case studies are presented that demonstrate how the scoring might be used in practice.

Defined Scoring Process Overview

After a vulnerability is identified using the AVA system, CVSS version 2.0 will be used as the core scoring process for assessing the vulnerability's potential importance to critical infrastructure.

CVSS is composed of three metric groups, Base metrics, Temporal metrics, and Environmental metrics. The scoring process and definitions for the Base and Temporal groups have remained the same as in the original CVSS. For the Environmental group however, some definitions have been altered to reflect a primary interest in critical infrastructure and control systems. Even with this slight modification, the essence of the CVSS environmental scoring remains intact.

Each of the three CVSS related metric groups is evaluated separately and in parallel with each other in order to reduce the time required to assess the potential importance of identified vulnerabilities to critical infrastructure. Each of the metric groups is discussed below and may be found fully specified in Appendix B, which is the CVSS Version 2.0 scoring guide with a few additional comments, control system examples, and environmental metric changes made by this team.

Scoring the Three Metric Groups

Upon AVA identification of a vulnerability, the ICS-CERT, the National Vulnerability Database (NVD), and the system vendor will be consulted and the Base CVSS score will be determined. If the vulnerability is newly discovered then the Base score will need to be calculated. If the vulnerability was previously identified, but not known to exist in the system under AVA evaluation, then the calculated Base score will be used if it exists and is available. If there are multiple differing Base score assessments, the AVA team will contact each party and make a final determination. The Base CVSS metric captures the most critical attributes of a software vulnerability independent of the particular system or temporal context. The Base metric vulnerability attributes focus on the level of access needed by the attacker; the complexity of the required attack; the authentication requirements; and the confidentiality, integrity, and availability of information and functions of the specific device that contains the vulnerability. Details of these base attributes may be found in Appendix B, Section 2.1.

In parallel with the Base metric score determination, the Temporal group CVSS score attributes will be assessed. The Temporal metric is dependent on the changing posture of both potential attackers and defenders, and thus is not an attribute of the vulnerability itself. The attributes used by the Temporal metric are exploitability; availability of remediation; and the confidence in the reality of the vulnerability.

Exploitability assesses the ease and reliability of obtaining exploit code and the reliability of the attack technique used by the code. The INL Mission Support Center (MSC), ICS-CERT, and other designated groups, will be queried for the current level of exploitability of the vulnerability. This attribute generally changes over time so a structured and accepted request channel between the AVA team, the MSC, ICS-CERT, and other designated groups will need to be put in place.

Remediation determines the ease and availability of mitigations for the vulnerability (e.g., is a patch available). As an AVA identified vulnerability, mitigations such as patches and configuration work-arounds may be available if the vulnerability had been previously discovered. With AVA newly discovered vulnerabilities, there is a high likelihood that there are no easy or credible mitigations available. However, with time, mitigations may be developed and made available so this attribute's assessed value will need to be periodically reassessed and the overall importance score recalculated. ICS-CERT and the specific vendor will be the primary sources for aiding assessment of this attribute.

Confidence in a vulnerability report is usually a challenge. Assessing the reality of a vulnerability will be even more difficult when it is newly discovered through the AVA process. There will usually be the question of whether the vulnerability exists in the actual systems and not just in the AVA emulation of the system. Thus with AVA newly discovered vulnerabilities, the initial value of this attribute will be unconfirmed. As with all of the temporal metrics, this attribute will need to be continuously monitored and updated as appropriate. Further details of the Temporal metrics may be found in Appendix B, Section 2.2.

Concurrent with evaluation of the Base and Temporal metric groups, the Environmental group metric attributes will be evaluated. The CVSS Environmental group attributes have not been altered, but the definition for each of the possible attribute values have been altered from the standard CVSS definitions to better reflect the nature of critical infrastructures and the physical processes being controlled. The Environmental group attributes are intended to reflect the potential attacker impact on the critical infrastructure if they were to exploit the AVA identified vulnerability. The attributes used by the Environmental metric are collateral damage potential; attacker target distribution; and the confidentiality, integrity, and availability requirements for the system or sector under evaluation.

Collateral damage potential is an assessment of the potential indirect monetary damages due to exploitation of the AVA identified vulnerability. Attacker target distribution reflects the level of pervasiveness of the vulnerability within a critical infrastructure sector and its subsystems. The confidentiality, integrity, and availability requirements indicate the potential physical process performance impacts from attacker exploitation of the vulnerability. Details of these Environmental attributes may be found in Appendix B, Section 2.3, which includes new definitions for each of the values that the Environmental metric attributes may be assigned.

To calculate the Environmental metric for an AVA identified vulnerability, the vulnerability will be mapped to a generic device found in critical infrastructures (e.g., PLC) by the AVA team. The potential impact from the device will then be evaluated according to the Environmental attribute values provided in tables similar to those found in Appendix C, Power Sector Consequence table. The values in these tables will be generated through a combination of Subject Matter Experts (SMEs) and market penetration studies.

After the attribute values for the three CVSS metric groups have been calculated, they are combined, as defined in CVSS version 2.0, to yield a single vulnerability importance metric. To aid in understanding the scoring process, three vulnerability case studies are now discussed. CVSS v2 calculators are available online:

- NIST (http://nvd.nist.gov/cvss.cfm?calculator&version=2)
- FIRST (http://www.first.org/cvss/cvss_links)

Vulnerability Case Studies: Power Sector

In this section, three case studies of ICS vulnerabilities are explored. Three representative vulnerabilities were chosen to mimic discovery from AVA in order to test how the CVSS might apply to ICS devices and then analyze the feasibility of extrapolating the scoring system to determine the overall consequence that a vulnerability may have on and/or across an Industrial Control System.

The three vulnerabilities are:

1. Siemens Simatic HMI Insecure Authentication Token Generation
2. Rockwell Automation ControlLogix PLC Improper Authentication Firmware Upload
3. SUBNET Solutions SubSTATION Server Telegyr 8979 Improper Input Validation

In this process, first consult with ICS-CERT and the National Vulnerability Database (NVD) to see if the vulnerability has been previously identified and, if so, use the CVSS score already defined.

Below three vulnerabilities are examined and the modified CVSS process is stepped through to assess the potential importance of each relative to the power grid. Keep in mind that even though these particular vulnerabilities are known, for the purposes of this document some are treated as newly discovered vulnerabilities.

Siemens Simatic HMI Insecure Authentication Token Generation

It has been determined that this vulnerability occurs in the Human Machine Interface (HMI) web server in the Siemens WinCC flexible runtime that generates predictable authentication tokens for cookies which makes it easy for remote attackers to bypass authentication via crafted cookies. For this example, it is assumed that searches do not find this vulnerability on either the ICS-CERT website or the NIST NVD and it is a new vulnerability that has been discovered through the AVA process.

Searching for “Human Machine Interface” in the “Electric Grid Component / Subsystem” column in the Appendix C Table, it is noted that HMIs are software and hardware used as an interface between the operator and the PLCs controlling the process. HMIs perform the following tasks: system visualization, operator control of the system, alarm display, system value and alarm archiving, and machine parameter management. HMIs are used in nearly all industries with ICSs, including power, food and beverage, water and wastewater, oil and gas, and chemical.

Successful exploitation of this HMI vulnerability could allow an attacker to log on to a vulnerable HMI as a user or administrator, where they would be able to perform any of the system tasks configured for that HMI. The attacker might also be able to execute arbitrary code or obtain full access to files on the HMI system.

If this affected HMI is used to control a generation station or generator, then the attacker can modify operation of the generator in any way they choose.

Following the process of Figure 4 and referring to the table in Appendix C for a “Generation Station” under the “Generation” category, provides the purpose, status & control, digital flows, load/utility power flows, consequences, and environmental factors. These columns show the potential upstream/downstream systems that may be affected, and consequences of an attacker taking control of a generator.

CVSS Base Score

The process begins with calculating the CVSS base score by filling in the CVSS Base Score metrics with the known attributes of the vulnerability as follows:

- The attack can be accomplished over a network
- The access conditions are somewhat specialized
- No authentication is required to exploit the vulnerability
- Allows unauthorized disclosure of information
- Allows unauthorized modification of the system
- Allows disruption of service.

Exploitability Metrics become:

- Access Complexity (AC): Medium (M)
- Authentication (Au): Not required to exploit (N)
- Access Vector (AV): Network (N)

Impact Metrics become:

- Confidentiality (C): Complete (C)
- Integrity (I): Complete (C)
- Availability (A): Complete (C)

The CVSS Base Score calculations are as follows and a full discussion of them may be found in Appendix B:

```
BaseScore = (0.6 * Impact + 0.4 * Exploitability - 1.5) * f(Impact)
Impact = 10.41 * (1 - (1 - ConfImpact)*(1 - IntegImpact)*(1 - AvailImpact))
Exploitability = 20 * AccessComplexity * Authentication * AccessVector
f(Impact) = 0 if Impact=0; 1.176 otherwise

AccessComplexity = case AccessComplexity of
            high: 0.35
            medium: 0.61
            low: 0.71

Authentication  = case Authentication of
            Requires no authentication: 0.704
            Requires single instance of authentication: 0.56
            Requires multiple instances of authentication: 0.45

AccessVector   = case AccessVector of
            Requires local access: .395
            Adjacent Network accessible: .646
```

```
            Network accessible: 1

ConfImpact    = case ConfidentialityImpact of
            none:       0
            partial:     0.275
            complete:     0.660

IntegImpact   = case IntegrityImpact of
            none:       0
            partial:     0.275
            complete:     0.660

AvailImpact   = case AvailabilityImpact of
            none:       0
            partial:     0.275
            complete:     0.660
```

Using the above equations, the base score calculations for this vulnerability are as follows:

Impact metrics are all determined to be “Complete”; therefore the Impact variables are:

```
AvailImpact = 0.66
IntegImpact = 0.66
ConfImpact = 0.66
```

The Access Vector is “Network”; therefore the AccessVector variable is:

```
AccessVector = 1.0
```

No authentication is required, therefore the Authentication variable is:

```
Authentication = 0.704
```

The Access Complexity is “Medium”; therefore the AccessComplexity variable is:

```
AccessComplexity = 0.61
```

As stated above, the Exploitability equation is:

```
Exploitability = 20 * AccessComplexity * Authentication * AccessVector
```

The Exploitability calculation for this vulnerability becomes:

```
Exploitability = 20.0 * 0.61 * 0.704 * 1.0 = 8.589
```

The Impact equation is:

```
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
```

The Impact calculation for this vulnerability becomes:

```
Impact = 10.41 * (1 – (1 – 0.66) * (1 – 0.66) * (1 – 0.66) = 10.0
```

The f(Impact) function is:

```
f(Impact) = 0 if Impact=0; 1.176 otherwise
```

Since Impact > 0 f(Impact) returns:

```
f(Impact) = 1.176
```

Finally the BaseScore equation is:

```
BaseScore = (0.6 * Impact + 0.4 * Exploitability - 1.5) * f(Impact)
```

The resultant BaseScore calculation becomes:

```
BaseScore = (0.6 * 10.0 + 0.4 * 8.589 - 1.5) * 1.176 = 9.33
```

After performing the calculations it is found that the CVSS Base Score for this vulnerability is 9.33, which is considered high severity by NVD.

CVSS Temporal Score

The CVSS Temporal Score is important over time as vulnerabilities go through a life cycle from discovery to exploitation to mitigations; however vulnerabilities newly discovered via AVA are generally going to have the same Temporal Score.

- Exploitability (E) = Unproven (U)
- Remediation Level (RL) = Unavailable (U)
- Report Confidence (RC) = Uncorroborated (UR)

To calculate the Temporal Score for this vulnerability the following calculations are used:

```
TemporalScore = round_to_1_decimal(BaseScore * Exploitability
                * RemediationLevel * ReportConfidence)

Exploitability = case Exploitability of
                        unproven:      0.85 proof-
                                 of-concept:  0.90
                        functional:     0.95 high:
                                 1.00 not defined:
                                              1.00

RemediationLevel = case RemediationLevel of
                             official-fix:    0.87
                           temporary-fix:     0.90
                              workaround:     0.95
                        unavailable:      1.00 not
                                defined:      1.00

ReportConfidence = case ReportConfidence of
                            unconfirmed:      0.90
                            uncorroborated:   0.95
                         confirmed:       1.00 not
                                defined:      1.00
```

Since this is a newly discovered vulnerability, the following is determined:

```
BaseScore = 9.33
Exploitability = 0.85
RemediationLevel = 1.00
ReportConfidence = 0.95
```

Then, the following equation results:

```
TemporalScore = BaseScore * Exploitability
       * RemediationLevel * ReportConfidence

TemporalScore = 9.33 * 0.85 * 1.00 * 0.95 = 7.5
```

Therefore the initial Temporal Score for this vulnerability is 7.5.

CVSS Environmental Score

As stated above, to determine the Environmental metric attribute values for an AVA identified vulnerability, the vulnerability will be mapped to a generic device found in critical infrastructures, e.g. PLC, by the AVA team and the values in these tables will be generated through a combination of SMEs and market penetration studies.

The Environment metric values for this type of vulnerability are listed in Scenario 1, Environmental Factors for CVSS (Figure 8).

- Collateral Damage Potential (CDP) = High (H)
- Target Distribution (TD) = Low (L)
- System Confidentiality Requirement (CR) = Low (L)
- System Integrity Requirement (IR)= Medium (M)
- System Availability Requirement (AR) = Medium (M)

The CVSS equations are:

```
EnvironmentalScore = (AdjustedTemporal + (10 - AdjustedTemporal)
                    * CollateralDamagePotential)
                    * TargetDistribution

AdjustedTemporal = TemporalScore recomputed with the Impact sub-equation
          replaced with the following AdjustedImpact equation.

AdjustedImpact = Min(10, 10.41 * (1 - (1 - ConfImpact * ConfReq)
                * (1 - IntegImpact * IntegReq)
                * (1 - AvailImpact * AvailReq)))

CollateralDamagePotential = case CollateralDamagePotential of
                 none:      0.0
                 low:       0.1
                 low-medium:   0.3
                 medium-high:   0.4
                 high:      0.5
                 not defined:   0.0

TargetDistribution    = case TargetDistribution of
                 none:      0.00
                 low:       0.25
```

```
                 medium:     0.75
                 high:      1.00
                 not defined:   1.00

ConfReq    = case ConfidentialityImpact of
            Low:       0.50
            Medium:      1.00
            High:       1.51
            Not defined:   1.00

IntegReq   = case IntegrityImpact of
            Low:       0.50
            Medium:      1.00
            High:       1.51
            Not defined    1.00

AvailReq   = case AvailabilityImpact of
            Low:       0.50
            Medium:      1.00
            High:       1.51
            Not defined:   1.00
```

The equation variables become:

```
AvailReq = 1.0
IntegReq = 1.0
ConfReq = 0.50
TargetDistribution = 0.25
CollateralDamagePotential = 0.5
```

From the Base Score variables:

```
AvailImpact = 0.66
IntegImpact = 0.66
ConfImpact = 0.66
```

The Temporal Score calculations are as follows:

```
AdjustedImpact = Min(10, 10.41 * (1 - (1 - ConfImpact * ConfReq)
                * (1 - IntegImpact * IntegReq)
                * (1 - AvailImpact * AvailReq)))
```

Or

```
AdjustedImpact = Min(10, 10.41 * (1 - (1 – 0.66 * 0.50)
                * (1 – 0.66 * 1.0)
                * (1 – 0.66 * 1.0)))
```

Simplifying:

```
AdjustedImpact = Min(10, 9.6) = 9.6
```

AdjustedTemporal with BaseScore recalculated with the AdjustedImpact value:

```
BaseScore = (0.6 * AdjustedImpact + 0.4 * Exploitability - 1.5) * f(Impact)
BaseScore = (0.6 * 9.6 + 0.4 * 8.589 - 1.5) * 1.176 = 9.05

AdjustedTemporal = BaseScore*Exploitability*RemediationLevel*ReportConfidence
AdjustedTemporal = 9.05 * 0.85*1.0*0.95 = 7.3
```

And finally the Environmental Score equation:

```
EnvironmentalScore = (AdjustedTemporal + (10 - AdjustedTemporal)
                     * CollateralDamagePotential)
                     * TargetDistribution
EnvironmentalScore = (7.3 + (10.0 – 7.3) * 0.5) * 0.25 = 2.2
```

So for this particular vulnerability, the base score of 9.3 indicates it is a severe vulnerability but the environmental metric score of 2.2 indicates that it is not currently of significant consequence to the power grid. This seems to be a reasonable initial score given the metric attribute values assigned to the vulnerability.

Now it will be important to track the vulnerability and reassess its potential importance to the infrastructure as exploit code becomes more accessible, greater understanding of the vulnerabilities general pervasiveness increases, and the other values used in both the temporal and environmental metrics change. In general, it would be expected that the importance of the vulnerability will increase initially and thus the environmental metric will also increase. But as the importance rises, it is also expected that mitigations are likely to be developed and thus reduce the importance of the vulnerability.

Rockwell Automation ControlLogix PLC Improper Authentication Firmware Upload

After searching with ICS-CERT and the NVD, a vulnerability was found that was previously discovered as was first reported by Rubén Santamarta of IOActive and described in ICS-CERT Advisory ICSA-13-011-03 with the CVE number: CVE-2012-6437. With this vulnerability, the device does not properly authenticate users and the potential exists for a remote user to upload a new firmware image to the Ethernet card, whether it is a corrupt or legitimate firmware image. Successful exploitation of this vulnerability could cause loss of availability, integrity, and confidentiality and a disruption in communications with other connected devices.

The ICS-CERT Advisory ICSA-13-011-03 for this vulnerability provides an overview, list of affected products, impact, background, vulnerability characterization and mitigation.

According to Rockwell, the products that become affected by a vulnerability can be reset by rebooting or power cycling the affected product. After the reboot, the affected product will require upload of the legitimate firmware image and may require some reconfiguration. To mitigate this and other associated vulnerabilities, Rockwell developed and released security patches on July 18, 2012, to address them.

Following the process of Figure 4 and referring to the table in Appendix C to find “Transmission Network” row under the “Transmission Substation” category shows us the purpose, status & control, digital flows, load/utility power flows, consequences, and environmental factors. These columns show the potential upstream/downstream systems that may be affected and consequences of disruption of service (loss of view and control) for a transmission substation.

CVSS Base Score. The CVSS base score was previously determined by ICS-CERT to be 10.0 (high severity) where the Base metrics are described as:

Exploitability Metrics:

- Access Complexity (AC): Low (L)
- Authentication (Au): Not required to exploit (N)
- Access Vector (AV): Network (N)

Impact Metrics:

- Confidentiality (C): Complete (C) – Allows unauthorized disclosure of information
- Integrity (I): Complete (C) – Allows unauthorized modification
- Availability (A): Complete (C) – Allows disruption of service

The previously calculated Base Score of 10.0, the highest score possible, and of great concern.

CVSS Temporal Score. In consultation with ICS-CERT and MSC the Temporal attribute values and Temporal Score for this vulnerability have been determined to be:

- Exploitability: Proof-of-Concept (POC)
- Remediation: Official fix (OF)
- Report Confidence: Confirmed (C)

The Temporal Score variables become:

```
BaseScore = 10.0
Exploitability = 10.0
RemediationLevel = 0.87
ReportConfidence = 1.0
```

Then use the equation:

```
TemporalScore = BaseScore * Exploitability
       * RemediationLevel * ReportConfidence
```

To determine that:

```
TemporalScore = 10.00 * 0.90 * 0.87 * 1.0 = 7.8
```

CVSS Environmental Score

As stated above, to assess the Environmental metric for an AVA identified vulnerability, the vulnerability will be mapped to a generic device found in critical infrastructures (e.g., PLC) by the AVA team and the values in these tables will be generated through a combination of SMEs and market penetration studies.

The Environment metric values for this type of vulnerability are listed in Scenario 2, Environmental Factors for CVSS (Figure 12).

- Collateral Damage Potential (CDP) = High (H)
- Target Distribution (TD) = Medium (M)
- System Confidentiality Requirement (CR) = Low (L)
- System Integrity Requirement (IR)= Medium (M)
- System Availability Requirement (AR) = Medium (M)

The relevant CVSS Environmental equations are:

```
EnvironmentalScore = (AdjustedTemporal + (10 - AdjustedTemporal)
                    * CollateralDamagePotential)
                    * TargetDistribution
```

```
AdjustedTemporal = TemporalScore recomputed with the Impact sub-equation
          replaced with the following AdjustedImpact equation.

AdjustedImpact = Min(10, 10.41 * (1 - (1 - ConfImpact * ConfReq)
                * (1 - IntegImpact * IntegReq)
                * (1 - AvailImpact * AvailReq)))

CollateralDamagePotential = case CollateralDamagePotential of
                 none:      0.0
                 low:       0.1
                 low-medium:   0.3
                 medium-high:   0.4
                 high:      0.5
                 not defined:   0.0

TargetDistribution    = case TargetDistribution of
                 none:      0.00
                 low:       0.25
                 medium:     0.75
                 high:      1.00
                 not defined:   1.00

ConfReq    = case ConfidentialityImpact of
            Low:       0.50
            Medium:      1.00
            High:       1.51
            Not defined:   1.00

IntegReq   = case IntegrityImpact of
            Low:       0.50
            Medium:      1.00
            High:       1.51
            Not defined    1.00

AvailReq   = case AvailabilityImpact of
            Low:       0.50
            Medium:      1.00
            High:       1.51
            Not defined:   1.00
```

The Environmental Score variables become:

```
AvailReq = 1.00
IntegReq = 1.00
ConfReq = 0.50
TargetDistribution = 0.75
CollateralDamagePotential = 0.5
```

From the externally ICS-CERT generated Base Score calculation follows:

```
AvailImpact = 0.66
IntegImpact = 0.66
ConfImpact = 0.66
Exploitability = 10.0
```

The Temporal Score variables:

```
Exploitability = 0.9
```

```
RemediationLevel = 0.87
ReportConfidence 1.0
```

The Adjusted Impact equation:

```
AdjustedImpact = Min(10, 10.41 * (1 - (1 - ConfImpact * ConfReq)
                 * (1 - IntegImpact * IntegReq)
                 * (1 - AvailImpact * AvailReq)))
```

Or

```
AdjustedImpact = Min(10, 10.41 * (1 - (1 – 0.66 * 0.50)
                 * (1 – 0.66 * 1.00)
                 * (1 – 0.66 * 1.00)))
```

Simplifying:

```
AdjustedImpact = Min(10, 9.60) = 9.6
```

The AdjustedTemporal with the BaseScore recalculated with the AdjustedImpact values:

```
BaseScore = (0.6 * AdjustedImpact + 0.4 * Exploitability - 1.5) * f(Impact)
BaseScore = (0.6 * 9.60 + 0.4 * 10.0 - 1.5) * 1.176 = 9.7

AdjustedTemporal = BaseScore*Exploitability*RemediationLevel*ReportConfidence
AdjustedTemporal = 9.7 * 0.9 * .87 * 1.0 = 7.6
```

And finally the Environmental Score equations will be used to calculate the overall importance of this vulnerability to the power grid:

```
EnvironmentalScore = (AdjustedTemporal + (10 - AdjustedTemporal)
                     * CollateralDamagePotential)
                     * TargetDistribution
EnvironmentalScore = (7.6 + (10 – 7.6) * 0.5) * 0.75 = 6.6
```

For this particular vulnerability, the base score of 10.00 indicates it is a quite severe vulnerability, but the environmental metric score of 6.6 indicates that it is currently of medium importance to the power grid. As with the first vulnerability case study, this seems to be a reasonable initial score given the metric attribute values assigned to the vulnerability.

As with the first vulnerability, it will be important to continue tracking the vulnerability and reassess its potential importance to the infrastructure as the temporal and environmental metrics evolve over time.

SubSTATION Server Telegyr 8979 Improper Input Validation

This has been identified as a buffer overflow vulnerability in the SUBNET Solutions Inc (SUBNET), SubSTATION Server 2, Telegyr 8979 Master application. It was found that by sending a specially crafted packet simulating an RTU to Master message exceeding allowable data length, an attacker can cause the Telegyr 8979 Master to crash. SUBNET has also discovered that after sending a specially crafted message containing a valid data length, any subsequent message sent immediately to the Telegyr 8979 will also crash the service.

For this example, it is assumed that searches do not find this vulnerability on either the ICS-CERT website or the NIST NVD and it is a new vulnerability that has been discovered through the AVA process.

Unfortunately, it is not clear from the names of this component and application what general function it performs in the energy sector other than that it is associated with RTUs at power substations.

Looking up information on SubSTATION Server 2 from subnet.com, it is found that this system replaces legacy Remote Terminal Units, performs data collection and protocol conversion from disparate field devices, and serves as a communications gateway for all power substation data and commands going to/from the substation control center. The telecontrol protocol Telegyr 8979 was developed by the Landis & Gyr company for coupling telecontrol stations to Telegyr substations using the master/slave principle. Landis and Gyr no longer lists any products for Telegyr, thus this is a legacy protocol. SUBNET.com's Telegyr 8979 Master application converts from/to the legacy Telegyr 8979 protocol and is one of many legacy communications protocols supported by this RTU.

The SubSTATION Server 2 hardware/software functions as an RTU for power substations. Looking at the purpose and status & control for RTUs in the Table in Appendix C, it is noted that RTUs are used for autonomous or aided control of substation equipment. This means that they are designed to operate and maintain the system within their existing setpoint limits and controls unless they receive changes from their SCADA System master. Data from RTUs is sent to substation control centers and personnel or automation systems send control commands back to the RTU's if needed.

Following the process of Figure 4 and referring to the table in Appendix C to find "Distribution Network" under the "Distribution Substation" category shows us the purpose, status & control, digital flows, load/utility power flows, consequences, and environmental factors for this type of system. These columns show the potential upstream/downstream systems that may be affected and consequences of loss of view and control for a distribution substation.

Note that the buffer overflow vulnerability causes the Telegyr 8979 Master application to "crash," which means the application and the RTU stop working rather than actually being physically damaged. The RTU system will likely return to normal after an operator stops and restarts the RTU, but this will require an operator to travel to the substation to physically restart the RTU.

Buffer overflow vulnerabilities can sometimes be found to be exploitable, which means that an attacker may eventually be able to figure out how to use the vulnerability to make the application crash in a way that allows the attacker to execute malicious code on the RTU. However, since this is a newly found vulnerability, it is not yet known if it can be exploited to cause more than just crashing the application.

CVSS Base Score

Begin with calculating the CVSS Base Score by filling in the CVSS Base Score metrics with the assessed attribute values of the vulnerability as follows:

- The attack can be accomplished over a network
- The access conditions are somewhat specialized
- No authentication is required to exploit the vulnerability
- This is no unauthorized disclosure of information
- There is no unauthorized modification of the system
- The attack causes complete loss of availability to view and control for the SCADA system and its associated RTUs and power distribution segment(s) until the SCADA application can be restarted by an operator.

- The attack may cause disruption of power distribution service if the SCADA application cannot be restarted within a short period of time.

Exploitability Metrics:

- Access Complexity (AC): Medium (M)
- Authentication (Au): Not required to exploit (N)
- Access Vector (AV): Network (N)

Impact Metrics:

- Confidentiality (C): None (N)
- Integrity (I): None (N)
- Availability (A): Complete (C)

The CVSS Base Score calculations are:

```
BaseScore = (0.6 * Impact + 0.4 * Exploitability - 1.5) * f(Impact)
Impact = 10.41 * (1 - (1 - ConfImpact)*(1 - IntegImpact)*(1 - AvailImpact))
Exploitability = 20 * AccessComplexity * Authentication * AccessVector
f(Impact) = 0 if Impact=0; 1.176 otherwise

AccessComplexity = case AccessComplexity of
            high: 0.35
            medium: 0.61
            low: 0.71

Authentication  = case Authentication of
            Requires no authentication: 0.704
            Requires single instance of authentication: 0.56
            Requires multiple instances of authentication: 0.45

AccessVector   = case AccessVector of
            Requires local access: .395
            Adjacent Network accessible: .646
            Network accessible: 1

ConfImpact    = case ConfidentialityImpact of
            none:       0
            partial:     0.275
            complete:     0.660

IntegImpact   = case IntegrityImpact of
            none:       0
            partial:     0.275
            complete:     0.660

AvailImpact   = case AvailabilityImpact of
            none:       0
            partial:     0.275
            complete:     0.660
```

The CVSS base score calculations, as determined by the base metrics are as follows:

One Availability Impact metric value has been determined to be “Complete,” and the other two Impact metric values are “None”; therefore the Impact variables evaluate to:

```
AvailImpact = 0.66
IntegImpact = 0.0
ConfImpact = 0.0
```

The Access Vector is “Network”; therefore the AccessVector variable is:

```
AccessVector = 1.0
```

No authentication is required; therefore, the Authentication variable is:

```
Authentication = 0.704
```

The Access Complexity is “Medium”; therefore, the AccessComplexity variable is:

```
AccessComplexity = 0.61
```

The Exploitability equation is:

```
Exploitability = 20 * AccessComplexity * Authentication * AccessVector
```

The Exploitability calculation for this vulnerability is:

```
Exploitability = 20.0 * 0.61 * 0.704 * 1.0 = 8.59
```

The Impact equation is:

```
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
```

The Impact calculation for this vulnerability is:

```
Impact = 10.41 * (1 – (1 – 0.0) * (1 – 0.0) * (1 – 0.66) = 6.87
```

The f(Impact) function is:

```
f(Impact) = 0 if Impact=0; 1.176 otherwise
```

Since Impact > 0 the function f(Impact) returns 1.176:

```
f(6.87) = 1.176
```

Finally the BaseScore equation is:

```
BaseScore = (0.6 * Impact + 0.4 * Exploitability - 1.5) * f(Impact)
```

The resultant BaseScore calculation becomes:

```
BaseScore = (0.6 * 6.87 + 0.4 * 8.589 - 1.5) * 1.176 = 7.1
```

Thus the above calculations found that the CVSS Base Score for this vulnerability is 7.1, which is categorized as high severity by NVD.

CVSS Temporal Score

The CVSS Temporal Score is important; however, vulnerabilities newly discovered via AVA are generally going to have the same Temporal Score.

- Exploitability (E) = Unproven (U)
- Remediation Level (RL) = Unavailable (U)

- Report Confidence (RC) = Uncorroborated (UR)

To calculate the Temporal Score for this vulnerability the following calculations are used:

```
TemporalScore = round_to_1_decimal(BaseScore*Exploitability
                *RemediationLevel*ReportConfidence)


Exploitability = case Exploitability of
                        unproven:      0.85 proof-
                        of-concept:           0.90
                        functional:     0.95 high:
                        1.00      not      defined:
                        1.00
RemediationLevel   =   case   RemediationLevel   of
                        official-fix:         0.87
                        temporary-fix:        0.90
                        workaround:           0.95
                        unavailable:      1.00 not
                        defined:     1.00
ReportConfidence   =   case   ReportConfidence   of
                        unconfirmed:          0.90
                        uncorroborated:       0.95
                        confirmed:        1.00 not
                        defined:     1.00
```

Since this is a newly discovered vulnerability, determine the following variables:

```
BaseScore = 7.1
Exploitability = 0.85
RemediationLevel = 1.00
ReportConfidence = 0.95
```

Then use the equation:

```
TemporalScore = BaseScore * Exploitability
       * RemediationLevel * ReportConfidence
```

To calculate:

```
TemporalScore = 7.1 * 0.85 * 1.00 * 0.95 = 5.8
```

Therefore the initial Temporal Score for this vulnerability is 5.8.

CVSS Environmental Score

As stated above, to determine the Environmental metric attribute values for an AVA identified vulnerability, the vulnerability will be mapped to a generic device found in critical infrastructures (e.g., PLC) by the AVA team and the values in these tables will be generated through a combination of SMEs and market penetration studies.

The Environment metric values for this type of vulnerability are listed in Scenario 3, Environmental Factors for CVSS (Figure 16).

- Collateral Damage Potential (CDP) = Low-Medium (LM)
- Target Distribution (TD) = Medium (M)
- System Confidentiality Requirement (CR) = Low (L)

- System Integrity Requirement (IR)= Medium (M)
- System Availability Requirement (AR) = Medium (M)

The CVSS equations are:

```
EnvironmentalScore = (AdjustedTemporal + (10 - AdjustedTemporal)
                    * CollateralDamagePotential)
                    * TargetDistribution

AdjustedTemporal = TemporalScore recomputed with the Impact sub-equation
          replaced with the following AdjustedImpact equation.

AdjustedImpact = Min(10, 10.41 * (1 - (1 - ConfImpact * ConfReq)
                * (1 - IntegImpact * IntegReq)
                * (1 - AvailImpact * AvailReq)))

CollateralDamagePotential = case CollateralDamagePotential of
                 none:       0.0
                 low:        0.1
                 low-medium:    0.3
                 medium-high:    0.4
                 high:       0.5
                 not defined:    0.0

TargetDistribution    = case TargetDistribution of
                 none:       0.00
                 low:        0.25
                 medium:      0.75
                 high:       1.00
                 not defined:    1.00

ConfReq    = case ConfidentialityImpact of
            Low:        0.50
            Medium:       1.00
            High:       1.51
            Not defined:    1.00

IntegReq   = case IntegrityImpact of
            Low:        0.50
            Medium:       1.00
            High:       1.51
            Not defined    1.00

AvailReq   = case AvailabilityImpact of
            Low:        0.50
            Medium:       1.00
            High:       1.51
            Not defined:    1.00
```

The Environmental variables yield the following values:

```
AvailReq = 1.0
IntegReq = 1.0
ConfReq = 0.50
TargetDistribution = 0.75
CollateralDamagePotential = 0.3
```

From the Base Score calculation:

```
AvailImpact = 0.66
IntegImpact = 0.0
ConfImpact = 0.0
```

From the Temporal Score calculation:

```
Exploitability = 0.85
RemediationLevel = 1.00
ReportConfidence = 0.95
```

The AdjustedImpact value can now be calculated:

```
AdjustedImpact = Min(10, 10.41 * (1 - (1 - ConfImpact * ConfReq)
                * (1 - IntegImpact * IntegReq)
                * (1 - AvailImpact * AvailReq)))
```

Or:

```
AdjustedImpact = Min(10, 10.41 * (1 - (1 – 0.0 * 0.50)
                * (1 – 0.0 * 1.0)
                * (1 – 0.66 * 1.0)))
```

Simplifying:

```
AdjustedImpact = Min(10, 6.9) = 6.9
```

The AdjustedTemporal with the BaseScore recalculated with the AdjustedImpact value:

```
BaseScore = (0.6 * AdjustedImpact + 0.4 * Exploitability - 1.5) * f(Impact)
BaseScore = (0.6 * 6.9 + 0.4 * 8.59 - 1.5) * 1.176 = 7.12

AdjustedTemporal = BaseScore*Exploitability*RemediationLevel*ReportConfidence
AdjustedTemporal = 7.12 * 0.85 * 1.0 * 0.95 = 5.75
```

And finally the Environmental Score equation:

```
EnvironmentalScore = (AdjustedTemporal + (10 - AdjustedTemporal)
                    * CollateralDamagePotential)
                    * TargetDistribution
EnvironmentalScore = (5.75 + (10.0 – 5.75) * 0.3) * 0.75 = 5.3
```

For this particular vulnerability, the base score of 7.1 indicates it is a moderately severe vulnerability and the environmental metric score of 5.3 shows that it is currently of medium importance to the power grid. As with the previous two vulnerability case studies, this seems to be a reasonable initial importance score given the metric attribute values assigned to the vulnerability.

Also, as with the first two vulnerabilities it will be important to continue tracking the vulnerability and reassess its potential importance to the infrastructure as the temporal and environmental metrics evolve over time.

Vulnerability Case Study Summary

The three vulnerability case studies resulted in the vulnerability Base, Temporal, and Environmental CVSS 2.0 scores shown in Table 1. The Severity Ratings, based on CVSS 2.0 scores, are defined by the NVD as shown in Table 2. All three vulnerability case studies had vulnerabilities with Base scores in the high severity category, with the first two generally being considered very high severity.

However, when Temporal and Power Grid Environmental attributes were factored in, significant changes occurred in both the CVSS scores and the resulting NVD Severity Ratings. It should be noted that while each of the three vulnerabilities had different Base scores, the vulnerabilities used in Case Studies 1 and 3 had common Temporal attribute values and similar Environmental attribute values, with only the Target Distribution attribute value being different. Also, Case Studies 2 and 3 had similar Environmental attribute values, with only the Collateral Damage Potential attribute having different values.

Based on both the Temporal and Power Grid related Environmental metrics, it was found that the Siemens related vulnerability, used in Case Study 1, was reduced from a very high severity rating down to a quite low severity rating. A significant change! It was also determined that the Rockwell Automation vulnerability used in Case Study 2 had its NVD severity rating reduced from extremely high down to a fairly high, but clearly a medium severity. In addition, it was found that the SUBNET Solutions SubSTATION Server vulnerability used in Case Study 3 underwent the least reduction in CVSS score, although the NVD Severity Rating did decrease from high severity down to medium severity.

Table 1. CVSS 2.0 CVSS Scores for Vulnerabilities Used in Case Studies

Vulnerability Case Study	CVSS Base Score (NVD Severity)	CVSS Temporal Score (NVD Severity)	CVSS Modified Environmental Score (NVD Severity)
1 Siemens Simatic HMI Insecure Authentication Token Generation	9.3 (High)	7.1 (High)	2.2 (Low)
2 Rockwell Automation ControlLogix PLC Improper Authentication Firmware Upload	10.0 (High)	7.8 (High)	6.6 (Medium)
3 SubSTATION Server Telegyr 8979 Improper Input Validation	7.1 (High)	5.8 (Medium)	5.3 (Medium)

Table 2. NVD-defined Mapping from CVSS Score to Qualitative Severity Rating

CVSS Score	NVD Qualitative Severity Rating
7.0 – 10.0	High
4.0 – 6.9	Medium
0.0 – 3.9	Low

CONCLUSIONS

This report documents a metrics-based CPMP process to tie physical impact to the malicious exploitation of cyber vulnerabilities in ICS systems with the potential for initiating consequence in the critical infrastructure. The CPMP process utilizes a CLAPI approach that ties the vulnerability of a component, level of access to the component provided by the vulnerability, and the physical impact that can be exploited through the component to a metric based upon the well-recognized CVSS. A modified CVSS was detailed and demonstrated for the power sector in three case studies, with significant consequence detail applied to the process across the sector. The following summarizes each of these case studies in Table 1:

- As with any recognized vulnerability, those of greatest impact to the compromised device are of greatest importance. The CPMP process first selects those of high importance in evaluating the resulting impact to the physical environment. The base severity of all three vulnerabilities used in the case studies is high. This indicates that compromise of an exploit can be done remotely and be used to significantly degrade performance of the component.
- The temporal metric, if used for the CPMP, provides consideration of attributes that may change over time and should affect the timing of mitigation decisions. In the case of the three case studies, the existence of malicious code to exploit the vulnerability that does not have a patch available indicates a more severe risk. Two of the three use cases have a high severity Temporal metric value, but the relevance of this metric should also be weighed in light of the final physical impact.
- The Environmental metric adds to a vulnerability's Temporal metric by incorporating the potential physical and monetary impact from exploit of the vulnerability; the prevalence of the vulnerability; and the confidentiality, integrity, and availability requirements for the vulnerability given the components the vulnerability may be found on. Physical impact has been codified within the CLAPI based upon a tabular reference developed by subject matter experts (SMEs) for the generation, transmission, and distribution elements of the power grid. Prevalence has also been considered, based upon SME awareness of the level of diversity among vendors for particular types of ICS components. Two of the case studies revealed a medium severity Environmental metric, while one was low severity. Of the two medium severity vulnerabilities, one was close to being rated as high severity so it would be considered of greatest concern to the power grid. It is important to recognize that even though each of the case studies involved a vulnerability with a high severity base metric, none of the scores for the environmental metric were rated as high, primarily due to having been assigned a medium or low prevalence (Target Distribution) value.

In light of these results from the case studies, it is clear that several considerations are necessary when understanding the impact to critical infrastructure. The following provides conclusions for the relevance of the CPMP:

- As with any metrics system, an understanding of the significance of the attributes considered is important. In the case of the CPMP and the use of the CVSS, what appears to be a vulnerability of grave concern based on its base score, may not lead to a severe impact even if exploited. For example, the Target Distribution attribute of the environmental metric represents the vulnerability's prevalence, and has a great effect on the metric calculation and, consequently, on the final severity rating. Within the context of the case studies in this report, the identified vulnerabilities are not expected to lead to high consequence impacts and potential cascading failures, and thus their final ratings of medium and low severity seem reasonable.
- Detailed prevalence understanding on the level of use for a particular ICS component requires vendor sales/service information, which is known at a higher level from sources such as Newton-Evans. Additional analysis from subject matter experts and regional installation specifics will

provide the proper context of the vulnerability's impact. To provide greater granularity in the determination of the environmental metric, a detailed evaluation of prevalence is proposed in the second phase of this effort.

- The CVSS system is useable for ICS, but requires some modification to specifically reflect the application to critical infrastructure. Consideration of other variables that relate to the current environment of ever increasing threat, such as the ability of an adversary to chain vulnerabilities, is important for making an improved assessment of a vulnerability's severity. Chained vulnerabilities are expected to be partially addressed in CVSS 3.0 which is expected to be released soon. Phase 2 of this effort will look to take advantage of CVSS 3.0 enhancements and other related metrics work to provide insight into new useful variables to incorporate into the Environmental metric for ICS.
- To illustrate the benefit of the approach, examples of similar consequence detail is provided for the chemical, water and wastewater and oil/gas sectors. It is clear from these tables, provided in Appendix E, that the CPMP process can be applied cross-sector based upon the development of similar consequence-related information and scoring.

FUTURE WORK

The following is a statement of work based upon prior discussion with OCIA. Phase 2 will enhance the CPMP to provide a more granular evaluation of metrics correlating cyber vulnerability to consequence. This look will include ICS market data collection, chaining of vulnerabilities and potential modification of the scoring system (including CVSS 3.0, if released). Secondly, this effort will also take a first look at correlating potential threat actors and avenues for exploitation, including physical failure, which would result in the consequence scenario initiation. Finally, as the AVA project progresses in parallel, this effort will align with one asset owner and vendor to vet the overall CPMP.

Assumptions

- Consequence analysis will provide a perspective on cyber vulnerabilities and physical factors that can be the precursor of high impact facility consequences. It will not examine how these events might lead to cascading events outside of the facility.
- As the AVA project has just started, access to an asset owner and/or vendor may occur until mid-year or later of this second phase. Engagement with only one (stakeholder) of the asset owner or vendor representatives will be coordinated to support this effort in addition to AVA. Vetting of the CPMP will occur to the level afforded by the stakeholder, as a minimum providing a review as notionally applied to the stakeholder’s facility but potentially including emulated evidence.
- Consequence initiation scenarios established in Phase 1 will be applied in Phase 2, as applicable. In certain cases additional scenarios will be developed for relevance to the facility associated with the stakeholder.

Task 1: Requirements for Data Collection: Correlation of Cyber to Physical Assets

- Cyber
  - Addition of data sources to provide evidence for level of ICS device implementation in critical infrastructure.
  - Correlation of scenario vulnerabilities to facility ICS components that host the controls for the consequence scenarios.
- Physical
  - Vetting of CPMP against stakeholder expertise and available emulations as evidence to confirm propagation of consequence as established in scenarios.
- Cyber-Physical
  - Correlation of the potential for vulnerability exploitation against cyber threat actors.
  - Development of analysis methodologies for both physical and cyber degradation to demonstrate propagation through an ICS environment, establishing the likelihood of the resulting consequence scenario initiation.

Task 2: Consequence Analysis: Confirmation of Consequence Propagation

- Cyber
  - Establish metrics for a chain of vulnerabilities and threat actors to enhance the CPMP. Also, adapt the CPMP process to CVSS 3.0, if released.

- Physical
  - Establish physical factors leads to consequence initiation scenarios for facility of interest, given key ICS components are compromised.
- Cyber-Physical
  - Demonstrate, for facility of interest, methodologies that correlate cyber exposure to cyber-physical degrading effects and the resulting consequence scenarios.

Deliverables

- Summary report on application and update of CPMP for one facility containing:
  - Overview of facility environment and evaluation of consequence initiation scenarios.
  - Enhancement of CPMP process to include vulnerability clustering, introduction of market data on implementation of vendor-specific ICS devices, and update for CVSS 3.0.
  - Metrics based evaluation of cyber-physical avenues achieving consequence scenarios.
- Summary report of cyber-physical exposure containing:
  - Threat actor analysis relative to exploitation likelihood of relevant vulnerabilities.
  - Cyber-physical degradation analysis of precursors to resulting consequence scenarios.

APPENDICES

APPENDIX A
AVA PROJECT PHASES

APPENDIX A
AVA PROJECT PHASES

Three common objectives are associated with Phases 1 and 2 of this effort, with the outcomes for Phase 1 focused on risk mitigation based upon a proof of concept and Phase 2 in the integration of technologies for transition. These objectives are based upon the end-to-end process envisioned for the AVA as shown in Figure A-1. These objectives are categorized as follows:

- Objective 1: Automated gathering and extraction of ICS configuration
- Objective 2: Automated configuration replication in replicated environment
- Objective 3: Automated vulnerability assessment technique application.

Phase 1 of the AVA program will validate the concepts and formalize metrics against an implementation of the AVA for a single use case. This is a necessary step to ensure that the gaps recognized within this report can be addressed to the maturity expected by DHS S&T. The single use case will be based upon a real-world example currently available to the National Protection and Programs Directorate (NPPD)/ICS-CERT program. The proof of concept will apply leveraged technologies to the extent necessary to establish the metrics-based performance, concluding with a proof of concept demonstration.

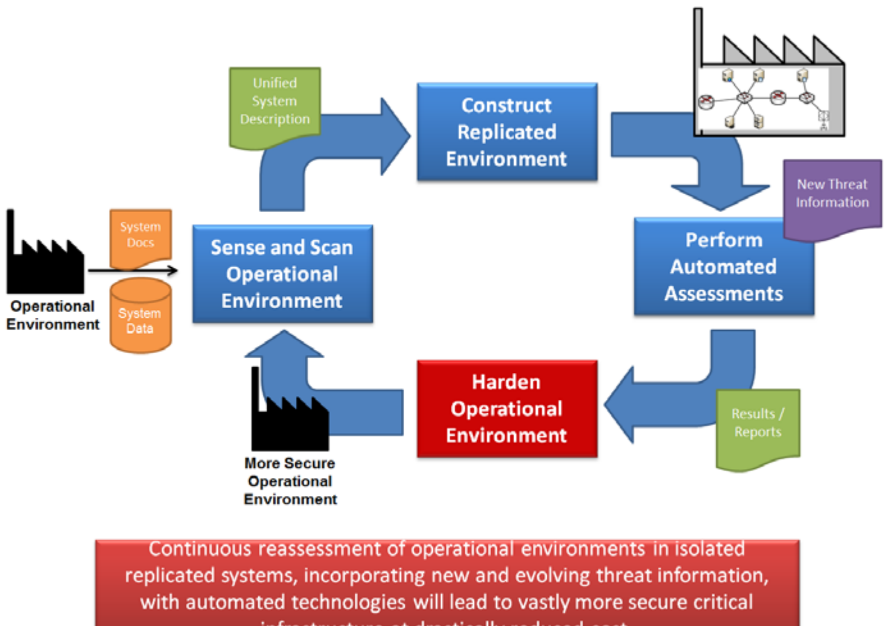


Figure A-1. AVA Objectives.

Each objective provides a necessary step in the development of the AVA, and therefore will have its own outcomes. The outcome for Objective 1 will be the demonstration of data gathering and extraction to metrics associated with data capture capability, detection and extraction accuracy, and impact. Use of automated scanning methods will be the primary source to collect data from asset owner implementations, but will be supplemented with other sources. These sources include automated scripting of a representative development system or system backups to complete the system picture, but minimizing the "hands-on" effort to do so. The outcome for Objective 2 will be the demonstration of the automated replication process, which takes the extraction data and uses this to build the replicated environment. For proprietary hardware, this includes a proof of concept that demonstrates ability to extract and emulate a simple proprietary controller in addition to a vendor-provided emulation. The performance of the approach, both fidelity and ease of implementation, will be measured by the accuracy and speed in establishing the replicated environment.

Phase 2 of the program will develop an operational application of the AVA, knitting together the leveraged technologies and developments from Phase 1. This demonstration will show a full integration of the technologies as applied to two asset owners, providing a necessary step to establish the process by which all ICS implementations can be similarly replicated. A cost of $3.5 million is estimated to fulfill this phase, scaled based upon the efforts of Draper, INL and LM ATL to evaluate and replicate two implemented environments to greater maturity.

As in Phase 1, each objective for Phase 2 has its own required outcome. For Objective 1, this outcome directly reflects the ability to automate the data gathering and extraction process. The resulting operational product will demonstrate the ability to closely extract the implemented environment, but do so with little in an operational deployment that cannot be automated. Note that the metrics associated with the Phase 2 outcomes are reflective of the refinement expected for this operational phase. The final metrics codified will be directly associated with the specifications of the environment expected by the sponsor(s) of Phase 3. The outcome for Objective 2 is the ability to replicate the environment to acceptable fidelity and provide for large-scale ICS implementations. For proprietary hardware, this includes a proof of concept that demonstrates ability to extract and emulate two proprietary devices in addition to vendor-provided emulations. Finally, the outcome for Objective 3 is the ability to perform an automated vulnerability assessment for two different ICS asset owner implementations. Depending upon the stakeholders supporting this effort, the intent is to replicate both a SCADA and a DCS architecture.

APPENDIX B
CVSS V2 SCORING GUIDE WITH ICS MODIFICATIONS

APPENDIX B
CVSS V2 SCORING GUIDE WITH ICS MODIFICATIONS

A Complete Guide to the Common Vulnerability Scoring System Version 2.0

June, 2007

Peter Mell, Karen Scarfone

National Institute of Standards and Technology

Sasha Romanosky

Carnegie Mellon University

Acknowledgements: The authors sincerely wish to recognize the contributions of all of the CVSS Special Interest Group members, including Barrie Brook, Seth Hanford, Stav Raviv, Gavin Reid, George Theall and Tadashi Yamagishi as well as the authors of the CVSS v1.0 standard [1].

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of three groups: Base, Temporal and Environmental. Each group produces a numeric score ranging from 0 to 10, and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

CONTENTS

1 INTRODUCTION

Currently, IT management must identify and assess vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk. But when there are so many to fix, with each being scored using different scales [2][3][4], how can IT managers convert this mountain of vulnerability data into actionable information? The Common Vulnerability Scoring System (CVSS) is an open framework that addresses this issue. It offers the following benefits:

Standardized Vulnerability Scores: When an organization normalizes vulnerability scores across all of its software and hardware platforms, it can leverage a single vulnerability management policy. This policy may be similar to a service level agreement (SLA) that states how quickly a particular vulnerability must be validated and remediated.

Open Framework: Users can be confused when a vulnerability is assigned an arbitrary score. “Which properties gave it that score? How does it differ from the one released yesterday?” With CVSS, anyone can see the individual characteristics used to derive a score.

Prioritized Risk: When the environmental score is computed, the vulnerability now becomes contextual. That is, vulnerability scores are now representative of the actual risk to an organization. Users know how important a given vulnerability is in relation to other vulnerabilities.

ICS Application: The document below has been modified to add examples of ICS-related application. The intent of this text is to clarify use in this deterministic environment that is distinctly different that IT.

2 WHAT IS CVSS?

CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics, as shown in Figure B-1.

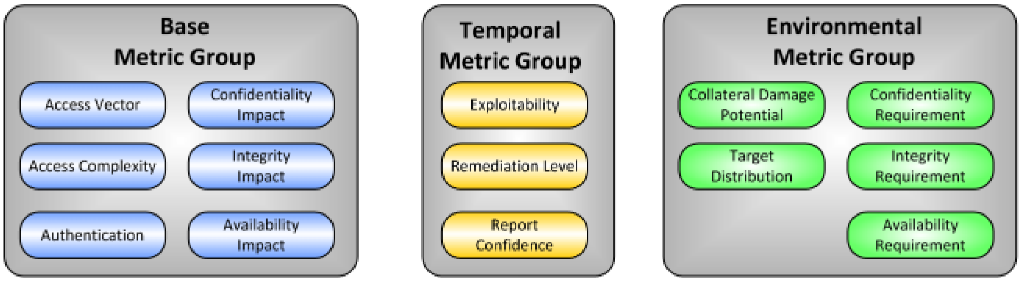


Figure B-1: CVSS Metric Groups

These metric groups are described as follows:

- **Base:** represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments. Base metrics are discussed in Section 2.1.
- **Temporal**: represents the characteristics of a vulnerability that change over time but not among user environments. Temporal metrics are discussed in Section 2.2.
- **Environmental**: represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment. Environmental metrics are discussed in Section 2.3.

The purpose of the CVSS base group is to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. Users can then invoke the temporal and environmental groups to provide contextual information that more accurately reflects the risk *to their unique environment*. This allows them to make more informed decisions when trying to mitigate risks posed by the vulnerabilities.

2.1 Other Vulnerability Scoring Systems

There are a number of other vulnerability "scoring" systems managed by both commercial and non-commercial organizations. They each have their merits, but they differ by what they measure. For example, CERT/CC produces a numeric score ranging from 0 to 180 but considers such factors as whether the Internet infrastructure is at risk and what sort of preconditions are required to exploit the vulnerability [3]. The SANS vulnerability analysis scale considers whether the weakness is found in default configurations or client or server systems [4]. Microsoft's proprietary scoring system tries to reflect the difficulty of exploitation and the overall impact of the vulnerability [2]. While useful, these scoring systems provide a one-size-fits-all approach by assuming that the impact for a vulnerability is constant for every individual and organization.

CVSS can also be described by what it is not. That is, it is none of the following:

- A threat rating system such as those used by the US Department of Homeland Security, and the Sans Internet Storm Center.[4] These services provide an advisory warning system for threats to critical US and global IT networks, respectively.
- A vulnerability database such as the National Vulnerability Database (NVD), Open Source Vulnerability Database (OSVDB) or Bugtraq. These databases provide a rich catalogue of known vulnerabilities and vulnerability details.

[4] http://www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm, http://isc.sans.org/

- A vulnerability identification system such as the industry-standard Common Vulnerabilities and Exposures (CVE) or a weakness dictionary such as the Common Weakness Enumeration (CWE). These frameworks are meant to uniquely identify and classify vulnerabilities according to the causes "as they are manifested in code, design, or architecture." [5]

2.2 How Does CVSS Work?

When the base metrics are assigned values, the base equation calculates a score ranging from 0 to 10, and creates a vector, as illustrated below in Figure B-2. The vector facilitates the "open" nature of the framework. It is a text string that contains the values assigned to each metric, and it is used to communicate exactly how the score for each vulnerability is derived. Therefore, the vector should always be displayed with the vulnerability score. Vectors are further explained in Section 2.4.

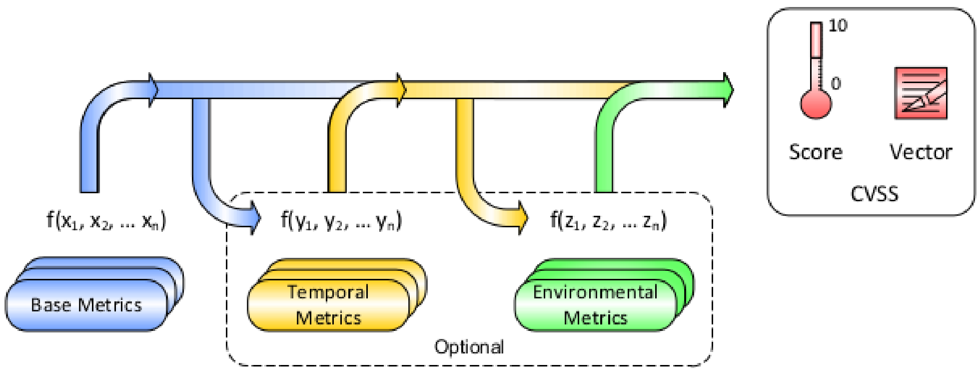


Figure B-2. CVSS Metrics and Equations

Optionally, the base score can be refined by assigning values to the temporal and environmental metrics. This is useful in order to provide additional context for a vulnerability by more accurately reflecting the risk posed by the vulnerability to a user's environment. However, this is not required. Depending on one's purpose, the base score and vector may be sufficient.

If a temporal score is needed, the temporal equation will combine the temporal metrics with the base score to produce a temporal score ranging from 0 to 10. Similarly, if an environmental score is needed, the environmental equation will combine the environmental metrics with the temporal score to produce an environmental score ranging from 0 to 10. Base, temporal and environmental equations are fully described in Section 3.2.

2.3 Who Performs the Scoring?

Generally, the base and temporal metrics are specified by vulnerability bulletin analysts, security product vendors, or application vendors because they typically have better information about the characteristics of a vulnerability than do users. The environmental metrics, however, are specified by users because they are best able to assess the potential impact of a vulnerability within their own environments.

2.4 Who Owns CVSS?

CVSS is under the custodial care of the Forum of Incident Response and Security Teams (FIRST).[6]However, it is a completely free and open standard. No organization "owns" CVSS and membership in FIRST is not required to use or implement CVSS. Our only request is that those

[5] http://cve.mitre.org/, http://cwe.mitre.org/index.html , http://cwe.mitre.org/about/process.html
[6] www.first.org/cvss

organizations who publish scores conform to the guidelines described in this document and provide both the score and the scoring vector (described below) so others can understand how the score was derived.

2.5 Who Is Using CVSS?

Many organizations are using CVSS, and each are finding value in different ways. Below are some examples:

Vulnerability Bulletin Providers: Both non-profit and commercial organizations are publishing CVSS base and temporal scores and vectors in their free vulnerability bulletins. These bulletins offer much information, including the date of discovery, systems affected and links to vendors for patching recommendations.

Software Application Vendors: Software application vendors are providing CVSS base scores and vectors to their customers. This helps them properly communicate the severity of vulnerabilities in their products and helps their customers effectively manage their IT risk.

User Organizations: Many private-sector organizations are using CVSS internally to make informed vulnerability management decisions. They use scanners or monitoring technologies to first locate host and application vulnerabilities. They combine this data with CVSS base, temporal and environmental scores to obtain more contextual risk information and remediate those vulnerabilities that pose the greatest risk to their systems.

Vulnerability Scanning and Management: Vulnerability management organizations scan networks for IT vulnerabilities. They provide CVSS base scores for every vulnerability on each host. User organizations use this critical data stream to more effectively manage their IT infrastructures by reducing outages and protecting against malicious and accidental IT threats.

Security (Risk) Management: Security Risk Management firms use CVSS scores as input to calculating an organization's risk or threat level. These firms use sophisticated applications that often integrate with an organization's network topology, vulnerability data, and asset database to provide their customers with a more informed perspective of their risk level.

Researchers: The open framework of CVSS enables researchers to perform statistical analysis on vulnerabilities and vulnerability properties.

2.6 Quick Definitions

Throughout this document the following definitions are used:

- **Vulnerability**: a bug, flaw, weakness, or exposure of an application, system, device, or service that could lead to a failure of confidentiality, integrity, or availability.
- **Threat**: the likelihood or frequency of a harmful event occurring.
- **Risk**: the relative impact that an exploited vulnerability would have to a user's environment.

3 METRIC GROUPS

3.1 Base Metrics

The base metric group captures the characteristics of a vulnerability that are constant with time and across user environments. The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. The three impact metrics measure how a vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability. For example, a vulnerability could cause a partial loss of integrity and availability, but no loss of confidentiality.

3.1.1 Access Vector (AV)

This metric reflects how the vulnerability is exploited. The possible values for this metric are listed in Table A-1. The more remote an attacker can be to attack a host, the greater the vulnerability score.

ICS: Other communication paths are frequently used in ICS, such as RS-232 and RS-485 serial connections. Many times data sharing and/or monitoring requirement between ICS sub-systems can create access vectors from one sub-system to another. These non-standard IT communication links must be evaluated as access vectors into Industrial Control Systems.

Table A-1: Access Vector Scoring Evaluation

Metric Value	**Description**
Local (L)	A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. Examples of locally exploitable vulnerabilities are peripheral attacks such as Firewire/USB DMA attacks, and local privilege escalations (e.g., sudo). **ICS Example: An attacker would need physical access to a Programmable Logic Controller (PLC) to manually switch it from “run” mode to “program” or “setup” mode in order to make modifications to its programming logic.**
Adjacent Network (A)	A vulnerability exploitable with *adjacent network access* requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. Examples of local networks include local IP subnet, Bluetooth, IEEE 802.11, and local Ethernet segment. **ICS Example: ICS adjacent network connections include many different ICS specific protocols such as BACnet, Modbus, Profibus, etc.**
Network (N)	A vulnerability exploitable with *network access* means the vulnerable software is bound to the network stack and the attacker does not require local network access or local access. Such a vulnerability is often termed “remotely exploitable”. An example of a network attack is an RPC buffer overflow. **ICS Example: ICS protocols such as BACnet, Modbus, Profibus, and others can have their own network stacks.**

3.1.2 Access Complexity (AC)

This metric measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. For example, consider a buffer overflow in an Internet service: once the target system is located, the attacker can launch an exploit at will.

Other vulnerabilities, however, may require additional steps in order to be exploited. For example, a vulnerability in an email client is only exploited after the user downloads and opens a tainted attachment. The possible values for this metric are listed in Table A-2. The lower the required complexity, the higher the vulnerability score.

ICS: ICS devices are subject to the same access complexity metrics.

Table A-2: Access Complexity Scoring Evaluation

Metric Value	Description
High (H)	Specialized access conditions exist. For example: • In most configurations, the attacking party must already have elevated privileges or spoof additional systems in addition to the attacking system (e.g., DNS hijacking). • The attack depends on social engineering methods that would be easily detected by knowledgeable people. For example, the victim must perform several suspicious or atypical actions. • The vulnerable configuration is seen very rarely in practice. • If a race condition exists, the window is very narrow. • **ICS Example: The attacking party needs detailed hands-on knowledge the ICS device.**
Medium (M)	The access conditions are somewhat specialized; the following are examples: • The attacking party is limited to a group of systems or users at some level of authorization, possibly untrusted. • Some information must be gathered before a successful attack can be launched. • The affected configuration is non-default, and is not commonly configured (e.g., a vulnerability present when a server performs user account authentication via a specific scheme, but not present for another authentication scheme). • The attack requires a small amount of social engineering that might occasionally fool cautious users (e.g., phishing attacks that modify a web browser's status bar to show a false link, having to be on someone's "buddy" list before sending an IM exploit). • **ICS Example: The attacking party needs basic ICS device knowledge.**
Low (L)	Specialized access conditions or extenuating circumstances do not exist. The following are examples: • The affected product typically requires access to a wide range of systems and users, possibly anonymous and untrusted (e.g., Internet-facing web or mail server). • The affected configuration is default or ubiquitous. • The attack can be performed manually and requires little skill or additional information gathering. • The "race condition" is a lazy one (i.e., it is technically a race but easily winnable). • **ICS Example: The ICS device has no access control or has default and/or hard-coded user names and passwords enabled.**

3.1.3 Authentication (Au)

This metric measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability. This metric does not gauge the strength or complexity of the authentication process, only that an attacker is required to provide credentials before an exploit may occur. The possible values for this metric are listed in Table A-3. The fewer authentication instances that are required, the higher the vulnerability score.

It is important to note that the Authentication metric is different from Access Vector. Here, authentication requirements are considered *once the system has already been accessed*. Specifically, for locally exploitable vulnerabilities, this metric should only be set to “single” or “multiple” if authentication is needed beyond what is required to log into the system. An example of a locally exploitable vulnerability that requires authentication is one affecting a database engine listening on a Unix domain socket (or some other non-network interface). If the user must authenticate as a valid database user in order to exploit the vulnerability, then this metric should be set to “single.”

ICS: ICS devices are subject to the same access authentication metrics; however the ICS device may have default and/or hard-coded user names and passwords. There is also a possibility that multiple ICS devices of the same kind within the ICS network utilize a common user name and password.

Table A-3: Authentication Scoring Evaluation

Metric Value	Description
Multiple (M)	Exploiting the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time. An example is an attacker authenticating to an operating system in addition to providing credentials to access an application hosted on that system. **ICS Example: Must log into the ICS device with a least user privilege account before providing higher level credentials.**
Single (S)	One instance of authentication is required to access and exploit the vulnerability.
None (N)	Authentication is not required to access and exploit the vulnerability. **ICS Example: The ICS device has no access control or has default and/or hard-coded user names and passwords.**

The metric should be applied based on the authentication the attacker requires before launching an attack. For example, if a remote mail server is vulnerable to a command that can be issued before a user authenticates, the metric should be scored as “None” because the attacker can launch the exploit before credentials are required. If the vulnerable command is only available after successful authentication, then the vulnerability should be scored as “Single” or “Multiple,” depending on how many instances of authentication must occur before issuing the command.

3.1.4 Confidentiality Impact (C)

This metric measures the impact on confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The possible values for this metric are listed in Table A-4. Increased confidentiality impact increases the vulnerability score.

ICS: ICS devices can contain a wealth of confidential information. This information can be set point values, pressure values, mixing times, temperatures, etc. A knowledgeable attacker can infer quite a bit about the process being controlled depending on the industrial control sector.

Table A-4: Confidentiality Impact Scoring Evaluation

Metric Value	Description
None (N)	There is no impact to the confidentiality of the system.
Partial (P)	There is considerable informational disclosure. Access to some system files is possible, but the attacker does not have control over what is obtained, or the scope of the loss is constrained. An example is a vulnerability that divulges only certain tables in a database. **ICS Example: An attacker can gain some confidential knowledge of a chemical process by capturing data from a process monitoring device.**
Complete (C)	There is total information disclosure, resulting in all system files being revealed. The attacker is able to read all of the system's data (memory, files, etc.) **ICS Example: An attacker can gain confidential knowledge of a chemical process by viewing the process control logic in a PLC.**

3.1.5 Integrity Impact (I)

This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information. The possible values for this metric are listed in Table A-5. Increased integrity impact increases the vulnerability score.

ICS: The Integrity of ICS devices varies based on the function of the device, in particular ICS devices may have set points or processing logic that could be added, modified, or deleted in a way that may be undetectable.

Table A-5: Integrity Impact Scoring Evaluation

Metric Value	Description
None (N)	There is no impact to the integrity of the system.
Partial (P)	Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited. For example, system or application files may be overwritten or modified, but either the attacker has no control over which files are affected or the attacker can modify files within only a limited context or scope. **ICS example: A Programmable Logic Controller (PLC) may not be able to be reprogrammed, but input set-points maybe modifiable causing a process to operate outside of safety bounds.**
Complete (C)	There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system. **ICS: The attacker is able to completely modify set-points, program logic, and directly interact with other devices and/or sub-processes.**

3.1.6 Availability Impact (A)

This metric measures the impact to availability of a successfully exploited vulnerability. Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of a system. The possible values for this metric are listed in Table A-6. Increased availability impact increases the vulnerability score.

ICS: An attacker may be able to disable access to a device by changing passwords, modifying firmware and/or program logic.

Table A-6: Availability Impact Scoring Evaluation

Metric Value	Description
None (N)	There is no impact to the availability of the system.
Partial (P)	There is reduced performance or interruptions in resource availability. An example is a network-based flood attack that permits a limited number of successful connections to an Internet service. **ICS example: An attacker could impact the quality a chemical process by causing an ICS device to periodically stop responding or transmitting data.**
Complete (C)	There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable. **ICS Example: An entire process can be halted by a vulnerable ICS device going off-line.**

3.2 Temporal Metrics

The threat posed by a vulnerability may change over time. Three such factors that CVSS captures are: confirmation of the technical details of a vulnerability, the remediation status of the vulnerability, and the availability of exploit code or techniques. Since temporal metrics are optional they each include a metric value that has no effect on the score. This value is used when the user feels the particular metric does not apply and wishes to “skip over” it.

3.2.1 Exploitability (E)

This metric measures the current state of exploit techniques or code availability. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability.

Initially, real-world exploitation may only be theoretical. Publication of proof of concept code, functional exploit code, or sufficient technical details necessary to exploit the vulnerability may follow.

Furthermore, the exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently. In severe cases, it may be delivered as the payload of a network-based worm or virus. The possible values for this metric are listed in Table A-7. The more easily a vulnerability can be exploited, the higher the vulnerability score.

Table A-7: Exploitability Scoring Evaluation

Metric Value	Description
Unproven (U)	No exploit code is available, or an exploit is entirely theoretical.
Proof-of-Concept (POC)	Proof-of-concept exploit code or an attack demonstration that is not practical for most systems is available. The code or technique is not functional in all situations and may require substantial modification by a skilled attacker.
Functional (F)	Functional exploit code is available. The code works in most situations where the vulnerability exists. **ICS example: Heartbleed (though not exclusive to ICS) has publicly available code to exploit the vulnerability.**
High (H)	Either the vulnerability is exploitable by functional mobile autonomous code, or no exploit is required (manual trigger) and details are widely available. The code works in every situation, or is actively being delivered via a mobile autonomous agent (such as a worm or virus). **ICS example: Stuxnet is able to leverage multiple exploits without the intervention of an attacker.**
Not Defined (ND)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

3.2.2 Remediation Level (RL)

The remediation level of a vulnerability is an important factor for prioritization. The typical vulnerability is unpatched when initially published. Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued. Each of these respective stages adjusts the temporal score downwards, reflecting the decreasing urgency as remediation becomes final. The possible values for this metric are listed in Table A-8. The less official and permanent a fix, the higher the vulnerability score is.

Table A-8: Remediation Level Scoring Evaluation

Metric Value	Description
Official Fix (OF)	A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available. **ICS example: The Windows exploits used by Stuxnet are now patched through Microsoft updates.**
Temporary Fix (TF)	There is an official but temporary fix available. This includes instances where the vendor issues a temporary hotfix, tool, or workaround.
Workaround (W)	There is an unofficial, non-vendor solution available. In some cases, users of the affected technology will create a patch of their own or provide steps to work around or otherwise mitigate the vulnerability.
Unavailable (U)	There is either no solution available or it is impossible to apply.
Not Defined (ND)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

3.2.3 Report Confidence (RC)

This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. Sometimes, only the existence of vulnerabilities are publicized, but without specific details. The vulnerability may later be corroborated and then confirmed through acknowledgement by the author or vendor of the affected technology. The urgency of a vulnerability is higher when a vulnerability is known to exist with certainty. This metric also suggests the level of technical knowledge available to would-be attackers. The possible values for this metric are listed in Table A-9. The more a vulnerability is validated by the vendor or other reputable sources, the higher the score.

Table A-9: Report Confidence Scoring Evaluation

Metric Value	Description
Unconfirmed (UC)	There is a single unconfirmed source or possibly multiple conflicting reports. There is little confidence in the validity of the reports. An example is a rumor that surfaces from the hacker underground.
Uncorroborated (UR)	There are multiple non-official sources, possibly including independent security companies or research organizations. At this point there may be conflicting technical details or some other lingering ambiguity.
Confirmed (C)	The vulnerability has been acknowledged by the vendor or author of the affected technology. The vulnerability may also be "Confirmed" when its existence is confirmed from an external event such as publication of functional or proof-of-concept exploit code or widespread exploitation. **ICS example: Reports from ICS-CERT and ICS device vendors.**
Not Defined (ND)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

3.3 Environmental Metrics

Different environments can have an immense bearing on the risk that a vulnerability poses to an organization and its stakeholders. The CVSS environmental metric group captures the characteristics of a vulnerability that are associated with a user's IT environment. Since environmental metrics are optional they each include a metric value that has no effect on the score. This value is used when the user feels the particular metric does not apply and wishes to "skip over" it.

ICS: The CVSS environmental metrics can provide meaningful information in trying to ascertain physical consequences from vulnerabilities within ICS devices that, if exploited, could have major impacts. See section 3.3.4 for additional guidance in determining the metric values.

3.3.1 Collateral Damage Potential (CDP)

This metric measures the potential for loss of life or physical assets through damage or theft of property or equipment. The metric may also measure economic loss of productivity or revenue. The possible values for this metric are listed in Table A-10. Naturally, the greater the damage potential, the higher the vulnerability score.

ICS: In the ICS realm, careful consideration must be taken on the number, location, function, and processes being controlled by the vulnerable device to effectively identify the appropriate metric value.

Table A-10: Collateral Damage Potential Scoring Evaluation

Metric Value	Description
None (N)	There is no potential for loss of life, physical assets, productivity or revenue.
Low (L)	A successful exploit of this vulnerability may result in slight physical or property damage. Or, there may be a slight loss of revenue or productivity to the organization.
Low-Medium (LM)	A successful exploit of this vulnerability may result in moderate physical or property damage. Or, there may be a moderate loss of revenue or productivity to the organization.
Medium-High (MH)	A successful exploit of this vulnerability may result in significant physical or property damage or loss. Or, there may be a significant loss of revenue or productivity.
High (H)	A successful exploit of this vulnerability may result in catastrophic physical or property damage and loss. Or, there may be a catastrophic loss of revenue or productivity.
Not Defined (ND)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Clearly, each organization must determine for themselves the precise meaning of "slight, moderate, significant, and catastrophic."

3.3.2 Target Distribution (TD)

This metric measures the proportion of vulnerable systems. It is meant as an environment-specific indicator in order to approximate the percentage of systems that could be affected by the vulnerability. The possible values for this metric are listed in Table A-11. The greater the proportion of vulnerable systems, the higher the score.

Table A-11: Target Distribution Scoring Evaluation

Metric Value	Description
None (N)	No target systems exist, or targets are so highly specialized that they only exist in a laboratory setting. Effectively 0% of the environment is at risk.
Low (L)	Targets exist inside the environment, but on a small scale. Between 1% - 25% of the total environment is at risk.
Medium (M)	Targets exist inside the environment, but on a medium scale. Between 26% - 75% of the total environment is at risk.
High (H)	Targets exist inside the environment on a considerable scale. Between 76% - 100% of the total environment is considered at risk.
Not Defined (ND)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

3.3.3 Security Requirements (CR, IR, AR)

These metrics enable the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user's organization, measured in terms of confidentiality, integrity, and availability, That is, if an IT asset supports a business function for which availability is most important, the analyst can assign a greater value to availability, relative to confidentiality and integrity. Each security requirement has three possible values: "low," "medium," or "high."

The full effect on the environmental score is determined by the corresponding base impact metrics. That is, these metrics modify the environmental score by reweighting the (base) confidentiality, integrity, and availability impact metrics.[7] For example, the confidentiality impact (C) metric has *increased* weight if the confidentiality requirement (CR) is "high." Likewise, the confidentiality impact metric has *decreased* weight if the confidentiality requirement is "low." The confidentiality impact metric weighting is neutral if the confidentiality requirement is "medium." This same logic is applied to the integrity and availability requirements.

Note that the confidentiality requirement will not affect the environmental score if the (base) confidentiality impact is set to "none." Also, increasing the confidentiality requirement from "medium" to "high" will not change the environmental score when the (base) impact metrics are set to "complete."

This is because the impact sub score (part of the base score that calculates impact) is already at a maximum value of 10.

The possible values for the security requirements are listed in Table A-12. For brevity, the same table is used for all three metrics. The greater the security requirement, the higher the score (remember that "medium" is considered the default). These metrics will modify the score as much as plus or minus 2.5.

Table A-12: Security Requirements Scoring Evaluation

Metric Value	Description
Low (L)	Loss of [confidentiality | integrity | availability] is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
Medium (M)	Loss of [confidentiality | integrity | availability] is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
High (H)	Loss of [confidentiality | integrity | availability] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
Not Defined (ND)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

In many organizations, IT resources are labeled with criticality ratings based on network location, business function, and potential for loss of revenue or life. For example, the U.S. government assigns every unclassified IT asset to a grouping of assets called a System. Every System must be assigned three "potential impact" ratings to show the potential impact on the organization if the System is compromised according to three security objectives: confidentiality, integrity, and availability. Thus, every unclassified IT asset in the U.S. government has a potential impact rating of low, moderate, or high with respect to the security objectives of confidentiality, integrity, and availability. This rating system is described within Federal Information Processing Standards (FIPS) 199.[8] CVSS follows this general model of FIPS 199, but does not require organizations to use any particular system for assigning the low, medium, and high impact ratings.

3.3.4 ICS Environmental Metric Enhancements

In order to enhance the Environmental Metrics to accommodate ICS devices and systems the following table has been added to this document in to assist in the determining of the appropriate values to calculate the Environmental score.

[7] Please note that the base confidentiality, integrity and availability impact metrics, themselves, are not changed.
[8] http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Table A-13. Evaluation Assumptions for ICS Environmental Factors

Collateral Damage Potential					
None	Low	Low Medium	Medium High	High	Not Defined
Vulnerable exploited without impact to systems	Slight Monetary damage covered by insurance and/or limited system disruption	Limited Monetary damage covered by insurance and/or system disruption	Monetary damage partially covered by insurance and/or Potential physical damage	Monetary damage not covered by insurance and/or Physical damage with hard to replace components due to tailored engineering or limited spares	

Target Distribution				
None 0%	Low 1-25%	Medium 26-75%	High 76-100%	
No evidence that vulnerable component exists in system	Vulnerable component rarely implemented in system	Vulnerable component readily identified in systems	Vulnerable component has ubiquitous functions in system	

System Confidentiality Requirement			
Low	Medium	High	Not Defined
State based information without context	Information in context but not complete system	End to end information on system in context	

System Integrity Requirement			
Low	Medium	High	Not Defined
Situational awareness, or current status repudiated	Situational awareness, and current status or control commands repudiated	Situational awareness, current status and control commands repudiated	

System Availability Requirement			
Low	Medium	High	Not Defined
Intermittent availability and/or loss of availability over a period of time that would impact performance	Intermittent availability and/or loss of availability over a period of time that would impact performance and control	Loss of availability over extended period of time	Local control remains available and operational

3.4 Base, Temporal, Environmental Vectors

Each metric in the vector consists of the abbreviated metric name, followed by a ":" (colon), then the abbreviated metric value. The vector lists these metrics in a predetermined order, using the "/" (slash) character to separate the metrics. If a temporal or environmental metric is not to be used, it is given a value of “ND” (not defined). The base, temporal, and environmental vectors are shown below in Table A-13.

Table A-13: Base, Temporal and Environmental Vectors

Metric Group	Vector
Base	AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]
Temporal	E:[U,POC,F,H,ND]/RL:[OF,TF,W,U,ND]/RC:[UC,UR,C,ND]
Environmental	CDP:[N,L,LM,MH,H,ND]/TD:[N,L,M,H,ND]/CR:[L,M,H,ND]/ IR:[L,M,H,ND]/AR:[L,M,H,ND]

For example, a vulnerability with base metric values of “Access Vector: Low, Access Complexity: Medium, Authentication: None, Confidentiality Impact: None, Integrity Impact: Partial, Availability Impact: Complete” would have the following base vector: “AV:L/AC:M/Au:N/C:N/I:P/A:C.”

4 SCORING

4.1 Guidelines

Below are guidelines that should help analysts when scoring vulnerabilities.

4.1.1 General

SCORING TIP #1: Vulnerability scoring should not take into account any interaction with other vulnerabilities. That is, each vulnerability should be scored independently.

SCORING TIP #2: When scoring a vulnerability, consider the direct impact to the target host only. For example, consider a cross-site scripting vulnerability: the impact to a user's system could be much greater than the impact to the target host. However, this is an indirect impact. Cross-site scripting vulnerabilities should be scored with no impact to confidentiality or availability, and partial impact to integrity.

SCORING TIP #3: Many applications, such as Web servers, can be run with different privileges, and scoring the impact involves making an assumption as to what privileges are used. Therefore, vulnerabilities should be scored according to the privileges most commonly used. This may not necessarily reflect security best practices, especially for client applications which are often run with root-level privileges. When uncertain as to which privileges are most common, scoring analysts should assume a default configuration.

SCORING TIP #4: When scoring the impact of a vulnerability that has multiple exploitation methods (attack vectors), the analyst should choose the exploitation method that causes the greatest impact, rather than the method which is most common, or easiest to perform. For example, if functional exploit code exists for one platform but not another, then Exploitability should be set to "Functional". If two separate variants of a product are in parallel development (e.g. PHP 4.x and PHP 5.x), and a fix exists for one variant but not another, then the Remediation Level should be set to "Unavailable".

4.1.2 Base Metrics

4.1.2.1 Access Vector

SCORING TIP #5: When a vulnerability can be exploited both locally and from the network, the "Network" value should be chosen. When a vulnerability can be exploited both locally and from adjacent networks, but not from remote networks, the "Adjacent Network" value should be chosen. When a vulnerability can be exploited from the adjacent network and remote networks, the "Network" value should be chosen.

SCORING TIP #6: Many client applications and utilities have local vulnerabilities that can be exploited remotely either through user-complicit actions or via automated processing. For example, decompression utilities and virus scanners automatically scan incoming email messages. Also, helper applications (office suites, image viewers, media players, etc.) are exploited when malicious files are exchanged via e-mail or downloaded from web sites. Therefore, analysts should score the Access Vector of these vulnerabilities as "Network".

4.1.2.2 Authentication

SCORING TIP #7: If the vulnerability exists in an authentication scheme itself (e.g., PAM, Kerberos) or an anonymous service (e.g., public FTP server), the metric should be scored as "None" because the attacker can exploit the vulnerability without supplying valid credentials. Presence of a default user account may be considered as “Single” or “Multiple” Authentication (as appropriate), but may have Exploitability of “High” if the credentials are publicized.

4.1.2.3 Confidentiality, Integrity, Availability Impacts

SCORING TIP #8: Vulnerabilities that give root-level access should be scored with complete loss of confidentiality, integrity, and availability, while vulnerabilities that give user-level access should be scored with only partial loss of confidentiality, integrity, and availability. For example, an integrity violation that allows an attacker to modify an operating system password file should be scored with complete impact of confidentiality, integrity, and availability.

SCORING TIP #9: Vulnerabilities with a partial or complete loss of integrity can also cause an impact to availability. For example, an attacker who is able to modify records can probably also delete them.

4.2 Equations

Scoring equations and algorithms for the base, temporal and environmental metric groups are described below. Further discussion of the origin and testing of these equations is available at www.first.org/cvss.

4.2.1 Base Equation

The base equation is the foundation of CVSS scoring. The base equation is:

```
BaseScore[9] = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)–1.5)*f(Impact))

Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))

Exploitability = 20* AccessVector*AccessComplexity*Authentication

f(impact)= 0 if Impact=0, 1.176 otherwise

AccessVector     = case AccessVector of
                        requires local access: 0.395
                        adjacent network accessible: 0.646
                        network accessible: 1.0

AccessComplexity = case AccessComplexity of
                        high: 0.35
medium: 0.61 low: 0.71

Authentication   = case Authentication of
                        requires multiple instances of authentication: 0.45
                        requires single instance of authentication: 0.56
                        requires no authentication: 0.704

ConfImpact       = case ConfidentialityImpact of
                        none:              0.0
                        partial:           0.275
                        complete:          0.660
```

[9] This is formula version 2.10

```
IntegImpact          =  case  IntegrityImpact  of
                         none:                  0.0
                         partial:             0.275
                         complete:           0.660

AvailImpact      = case AvailabilityImpact of

                         none:              0.0
                         partial:           0.275
                         complete:          0.660
```

4.2.2 Temporal Equation

If employed, the temporal equation will combine the temporal metrics with the base score to produce a temporal score ranging from 0 to 10. Further, the temporal score will produce a temporal score no higher than the base score, and no less than 33% lower than the base score. The temporal equation is:

```
TemporalScore = round_to_1_decimal(BaseScore*Exploitability

                *RemediationLevel*ReportConfidence)

Exploitability   = case Exploitability of

                         unproven:               0.85
                         proof-of-concept:       0.90
                         functional:             0.95
                         high:                   1.00
                         not defined:           1.00


RemediationLevel   =   case   RemediationLevel   of
                         official-fix:           0.87
                         temporary-fix:          0.90
                         workaround:             0.95
                         unavailable:            1.00
                         not defined:           1.00

ReportConfidence   =   case   ReportConfidence   of
                         unconfirmed:            0.87
                         uncorroborated:         0.90
                         confirmed:              0.95
                         not defined:           1.00
```

4.2.3 Environmental Equation

If employed, the environmental equation will combine the environmental metrics with the temporal score to produce an environmental score ranging from 0 to 10. Further, this equation will produce a score no higher than the temporal score. The environmental equation is:

```
EnvironmentalScore = round_to_1_decimal((AdjustedTemporal+

 (10-AdjustedTemporal)*CollateralDamagePotential)*TargetDistribution)

AdjustedTemporal = TemporalScore recomputed with the BaseScore’s Impact sub-
equation replaced with the AdjustedImpact equation

AdjustedImpact = min(10,10.41*(1-(1-ConfImpact*ConfReq)*(1-IntegImpact*IntegReq)

                  *(1-
                  AvailImpact*AvailReq)))

CollateralDamagePotential = case CollateralDamagePotential of

                                  none:            0
```

```
                                 low:              0.1
                                 low-medium:       0.3
                                 medium-high:      0.4
                                 high:             0.5
                                 not defined:     0
TargetDistribution       = case TargetDistribution of
                                 none:                0
                                 low:
                                 0.25         medium:
                                 0.75           high:
                                 1.00   not   defined:
                                 1.00
ConfReq          = case ConfReq of
                       low:             0.5
                       medium:            1.0
                       high:             1.51
                       not defined:      1.0
IntegReq         = case IntegReq of
                       low:               0.5
                       medium:            1.0
                       high:             1.51
                       not defined:      1.0
AvailReq         = case AvailReq of
                       low:               0.5
                       medium:            1.0
                       high:             1.51
                       not defined:      1.0
```

4.3 Examples

Below are examples of how CVSS is used for three different vulnerabilities.

4.3.1 CVE-2002-0392

Consider CVE-2002-0392: Apache Chunked-Encoding Memory Corruption Vulnerability. In June 2002, a vulnerability was discovered in the means by which the Apache web server handles requests encoded using chunked encoding. The Apache Foundation reported that a successful exploit can lead to denial of service in some cases, and in others, the execution of arbitrary code with the privileges of the web server.

Since the vulnerability can be exploited remotely, the Access Vector is "Network". The Access Complexity is "Low" because no additional circumstances need to exist for this exploit to be successful; the attacker need only craft a proper exploit message to the Apache web listener. No authentication is required to trigger the vulnerability (any Internet user can connect to the web server), so the Authentication metric is "None".

Since the vulnerability can be exploited using multiple methods with different outcomes, scores need to be generated for each method and the highest used.

If the vulnerability is exploited to execute arbitrary code with the permissions of the web server, thereby altering web content and possibly viewing local user or configuration information (including connection settings and passwords to back-end databases), the Confidentiality and Integrity Impact metrics are set to “Partial”. Together, these metrics result in a base score of 6.4.

If the vulnerability is exploited to cause a denial of service, the Availability Impact is set to "Complete". Together, the metrics produce a base score of 7.8. Since this is the highest possible base score of the exploitation options, it is used as the base score.

The base vector for this vulnerability is therefore: AV:N/AC:L/Au:N/C:N/I:N/A:C.

Exploit code is known to exist and therefore Exploitability is set to "Functional". The Apache foundation has released patches for this vulnerability (available to both 1.3 and 2.0) and so Remediation Level is "Official-Fix". Naturally, report confidence is "Confirmed". These metrics adjust the base score to give a temporal score of 6.4.

Assuming that availability is more important than usual for the targeted systems, and depending on the values for Collateral Damage Potential and Target Distribution, the environmental score could vary between 0.0 ("None"; "None") and 9.2 ("High"; "High"). The results are summarized below.

```
---------------------------------------------------
-  BASE  METRIC                           EVALUATION
SCORE
----------------------------------------------------
Access Vector               [Network]         (1.00)
Access Complexity           [Low]             (0.71)
Authentication              [None]           (0.704)
Confidentiality Impact      [None]            (0.00)
Integrity Impact            [None]            (0.00)
Availability Impact         [Complete]       (0.66)
---------------------------------------------------
- BASE FORMULA                                  BASE
SCORE
----------------------------------------------------
Impact = 10.41*(1-(1)*(1)*(0.34)) == 6.9
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore = (0.6*6.9 + 0.4*10.0 – 1.5)*1.176== (7.8)
----------------------------------------------------


----------------------------------------------------
TEMPORAL METRIC            EVALUATION        SCORE
----------------------------------------------------
Exploitability             [Functional]     (0.95)
Remediation Level          [Official-Fix]   (0.87)
Report Confidence          [Confirmed]      (1.00)
----------------------------------------------------
TEMPORAL FORMULA                      TEMPORAL SCORE
----------------------------------------------------
round(7.8 * 0.95 * 0.87 * 1.00)             == (6.4)
----------------------------------------------------
----------------------------------------------------
ENVIRONMENTAL METRIC        EVALUATION        SCORE
```

```
--------------------------------------------------
Collateral Damage Potential [None - High]  {0 - 0.5}
Target Distribution          [None - High]  {0 - 1.0}
Confidentiality Req.        [Medium]           (1.0)
Integrity Req.               [Medium]           (1.0)
Availability Req.          [High]            (1.51)
--------------------------------------------------
ENVIRONMENTAL FORMULA            ENVIRONMENTAL SCORE
--------------------------------------------------
AdjustedImpact = min(10,10.41*(1-(1-0*1)*(1-0*1)
         *(1-0.66*1.51))                  == (10.0)
AdjustedBase =((0.6*10)+(0.4*10.0)–1.5)*1.176
                                          ==  (10.0)
AdjustedTemporal  ==  (10*0.95*0.87*1.0)         ==
(8.3)  EnvScore  =  round((8.3+(10-8.3)*{0-0.5})*{0-
1})
                                   == (0.00 - 9.2)
--------------------------------------------------
```

4.3.2 CVE-2003-0818

Consider CVE-2003-0818: Microsoft Windows ASN.1 Library Integer Handling Vulnerability. In September 2003, a vulnerability was discovered that targets the ASN.1 library of all Microsoft operating systems. Successful exploitation of this vulnerability results in a buffer overflow condition allowing the attacker to execute arbitrary code with administrative (system) privileges.

This is a remotely exploitable vulnerability that does not require authentication, therefore the Access Vector is “Network” and “Authentication” is “None”. The Access Complexity is “Low” because no additional access or specialized circumstances need to exist for the exploit to be successful. Each of the Impact metrics is set to “Complete” because of the possibility of a complete system compromise. Together, these metrics produce a maximum base score of 10.0.

The base vector for this vulnerability is therefore: AV:N/AC:L/Au:N/C:C/I:C/A:C.

Known exploits do exist for this vulnerability and so Exploitability is “Functional”. In February 2004, Microsoft released patch MS04-007, making the Remediation Level “Official-Fix” and the Report Confidence “Confirmed”. These metrics adjust the base score to give a temporal score of 8.3. Assuming that availability is less important than usual for the targeted systems, and depending on the values for Collateral Damage Potential and Target Distribution, the environmental score could vary between 0.0 (“None”; “None”) and 9.0 (“High”; “High”). The results are summarized below.

```
--------------------------------------------------
BASE METRIC                 EVALUATION        SCORE
--------------------------------------------------
Access Vector                 [Network]        (1.00)
Access Complexity            [Low]             (0.71)
Authentication              [None]            (0.704)
Confidentiality Impact       [Complete]        (0.66)
Integrity Impact              [Complete]       (0.66)
Availability Impact        [Complete]      (0.66)
--------------------------------------------------
FORMULA                                  BASE SCORE
```

```
--------------------------------------------------
Impact = 10.41*(1-(0.34*0.34*0.34)) == 10.0
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore =((0.6*10.0)+(0.4*10.0)–1.5)*1.176
                                        == (10.0)
--------------------------------------------------

--------------------------------------------------
TEMPORAL METRIC            EVALUATION        SCORE
--------------------------------------------------
Exploitability              [Functional]      (0.95)
Remediation Level           [Official-Fix]    (0.87)
Report Confidence          [Confirmed]      (1.00)
--------------------------------------------------
FORMULA                                TEMPORAL SCORE
--------------------------------------------------
round(10.0 * 0.95 * 0.87 * 1.00) ==           (8.3)
--------------------------------------------------

--------------------------------------------------
ENVIRONMENTAL METRIC       EVALUATION        SCORE
--------------------------------------------------
Collateral Damage Potential [None - High]  {0 - 0.5}
Target Distribution          [None - High]  {0 - 1.0}
Confidentiality Req.       [Medium]            (1.0)
Integrity Req.              [Medium]            (1.0)
Availability Req.          [Low]             (0.5)
--------------------------------------------------
FORMULA                           ENVIRONMENTAL SCORE
--------------------------------------------------
AdjustedImpact = 10.41*(1-(1-0.66*1)*(1-0.66*1)
         *(1-0.66*0.5)) == 9.6
AdjustedBase =((0.6*9.6)+(0.4*10.0)–1.5)*1.176
                                         ==   (9.7)
AdjustedTemporal == (9.7*0.95*0.87*1.0)      == (8.0)
EnvScore = round((8.0+(10-8.0)*{0-0.5})*{0-1})
                ==                   (0.00 - 9.0)
--------------------------------------------------
```

4.3.3 CVE-2003-0062

Consider CVE-2003-0062: Buffer Overflow in NOD32 Antivirus. NOD32 is an antivirus software application developed by Eset. In February 2003, a buffer overflow vulnerability was discovered in Linux and Unix versions prior to 1.013 that could allow local users to execute arbitrary code with the privileges of the user executing NOD32. To trigger the buffer overflow, the attacker must wait for (or coax) another user (possibly root) to scan a directory path of excessive length.

Since the vulnerability is exploitable only to a user locally logged into the system, the Access Vector is “Local”. The Access Complexity is “High” because this vulnerability is not exploitable at the attacker's whim. There is an additional layer of complexity because the attacker must wait for another user to run the virus scanning software. Authentication is set to “None” because the attacker does not need to authenticate to any additional system. If an administrative user were to run the virus scan, causing the buffer overflow, then a full system compromise would be possible. Since the most harmful case must be considered, each of the three Impact metrics is set to “Complete”. Together, these metrics produce a base score of 6.2.

The base vector for this vulnerability is therefore: AV:L/AC:H/Au:N/C:C/I:C/A:C.

Partial exploit code has been released, so the Exploitability metric is set to “Proof-Of-Concept”. Eset has released updated software, giving a Remediation Level of “Official-Fix” and Report Confidence of “Confirmed”. These three metrics adjust the base score to give a temporal score of 4.9.

Assuming that confidentiality, integrity, and availability are roughly equally important for the targeted systems, and depending on the values for Collateral Damage Potential and Target Distribution, the environmental score could vary between 0.0 (“None”; “None”) and 7.5 (“High”; “High”). The results are summarized below.

```
--------------------------------------------------
-- BASE METRIC                         EVALUATION
SCORE
----------------------------------------------------
Access Vector                             [Local]
(0.395) Access Complexity                  [High]
(0.35) Authentication                      [None]
(0.704) Confidentiality Impact         [Complete]
(0.66) Integrity Impact                [Complete]
(0.66) Availability Impact             [Complete]
(0.66)
--------------------------------------------------
-- FORMULA                                   BASE
SCORE
----------------------------------------------------
Impact = 10.41*(1-(0.34*0.34*0.34)) == 10.0

Exploitability = 20*0.35*0.704*0.395 ==
1.9 f(Impact) = 1.176

BaseScore =((0.6*10)+(0.4*1.9)–1.5)*1.176

                                       ==  (6.2)
----------------------------------------------------


--------------------------------------------------
-- TEMPORAL METRIC                     EVALUATION
SCORE
----------------------------------------------------
Exploitability           [Proof-Of-Concept](0.90)

Remediation Level        [Official-Fix]   (0.87)
Report Confidence        [Confirmed]      (1.00)
```

```
----------------------------------------------------
FORMULA                               TEMPORAL SCORE
----------------------------------------------------
round(6.2 * 0.90 * 0.87 * 1.00) ==            (4.9)
--------------------------------------------------
--
--------------------------------------------------
--  ENVIRONMENTAL  METRIC               EVALUATION
SCORE
--------------------------------------------------
-- Collateral Damage Potential [None - High]  {0 -
0.5} Target Distribution         [None - High]  {0
-  1.0}  Confidentiality  Req.            [Medium]
(1.0)  Integrity  Req.                    [Medium]
(1.0)  Availability  Req.                 [Medium]
(1.0)
--------------------------------------------------
-- FORMULA                             ENVIRONMENTAL
SCORE
AdjustedTemporal == 4.9
EnvScore  =  round((4.9+(10-4.9)*{0-0.5})*{0-1})  ==   (0.00  -
7.5)
--------------------------------------------------
--
```

5 ADDITIONAL RESOURCES

Below is a list of resources that may be useful to anyone implementing CVSS. Vulnerability bulletins are helpful when searching for detailed information about a particular vulnerability. CVSS calculators are helpful when trying to compute your own base, temporal or environmental scores.

Vulnerability bulletins:

- The National Institute of National Institute of Standards and Technology (NIST) maintains the National Vulnerability Database (NVD), a vulnerability bulletin website that includes CVSS base scores. NIST provides these web-based bulletins in addition to XML feeds free for use. They can be found at http://nvd.nist.gov/nvd.cfm, and http://nvd.nist.gov/download.cfm#XML, respectively.
- IBM Internet Security Systems (ISS) publishes X-Force vulnerability bulletins free for use. They include CVSS base and temporal scores and can be found at http://xforce.iss.net/xforce/alerts.
- Qualys publishes vulnerability references that include both CVSS base and temporal scores. These can be found at http://www.qualys.com/research/alerts/.
- Cisco vulnerability bulletins including CVSS base and temporal scores can be found at http://tools.cisco.com/MySDN/Intelligence/home.x. (Note: requires a Cisco Connection Online account).
- Tenable Network Security publishes plugins for the Nessus vulnerability scanning tool. These plugins that include CVSS base score can be found at http://www.nessus.org/plugins/.

CVSS Calculators:

- The NIST CVSSv2 calculator can be found at http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2
- The Information-Technology Promotion Agency of Japan: http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/en/CVSSv2.html

6 FINAL REMARKS

The authors recognize that many other metrics could have been included in CVSS. Realize that no one scoring system will fit everyone's needs perfectly. The particular metrics used in CVSS were identified as the best compromise between completeness, ease-of-use and accuracy. They represent the cumulative experience of the CVSS Special Interest Group members as well as extensive testing of real-world vulnerabilities in end-user environments. As CVSS matures, these metrics may expand or adjust, making the scoring even more accurate, flexible and representative of modern vulnerabilities and their risks.

7 REFERENCES

[1] Mike Schiffman, Gerhard Eschelbeck, David Ahmad, Andrew Wright, Sasha Romanosky, “CVSS: A Common Vulnerability Scoring System,” National Infrastructure Advisory Council (NIAC), 2004.

[2] Microsoft Corporation. Microsoft Security Response Center Security Bulletin Severity Rating System. November 2002 [cited 16 March 2007]. Available from URL: http://www.microsoft.com/technet/security/bulletin/rating.mspx.

[3] United States Computer Emergency Readiness Team (US-CERT). US-CERT Vulnerability Note Field Descriptions. 2006 [cited 16 March 2007]. Available from URL: http://www.kb.cert.org/vuls/html/fieldhelp.

[4] SANS Institute. SANS Critical Vulnerability Analysis Archive. Undated [cited 16 March 2007].

[5] Available from URL: http://www.sans.org/newsletters/cva/.

APPENDIX C: POWER SECTOR CONSEQUENCE TABLE

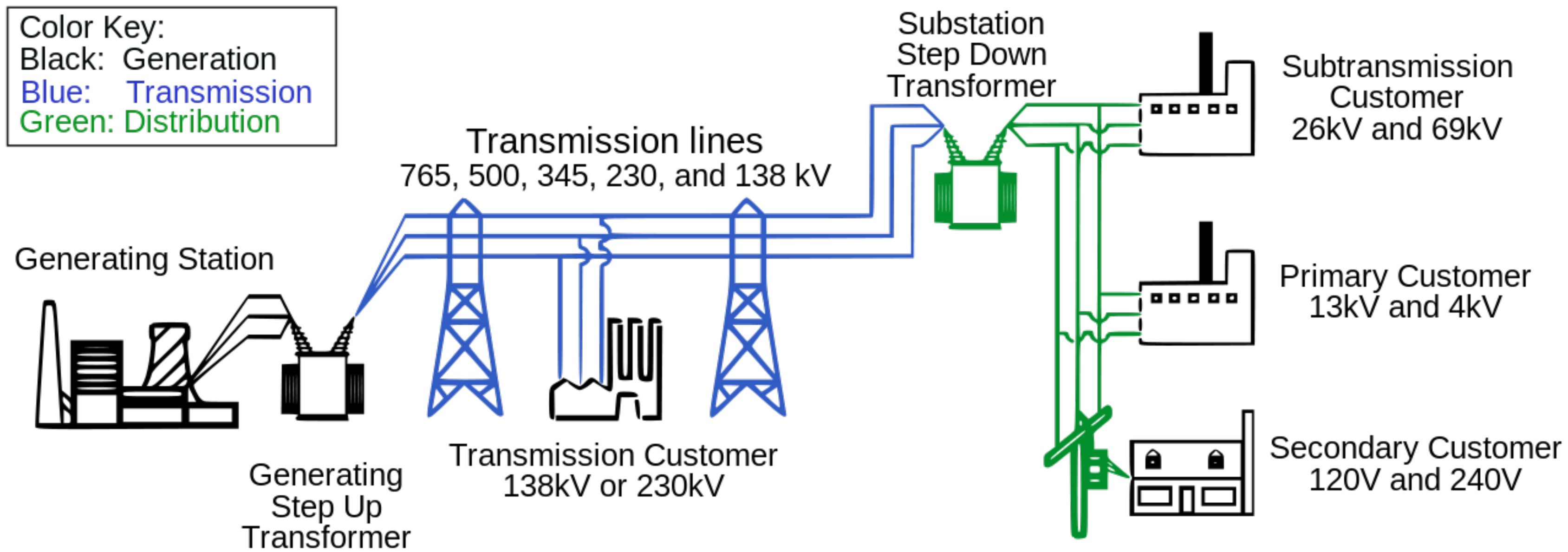


Figure C-1. Classical Representation of the US Electric Grid[1]

Figure C-1 represents the classical representation of the electric grid in the United States. This diagram does not represent the addition of digital devices that allow for communications and power controls to be managed in the new smart grid applications. The below simple diagram reflex the more advanced communications, intermittent generations, load control and distributed generation capabilities in today's grid.

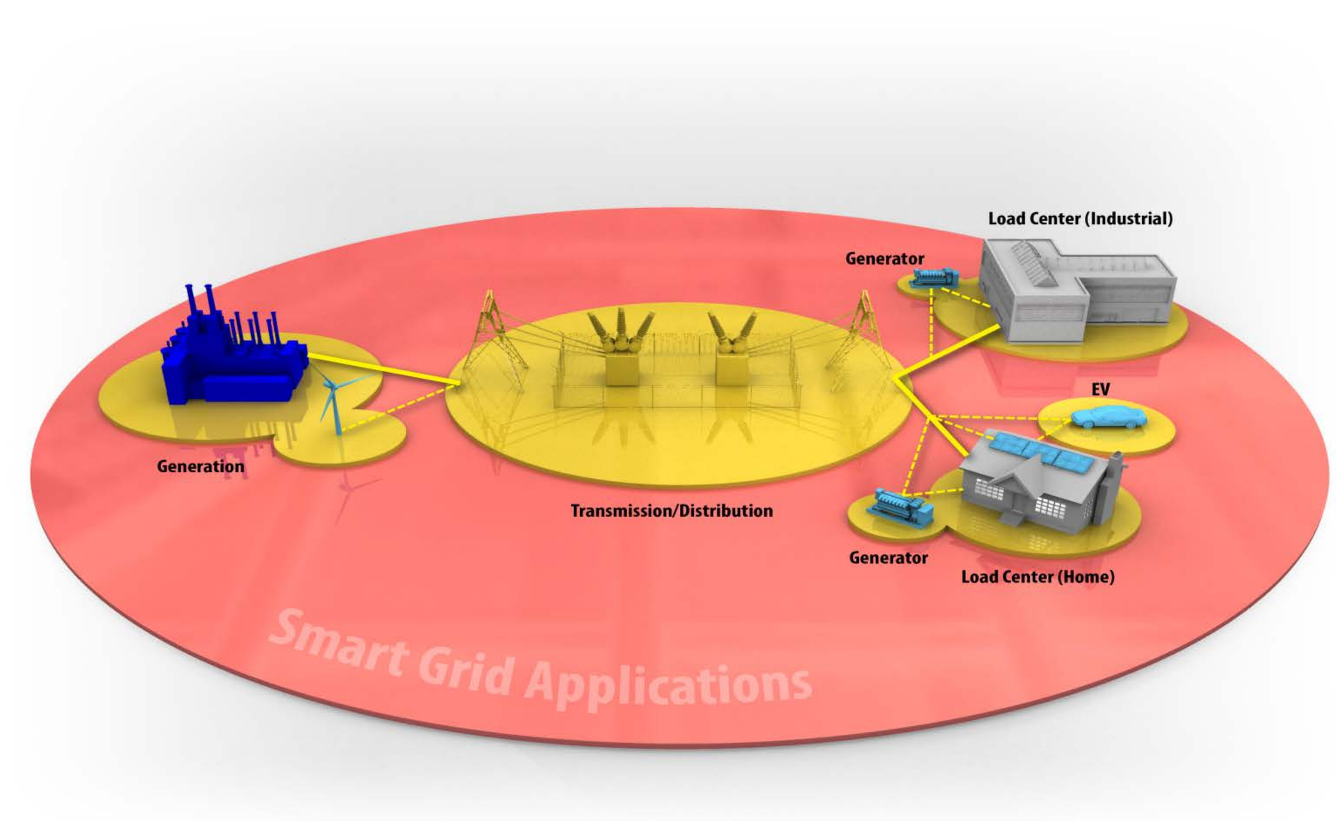


Figure C-2. Operational Representation of the US Electrical Grid

[1] http://en.wikipedia.org/wiki/Electricity_generation#mediaviewer/File:Electricity_grid_simple-_North_America.svg

Figure C-2 is a representation of the electric grid that considers evolution to smarter grid. Generation now contains larger (up to 30% in some locations) of intermittent renewable generations, load centers and residences that can provide limited generation or shed the load from the grid and go local generation only, and the traditional large plant generators (Fossil, Nuclear and Hydro). The Transmission/Distribution networks contain digital and electro mechanical operations to manage the limited resource of transmission of remote generation to load centers. The loads may be residential with vehicle to grid, roof top photovoltaics, and local backup generations to large load centers with uninterruptable power supplies and facility generation. Many load centers now have the capability to isolate from the grid for limited periods of time and reconnect. These decisions are made based on the reliability of the central grid or energy prices. Other net metering applications allow for the load center to provide power back to the electric grid. Residential customers can sell the energy produced by the roof top photovoltaics back to the central utility grid during daylight hours and use energy from the central utility grid during nighttime or other if need more power.

Table C-1 describes components commonly found on the electric grid. The electric grid in the United States is made up from three different electric interconnects (Eastern, Western and Texas) which are tied together allowing limited power flows between. These interconnections evolved over many years to the reliable electric grid we have today. Many new smart grid technologies have been added to the grids recently mainly impacting the distribution areas of the grid. Not all electric grid applications and components are listed but a range of applications and components to show the complexity. The major subsystems in the components described are:

- Generation,
- Transmission,
- Applications – SCADA, DCS, Specialized Equipment (RTU, PLC, IED)
- Distribution,
- Residential,
- Industrial and Commercial Loads and
- Energy Markets.

The Applications subsection describes the functions that maybe implement in any other of the subsystems. Due to the nature of the electric grids, not all applications' status and control are digital. Older electro mechanical status and control are common on older transmission subsystems and can still be found in some distribution, generation functions. Other newer components on the grid (i.e. wind turbines and advanced metering) will be digital control and status. The headings of Table C-1 are described as follows:

- Electric Grid Component/Subsystem: Scope of apparatus discussed.
- Purpose: Role the component/subsystem provided in the electric grids.
- Status & Control: Distinction between typical status and control mechanisms. While no communications is strictly one way in a cyber security view (host computer someplace to impact communications), status is generally from the component into the larger subsystems, and control acts on the status(es) or a command from an operator from the subsystem to the component.
- Digital Flows: Show the data network connectivity from the component to subcomponents to larger subsystems, control centers, and SCADA/EMS. If other control is not digital, electro mechanical functions are noted to understand impact determinations. Electromechanical controls works on a level of voltage on a copper wire that when raised or decreased cause a mechanical function (i.e. tripping a breaker).
- Load/Utility Power Flow: Describes the connectivity of the electric grid physics independent from the data communications.
- Consequence: This column follows the same logic as the Environmental Factors in the CVSS 2.0 with Monetary and Reputation also summarized for impact.

The CVSS 2.0 Environmental Factor categories scored in Table C-1 have the following options:

- **Metric:** CDP = Collateral Damage Potential (Organization specific potential for loss)
  Possible Values: N = None, L = Low, LM = Low-Medium, MH = Medium-High, H = High, ND = Not Defined
- **Metric:** TD = Target Distribution (Percentage of vulnerable systems)
  Possible Values: N = None (0%), L = Low (1-25%), M = Medium (26-75%), H = High (76-100%), ND = Not Defined
- **Metric:** CR = System Confidentiality Requirement (draft proposal)
  Possible Values: L = Low, M = Medium, H = High, ND = Not Defined
- **Metric:** IR = System Integrity Requirement (draft proposal)
  Possible Values: L = Low, M = Medium, H = High, ND = Not Defined
- **Metric:** AR = System Availability Requirement (draft proposal)
  Possible Values: L = Low, M = Medium, H = High, ND = Not Defined

Evaluation Assumptions for Environmental Factors are as follows, given that the highlighted scoring in Table A-13 is based upon worst case scenarios for a given subsystem or component:

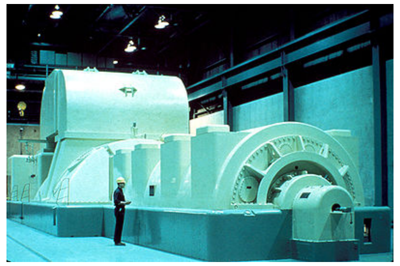
- Collateral Damage Potential: The consequence discussion includes monetary and physical damage which can be related to the subjective rating in collateral damage potential. Some components have large monetary value if physically damaged (i.e. large transformers), while other components may be easier to replace (i.e. historian database). If the damage potential is very localized, the rating would be lower (i.e. distribution meter vs transmission breaker).
- Target Distribution: Not all components are digital and will have a cyber-impact (i.e. electro-mechanical relays do not have an embedded digital system). To understand the Environmental Factors, the maximum impact based on the limited information available, is represented in the Target Distribution factor. For example, Relays are estimated to have a Target Distribution of 50% since most relays in transmission networks are electro-mechanical

and not readily impacted by a cyber-attack. If digital relay vendor X had an exploitable vulnerability with an impact, which would represent a smaller percentage than the 50% Target Distribution since vendor X does not supply all digital relays in the United States. Market surveys, installation specifics and subject matter experts will be needed to better understand the environmental factors.

- System Confidentiality: For the state and temporal nature of the electric grid, confidentiality is a lesser concern unless dealing with customer data.
- System Integrity: The ability for operations to understand the correct state or situational awareness makes integrity an important environmental factor for the electric grid.
- System Availability: Based on the safety and security needs of the electric grid, some command operations need to occur with minimum latency and in proper sequence with other actions making availability an important environment factor for control aspects of the electric grid.

Generation

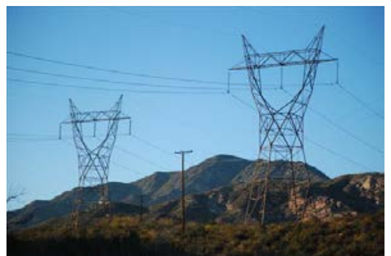
			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Digital Flows**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Generation Station – Balance of Plant  	Converts fuels or nuclear reaction energy to electric power, usually via steam-turning turbines coupled to electric generators. Some generation stations use a combination of steam and/or combustion exhaust to turn turbines. Generation stations are similar to any complex manufacturing plant with many subsystems to support the conversion of raw materials into a finished product. Large generating stations can take hours or days to respond to major changes to power output needed by the grid.	Power plants contain many industrial control and instrumentation systems. Primary plant controls • Fuel supply system • Fire/burner control • Feed water pumps • Steam valve motors • Chill water pumps • Oiling system • Water chemistry system • Temperature and pressure monitoring system	Energy Management Systems with digital and analog input/output, Human Machine Interfaces (HMI), status and control • Generation Dispatch Control • Voltage Regulation Control • Automatic Generation Control (AGC) Plant Operation Systems • Programmable Logic Controllers (PLC), Intelligent End Devices (IED), Remote Terminal Units (RTU) • HMI • Motor VSD, starters • Monitoring systems • Cooling • Balance of Plant Systems • Emergency Generation for shutdown or startup • Generation Substations • Step Up for Transmission	Utility Upstream – Energy Management Systems • Generation Dispatch Control • Voltage Regulation Control • Fuel Consumption / Fuel Costs Downstream – Plant Operation Systems • PLC • Motor VSD, starters • Monitoring systems	Monetary - Operating outside of EPA and other regulatory requirements Physical Damage - Physical damage to parts and equipment in balance of plant; Damage to core reactor highly unlikely; Collateral damage to balance of plant systems likely, limited target distribution due to isolation of systems and boundary protections Loss of Confidence - is low since time sensitive information Loss of Integrity – Balance of plant subsystems likely Loss of Availability - Nuisance failures and shut downs of subsystems. Long term power loss if failures cascade to a complete system shutdown since generating stations can take days or more to restart Reputation - Radiological or toxic material release highly unlikely but quite damaging to a company's reputation if one occurs; Frequent Loss of availability or unstable plant operation could result in major customers switching to alternate generation sources	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Generator Subsystem: Generation Station % in Subsystem 20% nuclear-60% Fossil/hydro N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Digital Flows**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Classical Generator 	Converts rotational mechanical power to electrical power (fossil, hydro, nuclear and wind) Protection systems, including: Excitation Control - maintaining electro-mechanical frequency/terminal voltage regulation, loss of excitation, and power system stabilizer. Power Control - reverse power protection (turns generator into a motor), frequency regulation, and area power control (generation equal to demand and tie line power commitments). Electrical Fault Control – over/under frequency and voltage	Local controls • Excitation control – DCS • Synchronization control – sync check relay • Speed control • Turbine governor control - DCS Protection controls – Current transformers (CT) Potential transformers (PT) and Voltage Transformers (VT), CT, PT/ VT, and circuit breaker • Electrical fault control • Reverse power detection • Loss of excitation detection Operational Control: • Automatic generation control – SCADA Maintenance status: oil Remote vendor access	Upstream – Energy Management System • Generation Dispatch Control • Voltage Regulation Control • Automatic Generation Control Downstream – Plant Operation Systems • PLC • Motor VSD, starters • Fuel Feeders • Balance of Plant Systems • Emergency Generation • Generation Substations • Step Up for Transmission • Remote maintenance connection with vendor	Utility Upstream • prime mover system (mechanical): speed regulation and steam valve motor • Dispatch control Plant subsystems-transform to transmission Downstream • generator step-up transformer, connecting to the grid • instrumentation transformers (CT & PT) to protective relays and control systems • DCS for generator, maintenance systems, vendor access, Automated Generation Control, SCADA	Monetary: if physical or if failed to provided expected generation Physical Damage: out of sync, loss of lubricant; Reduction of operational life; Loss of Confidentiality: Market estimates based on generation capacity Loss of Integrity: If spoofed synchronization, preventive maintenance data Loss of Availability: Power Outage localized or if coordinated and networked wide spread; Loss of stability of grid operations if large generations isolated from other generation and limited transmission Reputation: Unstable generation	**CDP** Collateral Damage Potential N | L | LM | **MH** | H | ND **TD** Target Distribution Component: Generator Subsystem: Generation % in Subsystem: 80-99% N | L | **M** | H | ND **CR** System Confidentiality Requirement **L** | M | H | ND **IR** System Integrity Requirement L | **M** | H | ND **AR** System Availability Requirement L | **M** | H | ND

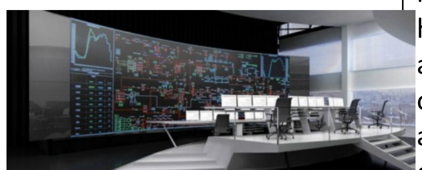
			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Digital Flows**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Large-Scale Intermittent Generation Solar and Wind Farms 	Converts renewable energy resources to electric power. Production scale is on the order of a moderate size power plant (50 MW to 300 MW). Multiple instances of subsystems to support the conversion of raw materials into a finished product.	Many industrial control and instrumentation systems. Primary plant controls • Weather monitoring system • Rotational positioning control • Cooling systems • Power regulating system • Voltage regulating system • Oiling system • Data monitoring system Protection controls – CT, PT/ VT, and circuit breaker • Electrical fault control • Reverse power detection • Loss of excitation detection Operational Control: • Automatic generation control – SCADA Maintenance status Remote vendor access	Upstream – Energy Management System • Generation Dispatch Control • Voltage Regulation Control • Automatic Generation Control • Blade Tilt • Turbine Control Downstream – Plant Operation Systems • PLC • Motor VSD, starters • Generation Substations • Step Up for Transmission	Utility Upstream – Energy Management System • Generation Dispatch Control • Voltage Regulation Control • Fuel Consumption / Fuel Costs Downstream – Turbine/DC-AC inverter/converters Systems • PLC • Motor starters and variable speed drives • Power inverters / converters Monitoring systems	Monetary: If physical damage, if not able to balance intermittent generation Physical Damage: out of sync on turbine, loss of lubricant on turbine, injection of DC if overloaded solar inverter; Reduction of operational life Loss of Confidentiality: Market estimates on generation forecast Loss of Integrity: spoofed turbine protection or inverter loads Loss of Availability: Power Outage - localized or if coordinated and networked wide spread; Loss of stability of grid operations if large enough generation; Force starting of other generation Reputation: if unable to balance to grid	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: RE Generation Subsystem: Generation % in Subsystem: 1-20% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Digital Flows**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
 Generator Step Up Transformer	Transforms power from the generator (operating in the range of 20 to 35 kV) to the transmission network voltage (69 kV to 765 kV).	Passive device from a power control perspective. Cooling system controls • Fans and circulating pumps Protection systems • Temperature rise • Sudden pressure detection • Differential current relay Monitoring systems • Historical operating temperatures • Oil gas analysis • Partial discharge monitoring	Downstream: Turbine protection control Upstream: Up load automatic generation control signals	Utility Upstream: • SCADA / EMS • Power plant supervisory control system Transformer systems Downstream: • Fan and pump motor starters and/or variable speed drives • Circuit breaker tripping for abnormal operating conditions (temperature, pressure, internal electrical faults)	Monetary: Generation revenue loss, potential damage Physical Damage: windings and core material (thermal and mechanical) Loss of Confidentiality: market prices based on expected generation capability Loss of Integrity: protective sensors spoofed or overridden Loss of Availability: Disabling the protective sensors (pressure and temperature rise) Disabling the cooling system (fans and pumps); Isolation the generator from the grid Reputation: if major generation not available	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Step Up Transformer Subsystem: Generation % in Subsystem: 99% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

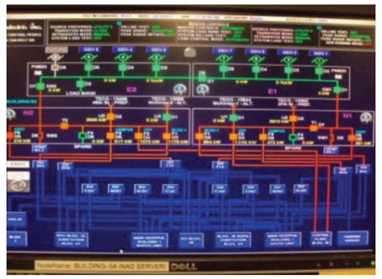
Transmission

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purpose**	**Status & Control**	**Digital Flows**	**Load/Utility Power Flow**	**Consequence**	**Environmental Factors**
Transmission Networks  	The transmission network consists of a number of transmission line circuits that connect generation stations to distribution substations. The mesh network serves as a bulk power delivery system to cities, rural areas, and industrial complexes. The primary components of the transmission network are the transmission lines and substations. Transmission lines are passive devices with practically no control points. Historically, any instrumentation of the transmission lines was associated at the substations. Common transmission network voltages: 138kV, 230kV, 345kV, 500kV and 765kV	The transmission lines are passive devices for transporting power. Instrumentation: • Conductor sagging monitors • Conductor temperature monitors • Weather condition monitoring • Current / Power flows Line fault protection system: • Short-circuit fault protection • Out-of-step / power swing detection and blocking / tripping	Electro-Mechanical: Instrumentation transformers (CTs & PTs) and thermal / mechanical transducers; Control signals to switches most non-digital Digital: • IED, PLC, RTU monitoring devices and systems with HMI • SCADA data input channels • Protective relaying inputs	Transmission from large generation Transmission to distribution centers Transmission to central power grid Transmission to major load industrial centers	Monetary: if physical damage or loss of efficiency (i.e. wrong line rating) Physical Damage: Failure of the conductors; Damaged insulators Reduction of operational life; Sagging conductors beyond elasticity point Loss of Confidentiality: Market estimate of transmission capacity Loss of Integrity: If spoofed line ratings Loss of Availability: Power Outage - localized or if coordinated and networked wide spread; Transfer of power flow to other transmission circuits; Increasing the susceptibility to cascading power outage Reputation: inefficient transmission	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Transmission Lines Subsystem: Transmission % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

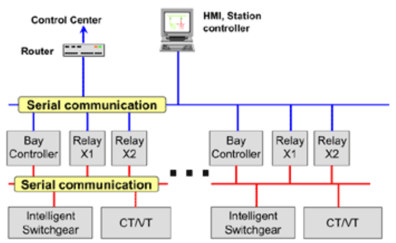
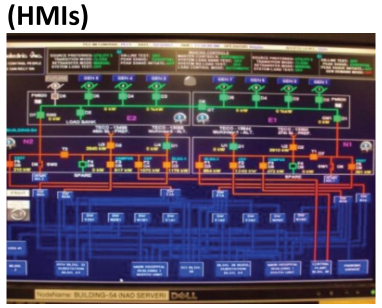
Applications on Control Centers and Specialized Equipment

Electric Grid Component / Subsystem	Purposes	Status & Controls	Environmental Vectors Up/Down Stream Digital	Load/Utility Power Flows	Consequences	Environmental Factors
Supervisory Control and Data Acquisition (SCADA) Systems 	Collection of remote status and control from multiple locations normally report. The SCADA system has a situational status display, historian of statuses and operator actions, normally geolocation specifics of the remote components and serves as the overall operations of the complex systems upon systems operations very common in electric grid systems. SCADA systems obtains information from other digital control systems, PLCs, IEDs, RTUs, digital relays and other sources, resolves that data to the system's status, acts upon urgent needs for the health and ongoing operations (must times automatically), allows for operator control of the systems, sends control commands to remote systems, records actions, enables a human in the loop operations, uses status for predictive forecast allowing for more efficient control.	Status received by many digital control systems, other data sources and other SCADAs which are displayed on large one-line or other visual board for operations with many other sub displays to aid the operators including alarms and alerts. Control: Automatic Generation Control for generators, fault isolation, switching and breaker operations, operational set points for subsystems; status feed into the state estimators, contingency analysis systems, load balance calculations and energy markets which controls energy market decisions. Supervisory control for maintenance (i.e. taking asset offline for maintenance) or restoration.	SCADA systems generally have the heaviest digital communications for the electric grid since this serves as the main control center for operations. Inter-Control Center Communications Protocol (ICCP) is commonly used between reliability coordinators and other load balancing entities operating the electric grid. There are fewer than 30 registered reliability coordinators in the United States, but over 1000 other entities[2]. DNP is the most common protocol in the electric grid for control of components. The communications mechanisms range from serial to full internet protocol enabled to short range wireless.	SCADA control and provides operational status for the Bulk Electric System	Monetary: SCADA data feeds connect to energy markets providing potential for large monetary impacts; Large potential impact if networked nature of SCADA used for wide impact. Physical Damage: Attacks on specific operations will cause physical damage (i.e. out of sync generation) Loss of Confidentiality: Markets, generation, load centers use and estimate of transmission capacity Loss of Integrity: State estimation, contingency analysis, reliability systems require integrity of data Loss of Availability: Power Outage potential if degraded system is unnoticed by operations with potential for wide spread; Reputation: Public loss of confidence in grid operations	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: SCADA Subsystem: All in Bulk Electric Grid % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

[2] http://www.nerc.com/pa/comp/Registration%20and%20Certification%20DL/NERC_Compliance_Registry_Matrix_Summary20141126.pdf

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Distributed Control Systems (DCSs) 	Used for more localized control of one or more tightly coupled systems. Common functions in a DCS include: 1) Human machine interface (HMI) for the operator human in the loop operations, 2) Historian for recording, 3) input and output to actuators, switches relays for actions, 4) data communication networks to and from the control and status components, 5) engineering workstations and/or non-production systems for design, development, updating and maintenance of the computer programs , 6) programs specific to the data for operational set points, alarm indicators, automatic actions for time sensitive critical operations; which may be layers upon layers of programs functioning on different platforms (i.e. RTU and control system).	Status received by other data sources and other DCSs which are displayed on large one-line or other visual board for operations with many other sub displays to aid the operators including alarms and alerts. Control: Automatic Generation Control for generators, fault isolation, switching and breaker operations, operational set points for subsystems; status feed into the localized state estimators, contingency analysis systems, load balance calculations and sometimes energy markets. Supervisory control for maintenance (i.e. taking asset offline for maintenance) or restoration.	Up to larger control centers, or SCADA systems will include common protocols on traditional networks (packet switched telephone modems, virtualized private networks isolated on the internet, private networks, cellular). Most networks will be IP (TCP/IP based and may tunnel in more electric grid specific protocols (ICCP, DNP, Modbus) Inside the local area network for the control system connecting the HMI, historian, energy management systems, engineering workstations together may be a typical TCP/IP network but use more UDP or stateless communications for low latency protocols such as (DNP, Modbus, FieldBus). Down to the control devices, other embedded microcontrollers (PLC, IED, RTU) may be TCP/IP based but more commonly serial or low latency communications.	Load side will have connection to switches/breakers, connect and disconnect capabilities, distributed generations Utility side may have higher connections to large generations, transmission resources other DCS, control centers and SCADA that may control parts of the Bulk Electric System.	Monetary: DCS data feeds connect to larger SCADA systems commonly and may feed into energy markets providing potential for large monetary impacts; Large potential impact if networked nature used for wide impact. Physical Damage: Attacks on specific operations will cause physical damage (i.e. out of sync generation) Loss of Confidentiality: Generation, load centers use and estimate of transmission capacity Loss of Integrity: Situational awareness, efficient operations, reliability systems require integrity of data Loss of Availability: Power Outage potential if degraded system is unnoticed by operations with localized impact and potential for wide spread; Reputation: Public loss of confidence in grid operations	**CDP** Collateral Damage Potential N | L | LM | MH | **H** | ND **TD** Target Distribution Component: DCS Subsystem: All % in Subsystem: 100% N | L | M | **H** | ND **CR** System Confidentiality Requirement L | **M** | H | ND **IR** System Integrity Requirement L | M | **H** | ND **AR** System Availability Requirement L | M | **H** | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Substations 	Manage frequency and voltage, isolate components for maintenance or restoration efforts. Substations are typically fenced in spaces remotely controlled and monitored via a control center or SCADA system. Large substations are commonly owned by more than one entity (i.e. distribution owner/operator and transmission owner). Specialized substations may be for moving power from a generation source onto the transmission grid, to a distribution substation or to reduce the voltage of the transmission source to a lower voltage used by load centers such as industry or residential.	Status from substations provide the situational awareness for almost all parts of the electric grid. Control of substations provides for efficient operations, to isolation for maintenance activities, fault isolation and restoration.	Upstream communications with substation control centers is from either local or remote DCS, SCADA (PLC, IED,RTU) or smart field devices with embedded microprocessors depended on the size the type of substations. Data from RTUs is sent to substation control centers and personnel or automation systems at the center monitor the data from the RTUs and send control commands back to the RTU's if needed. Internal to the substation the low latency protocols are common (DNP, Modbus, Fieldbus), fiber media or twisted pair with considerations for electromagnetic interference. Downstream communications requires the fastest processing and singles are needed for the safety systems to protect expensive electric components (ref. IEC-61850).	Load side includes connects and disconnects to load centers, localized generation, step down transformers Utility side includes connections to step up transformers, connect and disconnect to transmission or larger distribution assets for fault isolation or maintenance	Monetary: Substation data feeds connect to DCS, SCADA and most all aspects of the electric grid, potential for large monetary impacts if physical damage, localized outages with potential wider impact if networked or coordinated attack Physical Damage: Attacks on specific operations will cause physical damage (i.e. improper fault isolation) Loss of Confidentiality: Very state and temporal data may be used for gaining on energy markets, generation, load centers use and estimate of transmission capacity Loss of Integrity: will result in improper operations, reliability issues Loss of Availability: Power Outage potential if degraded system is unnoticed by operations with potential for wider spread; Reputation: Public loss of confidence in grid operations	**CDP** Collateral Damage Potential N | L | LM | **MH** | H | ND **TD** Target Distribution Component: Substation Subsystem: All % in Subsystem: 100% N | L | M | **H** | ND **CR** System Confidentiality Requirement L | **M** | H | ND **IR** System Integrity Requirement L | M | **H** | ND **AR** System Availability Requirement L | M | **H** | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Substation Automation Applications  	The following are applications that can be used on specialized equipment or programed on more generic equipment such as PLC, IED, and RTUs: • Digital Fault Recorder • Transient Recorder • SCADA Data Collection • Tap changer control • Capacitor Back Controls • Motorized Switch Gear Controls • Transfer Monitor • Health Systems Circuit Breakers • Lightning Counter Digital logic and signal processing systems for autonomous or aided control of substation equipment, apparatus and data acquisition systems				Refer to the Electric Grid Component or Subsystem which uses this component	
Human Machine Interfaces (HMIs) 	HMIs are computers running a software packages used as an interface between the operator and the Industrial Control Systems (SCADA systems, PLCs, DCSs, RTUs, etc.) controlling one or more process or system. HMIs perform the following tasks: • System visualization, • Operator control of the system, • Alarm display and acknowledgement, • System value and alarm archiving, and • Machine parameter management HMIs are is used in nearly all industries with Industrial Control Systems, including power, water and wastewater, oil and gas, and chemical.				Refer to the Electric Grid Component or Subsystem which uses the affected HMI for consequences of loss of HMI view or control for that Component or Subsystem for additional consequences Successful exploitation of an HMI vulnerability could allow an attacker to log on to a vulnerable HMI as a user or administrator, where they would be able to perform any of the system tasks configured for that HMI. The attacker might also be able to execute arbitrary code or obtain full access to files on the HMI system.	

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Substation Automation Devices: IED, RTU microprocessor relays and PLCs Intelligent Electronic Devices (IED) is a microcontroller that can be programmed as SCADA, alarm processing, volt/var control, circuit breaker operations, change tap settings, equipment failure indications, event recorders and other substation automation applications. 	Digital logic and signal processing systems for autonomous or aided control of substation equipment, apparatus and data acquisition systems • Collect inputs (analog/digital) for control algorithms of physical assets • Control reclosing and reconfiguration operations during and after a fault condition • Monitor power levels and the quality of power, system voltages, thermal conditions, switch positions • Manage the sequence of operations for complex switching arrangements				Refer to the Electric Grid Component or Subsystem which uses this component	
Remote Terminal Units (RTU) manage digital and analog inputs/outputs converting these signals to proper units for display at a master control systems or SCADA. Similar to an IED normally in more remote locations and wireless connectivity. 	Digital logic and signal processing systems for autonomous or aided control of substation equipment, apparatus and data acquisition systems • Collect inputs (analog/digital) for control algorithms of physical assets • Control reclosing and reconfiguration operations during and after a fault condition • Monitor power levels and the quality of power, system voltages, thermal conditions, switch positions • Manage the sequence of operations for complex switching arrangements				Refer to the Electric Grid Component or Subsystem which uses this component	

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Programmable logic controllers generally have more computing power than IEDs or RTUs but these distinctions are getting less with newer microprocessor capabilities. Normally communicate using copper conductors but many newer PLCs support wireless communications.. 	Digital logic and signal processing systems for autonomous or aided control of substation equipment, apparatus and data acquisition systems • Collect inputs (analog/digital) for control algorithms of physical assets • Control reclosing and reconfiguration operations during and after a fault condition • Monitor power levels and the quality of power, system voltages, thermal conditions, switch positions • Manage the sequence of operations for complex switching arrangements				Refer to the Electric Grid Component or Subsystem which uses this component	
 **Relays** - Convert voltage and currents to digital form and process with microprocessor communication back to SCADA, monitors contact inputs, metering waveform  Amount of current reduced to reset relay (open circuit breaker) - differential	Trips circuit breaker when a fault is detected Functions: • over current opens circuit breaker when load current exceeds value; • distance/impedance calculates impedance per km; • current differential protection used on transmission lines difference on each line amps; • direction relay determines direction of fault; • synchronism check relay provides contact closure when frequency and phase within tolerances- sync generator to transmission	Digital – obtain CT Old electromechanical still exist Safety related one few thousandths of a second response times	Some relays are manual less than half overall but more manual in transmission (over 60%) with most new purchases being digital relays[3] Almost all digital are non-IP based control, may have IP connectivity for programming and maintenance but not operations. DNP common	Status Input: CT, PT, VT, IED, RTU, PLC, Meters, DCS, SCADA Status output: IED, RTU, PLC, Meters, DCS, SCADA Control: IED, RTU, PLC, DCS, SCADA	Monetary: Safety and physical damage costs and potential outage isolated Physical Damage: over current protection loss; loss of synchronization of generation to grid Loss of Confidentiality: Minimal due to transient state; data exfiltration for targeted physical impact Loss of Integrity: Large impact and safety of systems Loss of Availability: Large impact some of the fastest controls needed. Reputation: poor safety	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Transmission Subsystem: Relays % in Subsystem: 50% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

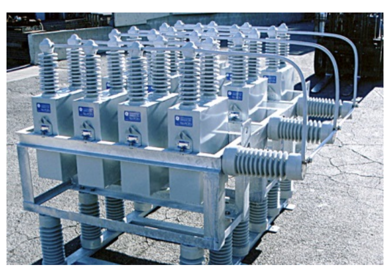
[3] http://www.newton-evans.com/wp-content/uploads/Relay-2012-brochure.pdf

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Circuit Breaker Controls 	Monitor power levels and the quality of power, system voltages, thermal conditions, switch positions Manage the sequence of operations for complex switching arrangements. Detect a fault condition and interrupt current flow Automated and manual breaker operations are also used to isolate grid segments for for maintenance	Status of actuator, terminals overcurrent, arc detection, CT, and PT Control: Actuator control, contacts, terminals, overcurrent solenoid and arc divider/extinguisher, may be configured as an automatic transfer switch or recloser	Upstream: DNP3, Modbus, IEC 61850-8-1, serial for modem, copper/fiber Downstream: UDP stateless, command signal	Upstream: RTU, IED, Protective Relay Downstream: sectionalizer and buses	Monetary: Outage costs; dispatch linemen crew to troubleshoot failed breaker operation Physical Damage: safety Loss of Confidentiality: state based data limited value unless large transmission breaker/outage information for energy markets Loss of Integrity: if reclose signal spoofed indication of breaker setting resulting in localized outage or safety issue Loss of Availability: Indication of bad breaker setting less likely due to other sensing and protection mechanisms Reputation: outage recover times or safety incident	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: All Subsystem: Breaker % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

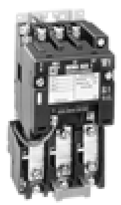
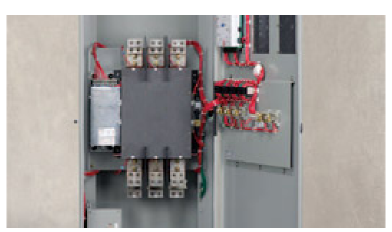
			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Transformer  Phase-Shifting Transformer 	Transformers are devices using mutual induction to change the voltage and current of a circuit Step up transformers to take generation to transmission Step down transformers to take transmission into distribution or distribution into a load center or residence Special purpose transformer that introduces a controlled shift in the phasor voltage angle between the primary and secondary terminals. The phase angle shift influences the direction and amount of power flowing through the transformer and connected transmission lines. Load center specific transformers for industrial applications (i.e. furnace operations) rectifiers.	Status of transformer efficiency and operations along with preventive maintenance needs (i.e. oil) Control with breakers and switching for safety and reliability of grid, may be part of islanding applications. Active tap changer that controls the amount of phase angle shift added to the voltage. Tap changer is controlled by the EMS to regulate the flow of power through the transformer.	Substations controls DCS, to SCADA systems all aspects of electric grid Preventive maintenance, operational logs may also be digital and connected with networks or local modules at transformer. Smaller distribution transformers have almost no digital components	Ubiquitous applications from smallest resident to large load centers, major generation and transmission	Monetary: potential for large monetary impacts if physical damage due to tailored engineering and long lead times for replacement; localized outages with potential wider impact if networked or coordinated attack Physical Damage: Attacks on specific operations will cause physical damage (i.e. improper fault isolation) Loss of Confidentiality: Very state and temporal data may be used for gaining on energy markets, generation, load centers use and estimate of transmission capacity Loss of Integrity: will result in improper operations, reliability issues Loss of Availability: Power Outage potential if degraded system is unnoticed by operations with potential for wider spread; Reputation: Public loss of confidence in grid operations	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Transformer Subsystem: All % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Sequence of Event Recorders Steady state recorder/Power quality recorder Continuous recorded (waveform/ RMS) 	Collect inputs (analog/digital) for control algorithms of physical assets	Digital Event Recorders are status only but are commonly coupled in a RTU with other control function	Up/Downstream: DNP3,Modbus, IEC 61850-8-1, RS232c serial for modem copper/fiber most typical integrated web based graphical interface common	Upstream: PLC, RTU, control system or SCADA Downstream: breakers, protection relays, PMU digital instrument transformer,	Monetary: if fined for no logging data Physical Damage: unlikely Loss of Confidentiality: state based potential for energy market advantage Loss of Integrity: if spoofed for erasing attackers actions; Spoofed situation awareness, state estimation feeds resulting in bad operator actions Loss of Availability: maybe all erased for difficult forensics Reputation: lack of control for data	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: All Subsystem: Event Recorders % in Subsystem: 80% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND
Digital Fault Identification Recloser 	Control reclosing and reconfiguration operations during and after a fault condition	Based on input sensing or commends from upstream control system or SCADA, circuit breakers and fuses are manipulated. Auto reclosers are typically responds to momentary faults on a system. The control function will detect a fault, open the connection and attempt to reclose 2 to 3 times. If the fault persists the reclosing function will keep the system de energized requiring a human intervention to reset (may be remote command to reclose)	Up/Downstream: DNP3,Modbus, IEC 61850-8-1, RS232c serial for modem copper/fiber most typical integrated web based graphical interface common	Upstream: PLC, RTU, control system or SCADA Downstream: breakers, protection relays, digital instrument transformer,	Monetary: Outage costs; dispatch linemen crew to clear faults Physical Damage: minimal Loss of Confidentiality: state based data limited value unless large transmission fault information for energy markets Loss of Integrity: if reclose signal spoofed indication of fault when none exists resulting in localized outage Loss of Availability: Indication of clear fault less likely due to other sensing and protection mechanisms Reputation: outage recover times	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Transmission, distribution Subsystem: Fault Recloser % in Subsystem: 30% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

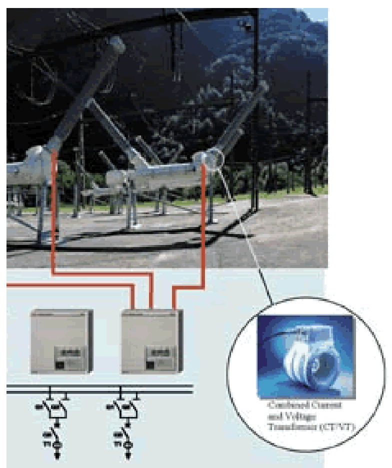
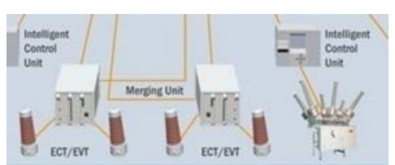
			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Transient Recorder 	Transient disturbance recorder normally with power quality measur4ments. Sometimes in a hardware software configuration or in only software using other measurements.	Status only Control on uploading data to another system such as an engineering workstation or simulation application for analalysis	EN50160 PQ standard Voltage, current, RMS, frequency, real and reactive power, power factor, current and voltage harmonics, voltage sages, and swells, voltage flicker – 32 analog and 64 binary channels common	Transient recorder information is stored local and uploaded for analysis or may be connected for periodic uploads, but not normally in series with other power equipment, instead hanging off of on group of assets to record behaviors.	Monetary: if fined for no logging data Physical Damage: unlikely unless tied to control scheme Loss of Confidentiality: state based potential for energy market advantage Loss of Integrity: if spoofed for erasing attackers actions; Spoofed situation awareness, if feeds state estimation may result in bad operator actions Loss of Availability: maybe all erased for difficult forensics Reputation: lack of control for data	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Transmission Subsystem: Event Recorders % in Subsystem: 75% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

Electric Grid Component / Subsystem	Purposes	Status & Controls	Environmental Vectors Up/Down Stream Digital	Load/Utility Power Flows	Consequences	Environmental Factors
Capacitor Bank Controllers   	Power Factor Correction and Voltage Supporting Capacitor Banks Provide voltage support by producing leading reactive power. Counteract inductive loading (motors or transmission lines) to make load appear to be mostly resistive. Large customers may have switched capacitor banks to provide power factor improvements, maintain voltage profile within specifications, and minimize the amount of reactive power consumption from the utility. Also used for reactive power compensation for transmission systems between shunt and transmission line and ground in in series to provide leading reactance to improve the total reactance. Shunt capacitor banks normally configured with switches relays and protections.[4] Can be used in static var compensation for improved power system transmission and distribution performance (with reactors, thyristor valves and control systems).[5]	Voltage, VARs, Current, Temperature and time control configurations – local or remote control for trip close switched capacitors, time delays for trip/close and reclose operations, overvoltage and overcurrent protections, 3-phase metering remote programming, downloading data logs and firmware updates, unsolicited reporting of state change filed alarms threshold violations neutral current sensing to report imbalance of blown fuses	Not all capacitor bank controls are digital, some have electro-mechanical switches, breakers and tap controls. Utility distribution substations and distribution feeder applications. • Voltage relay control • Remote control from EMS Industrial and commercial applications • Reactive power relay control • Voltage relay control • Timer control Upstream: Ethernet or serial, master station connections, Downstream: DNP common	Upstream: master stations RTU, IED, PLC, feeder circuit Downstream: Volt/VAR control applications, distribution management system or SCADA Poor power factor loads Voltage profile outside of utility specification. Damage to loads. Voltage spikes generated by repeated switching operations, Damage to loads and utility equipment. Harmonic signal amplification. Thermal damage to transformers.	Physical damage - Breakdown voltage: Explosive break down voltage when plates short; capacitance instability: degradation of the dielectric aging factors; Current and Voltage reversal: change polarity in a circuit for larger system Physical Damage: Fused capacitor elements can cause localized faults and outages – assuming percentage of digital capacitor control is similar to relaying if localized Monetary: potential if mis-operations causes outage to load center, or reduced capability on transmission network Loss of Confidentiality: state based Loss of Integrity: if spoofed for bad operational decisions or mis-operations Loss of Availability: fast as breaker switching operations, Degraded operations with poor power factors Reputation: lack of power control	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: All Subsystem: Capacitor Bank Controls % in Subsystem: 50% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

4 http://apps.geindustrial.com/publibrary/checkout/Shunt%20Capacitor?TNR=White%20Papers|Shunt%20Capacitor|generic
5 http://www02.abb.com/global/gad/gad02181.nsf/0/3074a73e6d914bb3c1257a620031034c/$file/Static+Var+Compensator+%28SVC%29+-+An+insurance+for+improved+grid+system+stability+and+reliability.pdf

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Motorized Switch Gear Controllers 	Many applications for motor control for feeders, starters, variable frequency drives (VFD)	Phase protection, imbalance protection, ground fault protection relay trip, trip indication, overload relays thermal capacity, RMS current, relay settings, line frequency, voltage present indicator, automatic insulation tester, incoming feeder terminations, owner metering with PT/CT, attenuation of harmonics, integral harmonic correction, motor control center, harmonic correction, THD, total demand distortion TDD, reactive current compensation,	Downstream: Upstream Modbus, TCP Ethernet IP fieldbus, web enabled communications,	Downstream: Circuit breakers, overcurrent devices, Fusible switches	Monetary: Outage costs; load center impacts Physical Damage: out of synchronization operations may cause damage and safety - localized Loss of Confidentiality: state based data limited value unless knowledge of load center Loss of Integrity: if reclose signal spoofed indication of breaker setting resulting in localized outage or safety issue Loss of Availability: Indication of bad breaker setting less likely due to other sensing and protection mechanisms Reputation: outage recover times or safety incident	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Transmission, distribution, generation Subsystem: motorized switch gear % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND
Automatic Transfer Switches 	Open, delay and close, and bypass switch allowing for isolation of circuitry. Operates momentarily energized solenoid operating mechanisms for transfer - can be programmed in a PLC, RTU or IED or in an automatic transfer switch – can be configured with a bypass transfer switch Used for load center islanding applications	Voltage and frequency sensing, time delays, ability to lock out automatic operations, overcurrent trips, over/under frequency set points, over/under voltage set points, voltage unbalance set points load shedding, load back control, data logging, alarms,	Upstream: DNP or fast communications master ATS or controller Downstream: DNP or fast communications to load shed or load bank control	Upstream: master ATS or Controller, Downstream: load shedding, load bank control	Monetary: Outage costs; load center impacts Physical Damage: out of synchronization operations may cause damage and safety - localized Loss of Confidentiality: state based data limited value unless knowledge of load center Loss of Integrity: if reclose signal spoofed indication of breaker setting resulting in localized outage or safety issue Loss of Availability: Indication of bad breaker setting less likely due to other sensing and protection mechanisms Reputation: outage recover times or safety incident	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Distribution, generation Subsystem: motorized switch gear % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Phasor Measurement Units (PMUs) 	Mainly status and feed into the larger state estimators that manage the load/generation balance for a system. Since data from PMUs used in state estimators can have impact on operations. Few used in distribution configurations. Limited emerging use in distribution systems for critical load centers – some relays embed PMUs capability as default but not used or enabled	Status: Data fed into state estimators or stand-alone situational awareness applications not integrated into operations but used as another tool for operator decisions	IEC 61850-9-2 IEEE C37.118 16 points per cycle waveform 1 point per cycle sampling (magnitude, phase, RMS-root mean squared of AC waveform, frequency positive and negative sequence, imbalance THD-total harmonic distortion, apparent, active and reactive power Traveling wave fault location)	Upstream: Phasor Data Concentrators, situational awareness Downstream: relays, switches, breakers – if PMU data used for local control and protection logic	Monetary: PMUs commonly used for large energy market trading Physical Damage: if coupled to relay bad switching or open/close Loss of Confidentiality: PMUs commonly used for large energy market trading – may be used to game the market Loss of Integrity: Spoofed situation awareness, state estimation feeds resulting in bad operator actions Loss of Availability: PMU data out of time synchronization due to spoofed GPS resulting in bad data for situational awareness Reputation: Bad Data	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Transmission Subsystem: Phasor Measurement Units % in Subsystem: 50% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND
Phasor Data Concentrators 	Collects PMU data for wide area measurement systems for situational awareness. Limited emerging use in distribution systems for critical load centers	Gathers input from many PMUs (~40+),	IEEE C37.118, LDAP, 1 to 240 messages per second,	Upstream: Situational awareness applications i.e. state estimators, contingency analysis systems, automatic generation control, transmission resource availability Downstream: PMUs	Monetary: PMUs commonly used for large energy market trading – data concentrators more common Physical Damage: Unlikely relay schemes would go through a data concentrator prior to acting on a local control Loss of Confidentiality: PMUs /concentrators commonly used for large energy market trading – may be used to game the market Loss of Integrity: Spoofed situation awareness, state estimation feeds resulting in bad operator actions Loss of Availability: PMU data out of time synchronization due to spoofed GPS resulting in bad data for situational awareness Reputation: Bad Data	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Transmission Subsystem: Phasor Data Concentrators % in Subsystem: 20% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Instrumentation Transducers    	Monitor high voltage system parameters safely for metering, protection systems, and controls. • Current transformers (CT) • Voltage or potential Transformers (PT). electromagnetic and capacitive coupled technologies • Analog output to IED • Digital inputs to IED…	Generally passive devices that replicate electrical current and voltage quantities at safer lower power and potential quantities.	Instrumentation transducers convert the analog output (i.e. ac current to dc voltage) switch gears, power system control equipment common in data acquisition is digital downstream CT, PT, VT are electro-mechanical meaning there is not digital signal , only a copper wire that signals to a instrumentation transducer, meter, oscilloscope or other devices to be calculated with current ratio to get operating status	Used for relays, circuit breakers, transformers, metering – ubiquitous applications used for signaling in electro-mechanical operations or digitized	Impact can only be once the CT,PT,VT signals are sent to a digital device such as a meter then localized Monetary: negligible Physical Damage: negligible localized impact to digital equipment connect to transducer signal, but if spoofed may result in physical damage of equipment operating based on CT/PT sensing Loss of Confidentiality: state based temporal Loss of Integrity: accuracy needed to understand status of the system Loss of Availability: feeds into the status of the larger system Reputation: negligible	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: All Subsystem: Instrumentation Transducers % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

Distribution

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Distribution Network 	The distribution network consists of a number of feeder circuits that connect the bulk transmission system to end-users/customers. The radial network serves as a distribution power delivery system to homes, business, and small industry. The primary components of the distribution network are the feeder lines coming out of the distribution substations and the step-down pole-top and pad-mount transformers. Most distribution lines are passive devices with some control points such as reclosers, sectionalizers, switched capacitor banks, and voltage regulators. Distribution is the focus from most newer applications such as demand response, microgrids, fault isolation, reclosing, islanding, distributed generation, outage management, customer information, pricing signals, net metering – which is changing distribution to be less passive and more digital control with data from the end load user. Common distribution network voltages: 4.8kV, 12.47kV, 13.8kV, 24.5kV and 34.5kV Many applications from municipality to rural	The distribution lines are mainly passive devices for delivering power locally. Emerging applications for reclosing and fault isolation and outage management systems provide more connectivity. Instrumentation: • Voltage magnitude monitors • Power flow monitors and meters Line fault protection system: • Short-circuit fault protection Status: of distribution network, outage management systems, dispatch control centers, load balance applications, potential for connectivity into energy markets, demand response applications, time of use and islanding. Control: connect and disconnect of load areas, isolation of faults, load shedding	Up: DCS, substation controls, SCADA systems that function as Dispatch center, outage management systems, meter data management system, customer information system, energy market Down: many communications paths to 'last mile' to residence or load center for connect, disconnect, islanding, time of use, market signal transactive data, distributed generation, net metering.	Load side: major load center, industrial complexes, residential areas Utility side: Dispatch centers, DCS, SCADA, Substation controls; generation and transmission	Monetary: Outage costs; dispatch linemen crew to troubleshoot failed isolation, safety issue potential; outage can range from residential area to large load center Physical Damage: safety and impact to load center and residences Loss of Confidentiality: state based data limited value unless large distribution network or critical load center; if connected to customer information systems (i.e. meter data management systems) potential for customer privacy concerns Loss of Integrity: if reclose signal spoofed indication of breaker setting resulting in localized outage or safety issue Loss of Availability: Indication spoofing less likely due to other sensing and protection mechanisms Reputation: outage recover times or safety incident	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Distribution Subsystem: Distribution Network % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

<table>
<tr><th></th><th></th><th></th><th>Environmental Vectors</th><th></th><th></th><th></th></tr>
<tr><th>Electric Grid Component / Subsystem</th><th>Purposes</th><th>Status & Controls</th><th>Up/Down Stream
Digital</th><th>Load/Utility
Power Flows</th><th>Consequences</th><th>Environmental Factors</th></tr>
<tr>
<td>Line Sectionalizers and Reclosers
</td>
<td>Distribution network switching devices:
• Opens circuits and clears faults on distribution lines
• Recloses (reconnects) circuits after a momentary fault is cleared
• Closes circuits and reconfigure the distribution grid after a fault to minimize areas of power outages.
Commonly found in Distribution Substations and downstream protective devices can count faults from the recloser normally programmed number of attempts to reconnect</td>
<td>Fault protection functions
• Overcurrent protective relay
• Timers to reclose the circuit
Sectionalizer functions
• Fault current counting relay
• Circuit isolation
• Circuit reconnection
Communications
Radio or fiber optic based communications for control setting and data collects.</td>
<td>Most sectionalizers and reclosers are electro mechanical with connection to copper line and signals to relays, breakers that may be digital

Emerging digital control for sectionalizers and reclosers exisits. Digital controls for automated sectionalizers work in 200 milliseconds programmable and connected via different media including wireless[6]</td>
<td>Utility: DCS, SCADA distribution management systems, dispatch control center

Load center or distribution network to switches breakers for isolation or reclosing

• Poor operations. Poor reconfiguration or lack of reconfiguration after a fault. Customers in serviceable areas remain without power.
• Loss of customer loads. Switching operations during normal operation can cause the loss of service to customers.</td>
<td>Monetary: Outage costs; dispatch linemen crew to troubleshoot failed isolation, safety issue potential

Physical Damage: safety and impact to load center

Loss of Confidentiality: state based data limited value unless large distribution network or critical load center

Loss of Integrity: if reclose signal spoofed indication of breaker setting resulting in localized outage or safety issue

Loss of Availability: Indication spoofing less likely due to other sensing and protection mechanisms

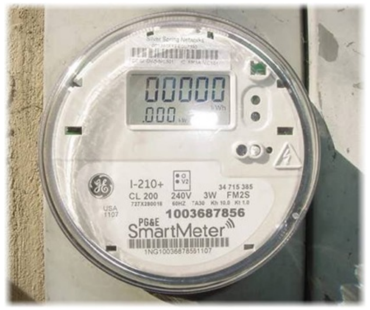
Reputation: outage recover times or safety incident</td>
<td><table>
<tr><td>CDP</td><td colspan="6">Collateral Damage Potential</td></tr>
<tr><td></td><td>N</td><td>L</td><td>LM</td><td>MH</td><td>H</td><td>ND</td></tr>
<tr><td>TD</td><td colspan="6">Target Distribution</td></tr>
<tr><td></td><td colspan="6">Component: All</td></tr>
<tr><td></td><td colspan="6">Subsystem: Breaker</td></tr>
<tr><td></td><td colspan="6">% in Subsystem: 100%</td></tr>
<tr><td></td><td>N</td><td>L</td><td>M</td><td>H</td><td>ND</td><td></td></tr>
<tr><td>CR</td><td colspan="6">System Confidentiality Requirement</td></tr>
<tr><td></td><td>L</td><td>M</td><td>H</td><td>ND</td><td></td><td></td></tr>
<tr><td>IR</td><td colspan="6">System Integrity Requirement</td></tr>
<tr><td></td><td>L</td><td>M</td><td>H</td><td>ND</td><td></td><td></td></tr>
<tr><td>AR</td><td colspan="6">System Availability Requirement</td></tr>
<tr><td></td><td>L</td><td>M</td><td>H</td><td>ND</td><td></td><td></td></tr>
</table></td>
</tr>
</table>

[6] http://www.celsa.com.co/index.php/en/proteccion-y-maniobra-en/mnuelectronicos-en/seccionalizadorelectronicodigital-en

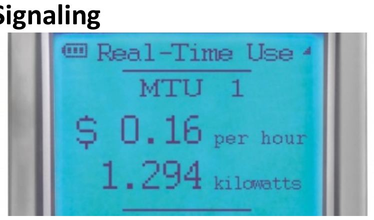
			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Circuit Breakers 	Switching devices that Interrupt fault currents, short circuit conditions, or overload currents while maintaining unaffected circuits and isolation of damaged circuits from power sources. Types: Oil; air puff compressed air; SF6; and vacuum	Instrumentation • Switch status (open/closed) Maintenance monitoring • Number of operations • Interrupted current levels • Stuck mechanical linkage detection • Quality or level of dielectric Controls • Open/close contacts (trip/reclose)	Open close status and commands, circuit breaker health monitoring Upstream: DNP3, Modbus, IEC 61850-8-1, serial for modem, copper/fiber Downstream: UDP stateless, command signal	Utility: Protective relays, SCADA control output channels, Substation automation PLCs, DCS, control centers, vendor access Load downstream: Switch gear monitoring equipment, Maintenance systems	Monetary: Outage costs; dispatch linemen crew to troubleshoot failed breaker operation – unless fault isolation and reclosing Physical Damage: safety Loss of Confidentiality: state based data limited value unless large critical load center Loss of Integrity: if reclose signal spoofed indication of breaker setting resulting in localized outage or safety issue Loss of Availability: Indication of bad breaker setting less likely due to other sensing and protection mechanisms Reputation: outage recover times or safety incident	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: All Subsystem: Breaker % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

Electric Grid Component / Subsystem	Purposes	Status & Controls	Environmental Vectors Up/Down Stream Digital	Load/Utility Power Flows	Consequences	Environmental Factors
Industrial and Commercial Load Curtailment Signaling 	Similar to load control for residential customers. Data link is often connected directly into the facilities energy management computer. Factories generally are given a command to curtail a specific amount of power. The facility operators have the flexibility to shut off different loads to minimize the impact on production.	Commands can come from the utility EMS directly for large power customers. More common on high priced energy markets or where there is a specific constraint in transmission or generation.	Time of pricing and curtailment signals range from day ahead to every 5 minutes depending on utility's programs. These applications are commonly web based, may be as simple as text message (SMS) type of notification. Connections into the load center/industrial switch gear are command and interface agreements are negotiated. Communications ranges from fast to 24 hour dependent on these programs.	Load: Odd curtailment request to industrial customers, or more planned curtailment based on program to start or stop localized generation or reduce heavy load processes Utility: Connect and Disconnect load center/industrial complex to grid	Monetary: Damage of critical load center potential; inefficiencies in shaving peak load; inefficient energy pricing • Physical Damage: limited to location but may be a larger load center. Inability of the utility to manage significant load demand in heavy loading conditions. Loss of system stability due to inability to service loads. Loss of Confidentiality: Customer information sensitivity Loss of Integrity: Potential loss of operation for load center Loss of Availability: Potential longer load center outage if damage to local generation or damage load center processes Reputation: Large impact due to most visible to customer	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Residential Subsystem: Load Control % in Subsystem: 25% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

Residential

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Meters    	The next generation of AMI meter infrastructure provide data collections for the utility as well as customer management, such as remote connecting and disconnecting services and quality of service monitoring. Net meters allow local generation to be sent to the grid (i.e. solar panels).	Status of distribution systems for residence on amount of electricity used Control for connect or disconnect Advanced net metered functions allow for residence to be a power producer and for the meter to 'run backwards' if providing energy to the grid Most modern advanced meters have multiple capabilities for communications, low powered wireless meter to meter or meter to data collector, wireless for update of firmware is common. Even the older advanced meters (AMR) have low range wireless reading where the utility worker drives by a meter to collect usage information. Older meters without any communications capabilities still exist – these are inspected visually to record usage	Some meters are electro-mechanical In the US over 43 million smart meters are installed[7] 15 States have over 50% smart meters installed for their customers[8] overall over 1/3 of US households have smart meters[9] Downstream: smart grid appliances, other meters, and thermostats – Zigbee or Homeplug Upstream: meter data management systems, outage management system, billing systems – commonly short RF mesh network to data collector or head end with fiber or cellular to centralized server Most meter communications is low range wireless meshed or peer to peer (not IP) This communications go to data concentrators, head end or pole type devices where the data is collected and sent to the meter data management system, customer information system and/or billing applications	Load downstream: Connect and Disconnect, setting of smart appliances Utility upstream: status of metered data management systems, billing, outage management system	Monetary: Cost of sending out crews for connect, disconnect s and meter readings; efficiencies if automated demand response Physical Damage: limited to location Loss of Confidentiality: Customer information sensitivity Loss of Integrity: Bad meter/billing information Loss of Availability: Potential if more automated load shedding and demand response applications Reputation: Large impact due to most visible to customer	**CDP** Collateral Damage Potential N | **L** | LM | MH | H | ND **TD** Target Distribution Component: Residential Subsystem: Smart Meters % in Subsystem: 75% N | L | M | **H** | ND **CR** System Confidentiality Requirement L | **M** | H | ND **IR** System Integrity Requirement L | **M** | H | ND **AR** System Availability Requirement **L** | M | H | ND

7 http://www.eia.gov/tools/faqs/faq.cfm?id=108&t=3
8 http://blog.opower.com/2013/09/report-smart-meters-in-us-now-generating-more-than-1-billion-data-points-per-day/
9 http://www.greentechmedia.com/articles/read/one-third-of-u.s.-homes-have-a-smart-meter

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Residential Load Control 	Remote control contactor (switching device) that respond to utility command signals to disconnect curtailable loads such as water heater or air conditioning during heavy power demand periods.	Control and command signals sent over the power lines, telephone lines, or radio. Commands come from the local area control center's SCADA/EMS in response to peak loading conditions.	Downstream: smart grid Demand Response signals to UPS and generators Upstream: meter data management systems, outage management system, billing systems	Load: Connect and Disconnect of grid and distribution/transmission resources Utility Upstream: status of metered data management systems, billing, outage management system, load signals to load balancing application – state estimator or dispatch	Monetary: Damage of critical load center potential; inefficiencies in shaving peak load Physical Damage: limited to location but may be a larger load center Loss of Confidentiality: Customer information sensitivity Loss of Integrity: Potential loss of operation for load center Loss of Availability: Potential longer load center outage if damage to local generation or damage load center processes Reputation: Large impact due to most visible to customer	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Residential Subsystem: Load Control % in Subsystem: 25% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND
Residential Energy Cost Signaling 	A new smart-grid technology for communicating spot or instantaneous energy prices to customer's smart appliances and/or smart building.	Pricing information and appliance operating behaviors are communicated using Blue Tooth and Wifi technologies. A customer management system coupled to the EMS system communicates with the home devices.	Downstream: Retailer third party (i.e. NEST) Upstream: Status to user and retail power broker application	Load side may be automated controls of thermostats or smart appliances Utility load management system (EMS) or a building energy management system	Monetary: poor energy choices Physical Damage: None known Loss of Confidentiality: Customer data sensitivity Loss of Integrity: consumer choices need accurate data Loss of Availability: Time sensitive actions for better efficiencies Reputation: High due to customer interface	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Residential Subsystem: Energy Cost Signaling % in Subsystem: 5% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Power Inverters  Device or circuitry that changes direct current to alternating current	Power inverters are commonly used by the direct current source such as a photo voltaic array. Inverters have sinusoidal ac (single phase) with stable voltage and frequencies and harmonic components DC to AC	Status of DC to AC generation. If used for spinning reserve dump generation to protect distributed energy resources	Common use of wireless for PV and wired fiber for wind turbines then local communications after data collection wireless or wired	Upstream: spinning reserve Downstream: turbine damage DC feed into distribution	Monetary: Potential inject of DC into AC system if malfunction damaging load devices Physical Damage: Potential inject of DC into AC system if malfunction damaging load devices Loss of Confidentiality: Temporal state based Loss of Integrity: correct controls needed Loss of Availability: Fast controls needed Reputation: Customer interface potential with rooftop solar Cause RE imbalance in localized system with high percentage of renewable energy distribution if networked attack, inject DC back into distribution grid, damage to VFD, load equipment and ramp up base stabilizing generation	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Residential Subsystem: Power Inverters % in Subsystem: 5% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

Industrial and Commercial Loads

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Emergency Short Term Backup Power: Batteries for substations or large load centers 1.5MW 	Batteries used in substations and generator stations for black start, ancillary power, newer applications include better frequency regulation	Load and balance application status control for recharge discharge signals	Downstream: Recharge and discharge signals, battery health Upstream: distribution localized balance issues or substation resilience or load center process through capability	Battery health, Load center process continuation, substation backup power or distribution balance Utility side to connect or disconnect if in curtailment program	Monetary: If battery damaged, if loss of load center service potential interruption of processes resulting in loss of revenue Physical Damage: Over charged battery Loss of Confidentiality: Slight market gain potential; more concern about exfiltration of specifics for targeted localized attack Loss of Integrity: Potential spoofing for battery status Loss of Availability: Reputation: Over charged battery physical damage localized disruption	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Industrial and Commercial Loads Subsystem: Batteries % in Subsystem: 1% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Emergency Backup Power Generation  	Backup Generations is commonly used for continual operations of load centers if processes are critical requiring power (i.e. sensitive chemical processing) or needed for availability (data centers). Automatic transfer switches, breakers, relays and reclosers may be configured to operate and islanding off grid operations and restore back to grid power. Large utilities offer incentives to use backup generation during peak loads in demand response applications causing the backup generation to operate while the grid is available.	Status: Generation maintenance, operations, Control: generation synchronization to load center, automatic transfer switch , resynchronization to distribution grid Generator controls: over speed Local controls • Excitation control – DCS • Synchronization control – sync check relay • Speed control • Turbine governor control - DCS	DCS, PLC, RTU, IED some sort of embedded microcontroller is common to manage the health and operations of the backup generation. Older system may still be electo-mechanical or in some cases manually operated starting and stopping generations and manual transfer switches for connect and disconnect to grid If digital, multiple communications media can be expected with DNP or other low latency protocol in use.	Load: Load center operations; generator control system if larger complex DCS Utility: power signals for demand response	Monetary: Damage of critical load center potential; inefficiencies in shaving peak load Physical Damage: limited to location but may be a larger load center or interruption of a production process Loss of Confidentiality: Customer information sensitivity Loss of Integrity: Potential loss of operation for load center Loss of Availability: Potential longer load center outage if damage to local generation or damage load center processes Reputation: Large impact due to most visible to customer if utility backup generation use mistake cost load center productivity	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Residential Subsystem: Load Control % in Subsystem: 25% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Localized Power Transfer Devices/Switches: **Uninterruptable Power Supply** **Power Transfer Load Center** **Automatic Transfer Switch**  	Microprocessor controller with distribution panel board, disconnect breakers, surge and load protections are commonly bundled together with an uninterruptable power supply that functions until longer term backup generators can take over the load.	Status: UPS health, breakers Control: Connect and disconnect, charge and discharge of batteries, start or stop of generator/flywheel	DNP or other low latency protocol networked or serial, some older configurations may be electo-mechanical without and embedded microprocessor system will exist.	Load: Load center UPS, Breakers, relays, substation for load center, backup generation, batteries Utility: Connect and Disconnect from grid	Monetary: Damage of critical load center potential; inefficiencies in shaving peak load Physical Damage: limited to location but may be a larger load center or interruption of a production process Loss of Confidentiality: Customer information sensitivity Loss of Integrity: Potential loss of operation for load center Loss of Availability: Potential longer load center outage if damage to local generation or damage load center processes Reputation: Mainly to load center customer	**CDP** Collateral Damage Potential N | L | **LM** | MH | H | ND **TD** Target Distribution Component: Residential Subsystem: Load Control % in Subsystem: 25% N | L | **M** | H | ND **CR** System Confidentiality Requirement **L** | M | H | ND **IR** System Integrity Requirement L | **M** | H | ND **AR** System Availability Requirement L | **M** | H | ND

Energy Markets

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Five Minute Markets	Shortest most expensive market to secure generation and transmission resources	Status of load demand and generation/transmission supply; provides wide area situational awareness and coordinates with other large entities in electrical interconnect such as the reliability coordinators.	All digital very IT looking configurations with hundreds of thousands of data points entering RTO/ISO networks every minute from remote locations (control centers, RTUs at substations)	Parallel system to power does not control but provides factors that impact control such as generation need for automatic generation control and transmission line ratings	Monetary: Financial impact with potential bad energy trades, inefficient operations of electric grid Physical Damage: slight potential impact to physical if energy trades imbalance the physical	**CDP** Collateral Damage Potential N | L | **LM** | MH | H | ND **TD** Target Distribution Component: Energy Markets Subsystem: Different Power Markets % in Subsystem: 60%
Imbalance Markets	Boundary between two control centers where one traditionally needs a specific type of generation or transmission from the other control area (i.e. NV and CA)					

			Environmental Vectors			
Electric Grid Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Load/Utility Power Flows**	**Consequences**	**Environmental Factors**
Hour Ahead Markets	Second most expensive market to secure generation and transmission resources	Control for Automated Generation Control, and Line ratings in transmission based on analysis modeling and forecasting	Automatic generation controls sent to generation stations, transmission capacity needed sent to transmission operators Other input for pricing signals, weather forecast, load forecast, demand response indications		supply/demand generation/load or overload transmission lines Loss of Confidentiality: Potential to game the energy market if information is made available Loss of Integrity: Efficiency of energy market trades Loss of Availability: Efficiency of energy market trades Reputation:	N L M H ND **CR** System Confidentiality Requirement L M H ND **IR** System Integrity Requirement L M H ND **AR** System Availability Requirement L M H ND
Day Ahead Markets	Daily planning market to secure generation and transmission					
Long Term Contracts 	Traditionally base load or base transmission capability purchases for electricity					

APPENDIX D: ICS VULNERABILITIES CHOSEN FOR SCENARIOS

Advisory (ICSA-11-356-01)

Siemens Simatic HMI Authentication Vulnerabilities

Original release date: December 22, 2011 | Last revised: April 22, 2013

Legal Notice

Overview

ICS-CERT is aware of a public report by independent security researchers Billy Rios and Terry McCorkle concerning authentication bypass vulnerabilities affecting Siemens SIMATIC HMI products which are supervisory control and data acquisition/human-machine interface (SCADA/HMI) products.

According to this report, systems running affected versions of this product are accessible using a default username and password. These systems also generate an insecure authentication token for browser sessions. Prior to public disclosure, the researchers notified ICS-CERT of the vulnerabilities. ICS-CERT is continuing to coordinate mitigations with the researchers and Siemens.

Siemens was previously aware of these vulnerabilities and intends to address them in Service Packs to be released in January 2012. Please see mitigation section of this document for additional information regarding the release of the Service Packs. Siemens has also updated its product documentation with instructions for configuring a strong password and removing default passwords during initial setup.

Affected Products

According to Siemens, the following software packages are vulnerable:

- martAccess option package for SIMATIC WinCC flexible RT 2004, 2005, 2005 SP1, 2007, 2008, 2008 SP1, and 2008 SP2
- SIMATIC WinCC Runtime Advanced V11, V11 SP1, and V11 SP2
- Multiple SIMATIC Panels (TP, OP, MP, Mobile, Comfort)

Impact

Successful exploitation of these vulnerabilities could allow an attacker to log on to a vulnerable system as a user or administrator with the ability to execute arbitrary code or obtain full access to files on the system.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

Background

The Siemens SIMATIC HMI product family is used as an interface between operators and corresponding PLCs. SIMATIC HMI does the following tasks: process visualization, operator control of the process, display of alarms, archiving of process values and alarms and management of machine parameters. This software is used in many industries including: food and beverage, water and wastewater, oil and gas, and chemical.

Vulnerability Characterization

Vulnerability Overview

Insecure Authentication Token Generation[1]

The authentication token/cookie values set when a user (administrator) logs are predictable when non-encrypted HTTP communication is used. This can allow for an attacker to bypass authentication checks and escalate privileges.

CVE-2011-4508 has been assigned to this vulnerability. Siemens' assessment of the vulnerabilities using the CVSSVersion 2.0[2] calculator rates an Overall CVSS Score of 6.5.

Weak Default Passwords[3]

There is a default administrator password, which is weak and easily bruteforced or guessed. Siemens has changed the documentation to encourage the user to change the password upon first login.

CVE-2011-4509 has been assigned to this vulnerability.

Vulnerability Details

Exploitability

This vulnerability can be exploited remotely against installations that are not following security practices recommended by Siemens and ICS-CERT.

Existence of Exploit

No known exploits specifically target these vulnerabilities.

Difficulty

It would be very simple to exploit the default password, it would require a greater amount of work and knowledge to exploit the insecure token generation vulnerability.

Mitigation

The authentication token generation vulnerability will be addressed by Siemens in its “SIMATIC WinCC V11.0 SP 2 Update 1,” which is to be released on January 13, 2012 or “SIMATIC WinCC flexible 2008 SP3” which is to be released on January 18, 2012.

Product documentation has been updated to tell the user how to set a proper password during initial setup to remove the risk of the default password vulnerability.

Siemens has published a statement on their Industrial Security web pages that addresses these issues.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages.
2. Refer to *Recognizing and Avoiding Email Scams* for more information on avoiding e-mail scams.
3. Refer to *Avoiding Social Engineering and Phishing Attacks* for more information on social engineering attacks.

---

1. CWE-287: Improper Authentication, http://cwe.mitre.org/data/definitions/287.html, website last accessed April 16, 2012.
2. NVD Common Vulnerability Scoring System Support v2, http://nvd.nist.gov/cvss.cfm, website last accessed April 16, 2012.
3. CWE-255: Credentials Management, http://cwe.mitre.org/data/definitions/255.html, website last accessed April 16, 2012.

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

Advisory (ICSA-13-011-03)

Rockwell Automation ControlLogix PLC Vulnerabilities

Original release date: January 10, 2013 | Last revised: February 17, 2014

Legal Notice

Overview

This advisory is a follow up to the original alert titled ICS-ALERT-12-020-02A—Rockwell Automation ControlLogix PLC Vulnerabilities that was published February 14, 2012, on the ICS-CERT Web page.

Independent researcher Rubén Santamarta of IOActive identified vulnerabilities in Rockwell Automation's ControlLogix PLC and released proof-of-concept (exploit) code at the Digital Bond S4 Conference on January 19, 2012. The vulnerabilities are exploitable by transmitting arbitrary commands from a control interface to the programmable logic controller (PLC) or network interface card (NIC). The information was released without coordination with either the vendor or ICS-CERT. Rockwell Automation released firmware patches on July 18, 2012, that resolve the following vulnerabilities. There have been no updates from Rockwell since these patches were released. Exploitation of these vulnerabilities could allow loss of confidentiality, integrity, and availability of the device.

These vulnerabilities could be exploited remotely. Exploits that target these vulnerabilities are publicly available.

Affected Products

The following Rockwell products are affected:

- All EtherNet/IP products that conform to the CIP and EtherNet/IP specifications,
- 1756-ENBT, 1756-EWEB, 1768-ENBT, 1768-EWEB communication modules,
- CompactLogix L32E and L35E controllers,
- 1788-ENBT FLEXLogix adapter,
- 1794-AENTR FLEX I/O EtherNet/IP adapter,
- ControlLogix, CompactLogix, GuardLogix, and SoftLogix, Version 18 and prior,
- CompactLogix and SoftLogix controllers, Version 19 and prior,
- ControlLogix and GuardLogix controllers, Version 20 and prior,
- MicroLogix 1100, and
- MicroLogix 1400.

Impact

Successful exploitation of these vulnerabilities may result in a denial-of-service (DoS) condition, controller fault, or enable a Man-in-the-Middle (MitM) attack, or Replay attack.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

Background

Rockwell Automation provides industrial automation control and information products worldwide, across a wide range of industries.

The affected products are PLCs and communication modules. According to Rockwell Automation, these products are deployed across several sectors including agriculture and food, water, chemical, manufacturing and others. According to Rockwell's Web site, these products are used in France, Italy, the Netherlands, and other countries in Europe, as well as the United States, Korea, China, Japan, and Latin American countries.

Vulnerability Characterization

Vulnerability Overview

Improper Access Control—Change IP[a]

When an affected product receives a valid CIP message from an unauthorized or unintended source to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP that changes the product's configuration and network parameters, a DoS condition can occur. This situation could cause loss of availability and a disruption of communication with other connected devices.

CVE-2012-6439 has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:P/A:C).

Improer Access Control—Reset[b]

When an affected product receives a valid CIP message from an unauthorized or unintended source to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP that instructs the product to reset, a DoS can occur. This situation could cause loss of availability and a disruption of communication with other connected devices.

This vulnerability was discovered by Rockwell Automation engineers as they were investigating other vulnerabilities reported at the Digital Bond S4 2012 Conference.

CVE-2012-6442 has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).

Improper Access Control—Stop[c]

When an affected product receives a valid CIP message from an unauthorized or unintended source to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP that instructs the CPU to stop logic execution and enter a fault state, a DoS can occur. This situation could cause loss of availability and a disruption of communication with other connected devices.

CVE-2012-6435 has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).

Information Exposure[d]

An information exposure of confidential information results when the device receives a specially crafted CIP packet to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP. Successful exploitation of this vulnerability could cause loss of confidentiality.

This vulnerability was discovered by Rockwell Automation engineers as they were investigating other vulnerabilities reported at the Digital Bond S4 2012 Conference.

CVE-2012-6441 has been assigned to this vulnerability. A CVSS v2 base score of 5.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:N/A:N).

Improper Validation—NIC[e]

The device does not properly validate the data being sent to the buffer. An attacker can send a malformed CIP packet to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP, which creates a buffer overflow and causes the NIC to crash. Successful exploitation of this vulnerability could cause loss of availability and a disruption in communications with other connected devices.

CVE-2012-6438 has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).

Improper Validation—CPU[f]

The device does not properly validate the data being sent to the buffer. An attacker can send a malformed CIP packet to Port 2222/TCP, Port 2222/UDP, Port 44818/TCP, or Port 44818/UDP, which creates a buffer overflow and causes the CPU to crash. Successful exploitation of this vulnerability could cause loss of availability and a disruption in communications with other connected devices.

CVE-2012-6436rhas been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).

Authentication Bypass by Capture—Replay[g]

The Web server password authentication mechanism used by the products is vulnerable to a MitM and Replay attack. Successful exploitation of this vulnerability will allow unauthorized access of the product's Web server to view and alter product configuration and diagnostics information.

his vulnerability was discovered by Rockwell Automation engineers as they were investigating other vulnerabilities reported at the Digital Bond S4 2012 Conference.

CVE-2012-6440 has been assigned to this vulnerability. A CVSS v2 base score of 9.3 has been assigned; the CVSS vector string is (AV:N/AC:M/Au:N/C:C/I:C/A:C).

Improper Authentication—Firmware Upload[h]

The device does not properly authenticate users and the potential exists for a remote user to upload a new firmware image to the Ethernet card, whether it is a corrup or legitimate firmware image. Successful exploitation of this vulnerability could cause loss of availability, integrity, and confidentiality and a disruption in communications with other connected devices.

CVE-2012-6437 has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C)

Vulnerability Details

Exploitability

These vulnerabilities could be exploited remotely.

Existence of Exploit

Exploits that target these vulnerabilities are publicly available.

Difficulty

An attacker with a low-medium skill would be able to exploit these vulnerabilities.

Mitigation

According to Rockwell, any of the above products that become affected by a vulnerability can be reset by rebooting or power cycling the affected product. After the reboot, the affected product may require some reconfiguration.

To mitigate the vulnerabilities, Rockwell has developed and released security patches on July 18, 2012, to address each of the issues. To download and install the patches please refer to Rockwell's Advisories at:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/470154
https://rockwellautomation.custhelp.com/app/answers/detail/aid/470155
https://rockwellautomation.custhelp.com/app/answers/detail/aid/470156

For more information on security with Rockwell Automation products, please refer to Rockwell's Security Advisory Index.

Rockwell recommends updating to the newest firmware patches to fix the vulnerabilities, but if not able to do so right away, then Rockwell advises immediately employing the following mitigations for each of the affected products.

To mitigate the vulnerabilities pertaining to receiving valid CIP packets:

1. Block all traffic to the Ethernet/IP or other CIP protocol-based devices from outside the Manufacturing Zone by restricting or blocking access to TCP and UDP Ports 2222 and 44818 using appropriate security technology such as a firewall or Unified Threat Management (UTM).
2. Employ a UTM appliance that specifically supports CIP message filtering.

To mitigate the vulnerability pertaining to the corrupted firmware update:

1. At this time, Rockwell is still evaluating the feasibility of creating an update for the 1756-ENBT communication module to include a digital signature validation mechanism on the firmware.
2. Until Rockwell creates an update, concerned customers are recommended to employ good security design practices and consider using the more contemporary 1756-EN2T Ethernet/IP communication modules for the ControlLogix platform. The 1756-EN2T has been able to validate digital signatures since firmware Release 5.028.

To mitigate receiving malformed CIP packets that can cause the controller to enter a fault state:

1. Where possible, Rockwell recommends users to upgrade the affected products to Logix Release V20 and higher.

To mitigate receiving valid CIP packets that instruct the controller to stop logic execution and enter a fault state:

1. Where possible, upgrade CompactLogix and SoftLogix affected products to Logix Release V20 or higher.
2. Where possible, upgrade ControlLogix and GuardLogix affected products to Logix Release v20.012 or higher.
3. Block all traffic to the Ethernet/IP or other CIP protocol devices as directed above.
4. Employ a UTM as directed above.

To mitigate the vulnerability with the Web server password authentication mechanism:

1. Upgrade the MicroLogix 1400 firmware to FRN 12 or higher.
2. Because of limitations in the MicroLogix 1100 platform, none of the firmware updates will be able to fix this issue, so users should use the following techniques to help reduce the likelihood of compromise.
3. Where possible, disable the Web server and change all default Administrator and Guest passwords.
4. If Web server functionality is needed, then Rockwell recommends upgrading the product’s firmware to the most current version to have the newest enhanced protections available such as:
   1. When a controller receives two consecutive invalid authentication requests from an HTTP client, the controller resets the Authentication Counter after 60 minutes.
   2. When a controller receives 10 invalid authentication requests from any HTTP client, it will not accept any valid or invalid authentication packets until a 24-hour HTTP Server Lock Timer timeout.
5. If Web server functionality is needed, Rockwell also recommends configuring user accounts to have READ only access to the product so those accounts cannot be used to make configuration changes.

In addition to the above, Rockwell recommends concerned customers remain vigilant and continue to follow security strategies that help reduce risk and enhance overall control system security. Where possible, they suggest you apply multiple recommendations and complement this list with your own best-practices:

1. Employ layered security and defense-in-depth methods in system design to restrict and control access to individual products and control networks. Refer to http://www.ab.com/networks/architectures.html for comprehensive information about implementing validated architectures designed to deliver these measures.
2. Restrict physical and electronic access to automation products, networks, and systems to only those individuals authorized to be in contact with control system equipment.
3. Employ firewalls with ingress/egress filtering, intrusion detection/prevention systems, and validate all configurations. Evaluate firewall configurations to ensure other appropriate inbound and outbound traffic is blocked.
4. Use up-to-date end-point protection software (e.g., antivirus/antimalware software) on all PC-based assets.
5. Make sure that software and control system device firmware is patched to current releases.
6. Periodically change passwords in control system components and infrastructure devices.
7. Where applicable, set the controller key-switch/mode-switch to RUN mode.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

---

a. CWE, http://cwe mitre.org/data/definitions/284.html, CWE-284: Improper Access Control, Web site last accessed January 09, 2013.

b. http://cwe.mitre.org/data/definitions/284.html
c. CWE, http://cwemitre.org/data/definitions/284.html, CWE-284: Improper Access Control, Web site last accessed January 11, 2013.
d. CWE, http://cwemitre.org/data/definitions/200.html, CWE-200: Information Exposure, Web site last accessed January 11, 2013.
e. CWE, http://cwemitre.org/data/definitions/20html, CWE-20: Improper Input Validation, Web site last accessed January 11, 2013.
f. CWE, http://cwemitre.org/data/definitions/20.html, CWE-20: Improper Input Validation, Web site last accessed January 11, 2013.
g. CWE, http://cwe.mitre.org/data/definitions/294html, CWE-294: Authentication Bypass by Capture-replay, Web site last accessed January 11, 2013.
h. CWE, http://cwemitre.org/data/definitions/284.html, CWE-284: Improper Access Control, Web site last accessed January 11, 2013.

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

Advisory (ICSA-14-196-01)

SubSTATION Server Telegyr 8979 Master Vulnerabilities

Original release date: July 31, 2014

Legal Notice

OVERVIEW

This advisory was originally posted to the US-CERT secure Portal library on July 15, 2014, and is being released to the NCCIC/ICS-CERT web site.

Adam Crain of Automatak and Chris Sistrunk of Mandiant have identified a Buffer Overflow Vulnerability in the SUBNET Solutions Inc (SUBNET), SubSTATION Server 2, Telegyr 8979 Master application. SUBNET has produced a hot fix that mitigates this and a related vulnerability the vendor found independently. The researchers have tested the new hot fix and validate that it resolves these vulnerabilities.

These vulnerabilities could be exploited remotely.

AFFECTED PRODUCTS

The following SUBNET product is affected:

- SubSTATION Server 2 Telegyr 8979 Master Protocol – All Versions.

IMPACT

By sending specially crafted invalid RTU messages to the Telegyr 8979 master, a buffer overflow can occur, resulting in a denial of service (DoS).

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

SUBNET is based in Calgary, Alberta, Canada.

The affected product, SubSTATION Server, is a vendor agnostic multifunction software application used in intelligent substation automation and IT networking. SubSTATION Server performs data concentration, protocol translation, automation logic, event file collection, and enterprise connectivity. This allows replacement of separate legacy devices, such as RTU data concentrators, relay communications processors used in the operation of electrical substations. According to SUBNET, SubSTATION Server is deployed in the Energy sector including oil and gas and electric utilities. SUBNET estimates that these products are used primarily in the United States and Canada.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER INPUT VALIDATION[a]

The researchers found that by sending a specially crafted packet simulating an RTU to Master message exceeding allowable data length, an attacker can cause the Telegyr 8979 Master to crash. SUBNET has also discovered that after sending a specially crafted message containing a valid data length, any subsequent message sent immediately to the Telegyr 8979 will also crash the service. SUBNET had also determined the root issue was in the GPT software library.

CVE-2014-2357[b] has been assigned to this vulnerability. A CVSS v2 base score of 8.3 has been assigned; the CVSS vector string is (AV:A/AC:L/Au:N/C:C/I:C/A:C).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

Crafting a working exploit for these vulnerabilities would be difficult. An attacker with a moderate to high skill level would be able to exploit these vulnerabilities.

MITIGATION

SUBNET has produced hot fix “SSNET v2.12 HF18808” to resolve this issue.

This hot fix can be obtained by secure FTP provided by the SUBNET support department. Please contact SUBNET Customer Support at: (403) 270-8885, or by email at: support@SUBNET.com and reference SUBNET Release Bulletin “SubSTATION Server 2.12 HF18808 Release, 21 May 2014” for a copy of this release bulletin and download/installation information (This bulletin is being sent to registered users only).

Vendor Recommendation:

- The exploit results in an unrecoverable exception, but all software components are registered as Services under Windows and can be configured to automatically restart after any stoppage. Users can configure the service to automatically restart, which limits the DoS to a momentary disruption.
- Backward compatible releases will be available by request for customers using older versions of SubSTATION Server.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page at: http://ics-cert.us-cert.gov/content/recommended-practices. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

---

a. CWE-20: Improper Input Validation, http://cwe.mitre.org/data/definitions/20.html, web site last accessed July 15, 2014.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-2357, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?calculator&version=2&vector=AV:A/AC:L/Au:N/..., web site last accessed July 15, 2014.

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

ICS-CERT continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

APPENDIX E: EXAMPLES OF CONSEQUENCE TABLE FOR OTHER SECTORS

Appendix E
Examples of Consequence Table for Other Sectors

Critical Infrastructure: Chemical Sector

NOTE: The security issues associated with the Chemical Sector are similar to those for the Petroleum and Oil & Gas Subsectors of the Energy Sector.

Per the NIPP, the Chemical Sector can be divided into 4 key functional areas. Cyber vulnerability/consequence tables are provided in this appendix for each of these 4 key functional areas in the Chemical Sector:

(1) Manufacturing plants;

(2) Transportation systems;

(3) Warehousing and storage systems, including stockpile and supply areas; and

(4) Chemical end users.

Each table provides some examples of the major subsystems and components used in the majority of facility types in each of the four functional areas the Chemical Sector.

The Applications subsection describes the functions that maybe implement in any other of the subsystems. Due to the nature of the nature of chemical systems, not all applications' status and control are digital. Older electro mechanical status and control are common on older subsystems and can still be found in some areas. Other newer components will be digital control and status.

The headings on the columns are described as follows:

- Chemical Sector Functional Area Component or Subsystem: Scope of apparatus discussed.
- Purposes: Descriptions of the functional roles the subsystems and components.
- Status & Controls: Distinction between typical status and control mechanisms. While no communications is strictly one way in a cyber security view (host computer someplace to impact communications), status is generally from field components and field controllers into the larger subsystems, and control acts on the status(es) or a command from an operator from the subsystem to the field components and field controllers.
- Digital Flows: Show the data network connectivity between the component to other subcomponents to larger subsystems, and control centers.. If other control is not digital, manual functions or controls for impact determinations. Manual or local controls controls may work independent of a digital system, such as a pressure relief valve or float that shuts off valves on high tank level).
- Material Flows: Describes the upstream and downstream dependencies of the particular subsystem on material flows.
- Consequences: This column follows the same logic as the Environmental Factors in the CVSS 2.0 with Monetary and Reputation also summarized for impact.

A flow diagram of the typical chemical process and supply chain for a chemical product is shown in Figure 1.

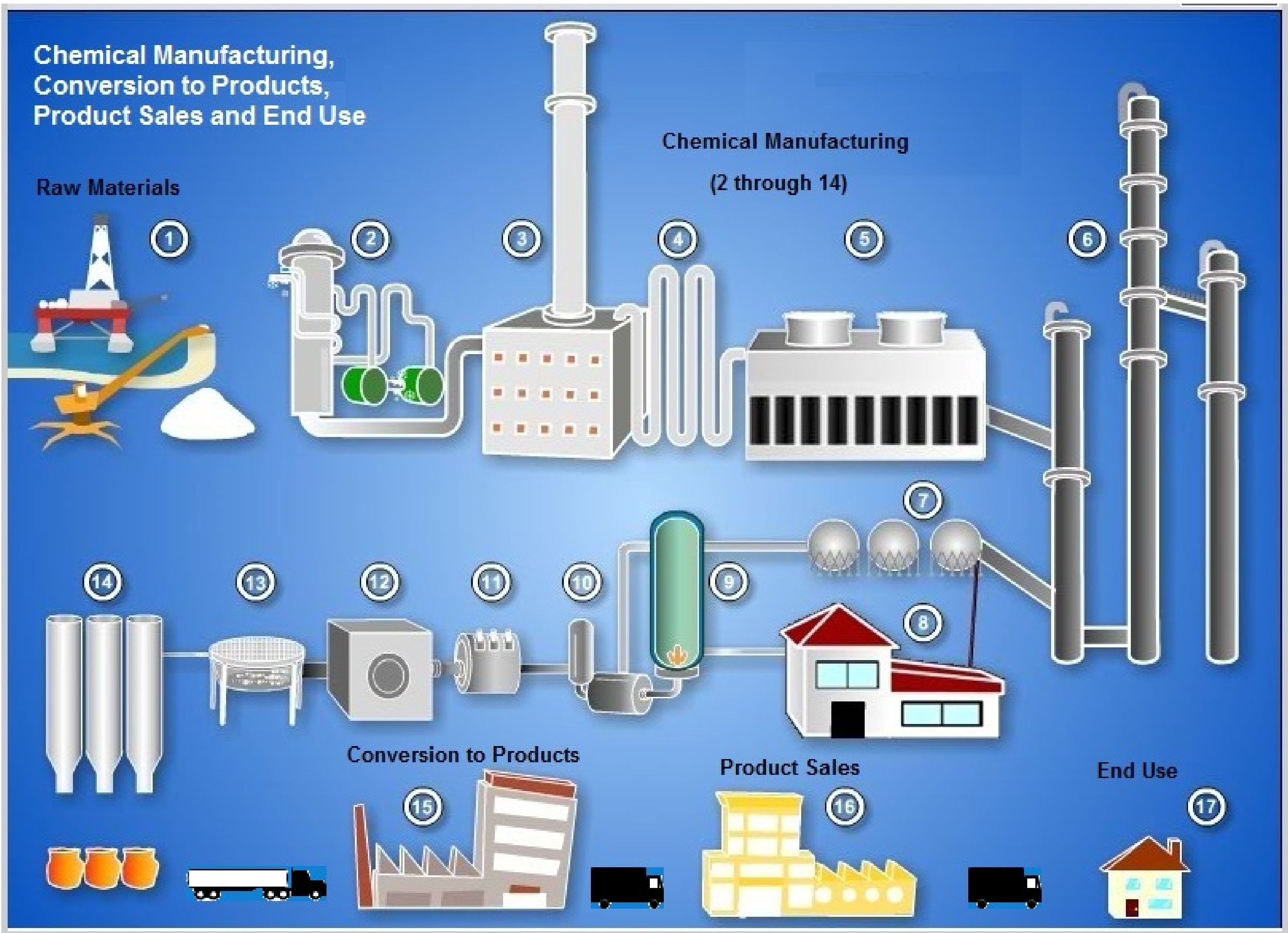


Figure E-1. Example of Processes in a Typical Chemical Sector Supply Chain.

Each of the four functional areas depends on digital devices and computer systems for a variety of purposes, including the following:

a) Operating manufacturing processes using automated industrial control systems and process safety systems;
b) Tracking inventory, storage, and movement of chemical products;
c) Storing customer information, including products that are bought on a regular basis and the locations where they are typically sent;
d) Storing personnel information to prevent the theft of personal identity information; and
e) Operating perimeter security systems.

Personnel surety is also an important aspect of securing cyber systems at chemical facilities. Many companies in the sector have mitigated the risk of coercion or insider threat by utilizing policies, practices, and technologies that protect the linkage of critical plant systems with corporate networks. Secure authentication technology may be used to restrict access based on roles and clearances while proper policies are employed to terminate user accounts once an employee’s relationship with the company is terminated.

As a result of the importance of cyber systems in the sector and the focused effort on cybersecurity, many companies are trying to improve communication among industrial control systems security, the security of business systems, and physical security. Companies are increasingly likely to include an information technology security representative on the corporate crisis management team. Other members of the crisis management team may include representatives from the public affairs office, physical security officers, and representatives from business and finance.

Environmental Factors are listed from CVSS 2.0 below.

Common Vulnerability Scoring Systems Environmental Vectors

Metric: CDP = Collateral Damage Potential (Organization specific potential for loss)
Possible Values: N = None, L = Low, LM = Low-Medium, MH = Medium-High, H = High, ND = Not Defined

Metric: TD = Target Distribution (Percentage of vulnerable systems)
Possible Values: N = None (0%), L = Low (1-25%), M = Medium (26-75%), H = High (76-100%), ND = Not Defined

Metric: CR = System Confidentiality Requirement (draft proposal)
Possible Values: L = Low, M = Medium, H = High, ND = Not Defined

Metric: IR = System Integrity Requirement (draft proposal)
Possible Values: L = Low, M = Medium, H = High, ND = Not Defined

Metric: AR = System Availability Requirement (draft proposal)
Possible Values: L = Low, M = Medium, H = High, ND = Not Defined

Evaluation Assumptions for Environmental Factors

Collateral Damage Potential: The consequence discussion includes monetary and physical damage which can be related to the subjective rating in collateral damage potential. Some components have large monetary value, potential for personnel injury or potential for damage to the real world environment (e.g. pollution of groundwater) if physically damaged, while other components may have little or no damage potential and be easier to replace (i.e. historian database). If the damage potential is very localized, then the rating would be lower (e.g. failure of a single controller or chemical plant component versus major plant damage causing a major fire, explosion or toxic material leak that affects an entire plant, surrounding communities and waterways).

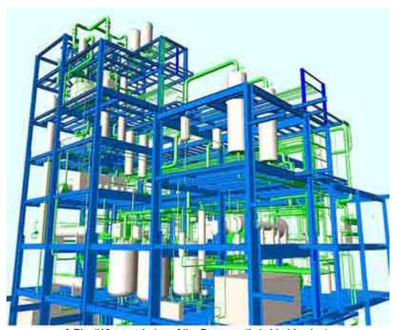
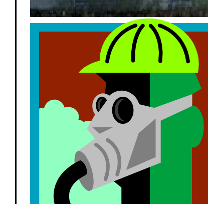
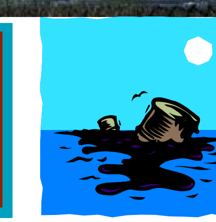
Target Distribution: Not all subsystems and components are digital and will have a cyber impact (i.e. manual valves do not have an embedded digital system). To understand the Environmental Factors, the maximum impact based on the limited information available, is represented in the Target Distribution factor. For example, the number and extent of digital and cyber control systems versus manual operation of systems in a chemical plant depends on numerous factors such as plant size, age, process complexity, level of regulatory oversight and/or quantities of chemical(s). Only a small fraction of the total number of chemical facilities have the potential for causing major impact as identified from EPA risk management plans and DHS Chemical Facility Anti-terrorism Act analyses. Of those facilities with the potential for major impact, only some portion (unknown) of the facilities may use digital systems that can be readily impacted by a cyber attack. If industrial control system vendor X had an exploitable vulnerability, only a portion of high-risk chemical facilities would be expected to use that vendor's system since vendor X does not supply all If industrial control system in the United States. Government data on chemical facilities, market surveys, installation specifics and subject matter experts will be needed to better understand and quantify the environmental factors.

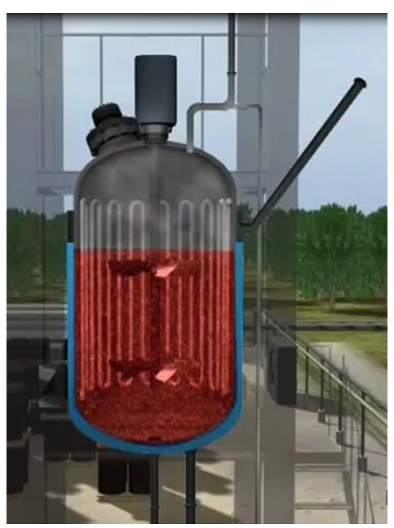
System Confidentiality: For the state and temporal nature of the chemical systems, confidentiality is a lesser concern unless dealing with customer data.

System Integrity: The ability for operations to understand the correct state or situational awareness makes integrity an important environmental factor for chemical systems.

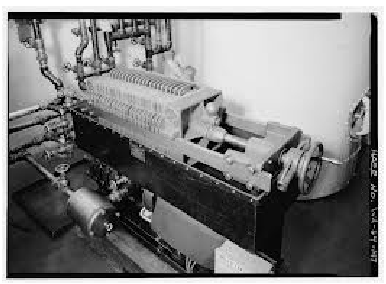
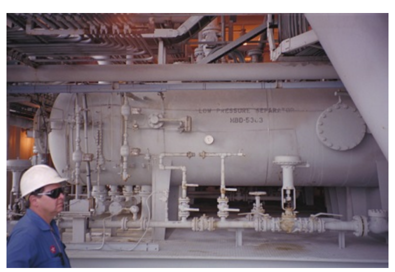
System Availability: Based on the safety and security needs of the chemical component or subsystem, some command operations may need to occur with minimum latency and in proper sequence with other actions making availability an important environment factor for control system components.

Chemical Manufacturing

			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
Chemical Manufacturing Plant   A PlantWise rendering of the Bayer methyl chloride plant.  PlantBuilder automatically generates 3D plant layouts from equipment information.	Convert raw materials (e.g. bulk chemicals, fuels or renewable resources) into chemical products. Chemical Manufacturing Plants are similar to any complex manufacturing system with many subsystems to support the conversion of raw materials into a finished product. The key functional areas for Chemical Manufacturing Plants are similar to those for Petroleum/Oil Refineries and Natural Gas Processing Plants.	Operating manufacturing processes use many automated industrial control systems, process safety systems Primary plant controls: • Raw materials storage(gas, liquid and/or solid) • Raw materials transfer • Reactor(s) control • Temperature, flow, pressure and chemical/gas composition monitoring and control • Intermediate product transfer and storage • Final product transfer and storage (gas, liquid and/or solid) • Utilities: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation, communications Process safety systems: • Chemical Safety Systems • Pressure Relief Safety Systems • Toxic / flammable release safety systems • Fire safety/suppression systems • Leak detection and alarms • Emergency or backup power generation for safe emergency shutdown Maintenance status	Upstream Communications: • Process monitoring and control: • Pressure, temperature and level monitoring • Leak monitoring and detection • Tracking inventory, storage, and movement of raw materials • Monitoring Status and availability of Utilities: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation Local Communications: • Plant Control systems • Process communications within the plant can be a combination of digital, analog, and wireless • Control rooms and controllers may exist local to individual processes within the plant • Data aggregation within the plant is usually at a central control room or main plant automation servers (e.g. DCS, SCADA server) • Remote vendor access Downstream Communications – • Data transfer to corporate systems • Tracking inventory, storage, and movement of chemical products and waste products • Air and water emissions monitoring and data	Upstream raw materials (e.g. bulk chemicals, fuels or renewable resources and utilities • Movement and storage, of raw materials • Raw materials storage(gas, liquid and/or solid) • Utilities: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation Local: • Movement and storage, of raw materials, feeds, products and wastes throughout the plant • Reaction of feeds to products and byproducts • May be gases, liquids, solids or mixtures Downstream – Plant Operation Systems and environmental monitoring and control systems. • Storage, and movement of chemical products and waste products • Waste Storage (gas, liquid and/or solid) • Waste disposal (gas, liquid and/or solid) • Air and water emissions •	Monetary – losses from nuisance failures and shut downs of subsystems or fines from operating outside of EPA and other regulatory requirements Physical Damage - depends upon the number of different chemicals on-site, chemical quantities, chemical hazards (toxicity, reactivity, flammability, explosivity), chemical state (gas, liquid, solid) and system operating parameters (temperature, pressure) • Loss of reaction control • Fire or explosion • Loss of life or injury to personnel • Physical damage to parts and equipment in balance of plant • Damage to the environment: • Loss of confidentiality – low Loss of Integrity – can be low to high depending on the chemical and plant systems (e.g. integrity requirement can be medium to high for air and water emissions monitoring systems) Loss of System availability - requirement is high due to need for real-time or near-real-time status of plant systems.	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Chemical Manufacturing Subsystem: Chemical Manufacturing Plant % in Subsystem: much less than 10% of Chemical plants are both high hazard/risk <u>and</u> use digital systems from the same vendor N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND    

			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
			transfer to regulators • Balance of Plant Systems • Leak detection • Emergency or backup power generation for safe emergency shutdown of digital systems			
Chemical Reactors  	Converts raw materials (e.g. bulk chemicals, fuels or renewable resources) into chemical products. Chemical reactors are common in Chemical Manufacturing Plants and Petroleum/Oil Refineries and Natural Gas Processing Plants.	Local controls • Reactant and product transfer system (pumps) • Manual valves • Local process indicators (e.g. temperature, pressure, flow, level, sight glasses, etc.) • Utilities: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation, communications Protection controls: • Pressure Relief Safety Systems • Toxic / flammable release safety systems • Fire safety/suppression systems • Leak detection • Ventilation systems Operational Controls: • Reactants, inerts and products inlet and outlet flow control (pumps and control valves) • Reactor temperature, flow, pressure and chemical/gas composition monitoring and control • Control of utilities needed to control reactor conditions: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation • Product outlet flow control	Upstream Communications: • Chemical feed storage level, flow control and alarms • Utility flow control • On/off or variable position control valves • Leak detection • On/off or variable flow pumps or conveyor systems Local Communications: • Field devices at the reactor may communicate with a local controller or local safety systems/ alarms • Local safety systems may be linked to control automatic valves, switches, pump relays or fire suppression systems. Downstream Communications Control Systems for Reactor Operation • PLC • Motor VSD, starters • Fuel Feeders • Balance of Plant Systems • Feedforward control of downstream product storage and reactors. • Control of reactor area	Upstream • Chemical Supplies and utilities • Reactant transfer systems. • May be gases, liquids, solids or mixtures • Utilities: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation Local: • Reaction of feeds to products and byproducts • May be gases, liquids, solids or mixtures Downstream • Product(s), unused reactant(s), waste and utilities (e.g. cooling water) outlet flows. May be gases, liquids, solids and/ or mixtures • Balance of Plant Systems • Downstream product storage and reactors. • Reactor area ventilation systems • Ventilation and process exhaust	Monetary – losses from nuisance failures and shut downs of subsystems or fines from operating outside of EPA and other regulatory requirements Physical Damage - depends upon the number and quantity of different chemicals in the process unit, hazards of the chemical(s) (toxicity, reactivity, flammability, explosivity), chemical state (gas, liquid, solid) and system operating parameters (temperature, pressure) • Loss of process control • Fire or explosion • Loss of life or injury to personnel in the vicinity of the process unit • Collateral damage to nearby plant systems likely, but will be limited within any one plant, due to separation of hazardous systems and boundary protections Loss of Confidentiality - is low Loss of Integrity – can be low to high depending on the chemical and plant systems (e.g. integrity requirement can be medium to high for process safety systems, and air and water emissions monitoring systems) Loss of Availability – Timely status	**CDP** Collateral Damage Potential N | L | LM | **MH** | H | ND **TD** Target Distribution Component: Chemical Plant Subsystem: Chemical Reactor % in Subsystem: much less than 10% of Chemical plants are both high risk for more than local damage and use digital systems from the same vendor N | **L** | M | H | ND **CR** System Confidentiality Requirement **L** | M | H | ND **IR** System Integrity Requirement **L** | M | H | ND **AR** System Availability Requirement L | M | **H** | ND

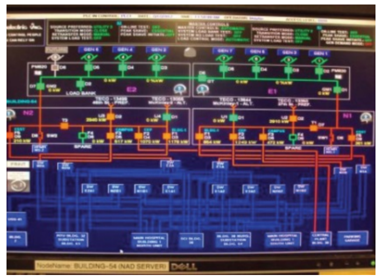
			Environmental Vectors			
Chemical Sector Component or Subsystem	Purposes	Status & Controls	Up/Down Stream Digital	Up/Down Stream Material Flows	Consequences	Environmental Factors
			ventilation systems • Chemical storage level, flow control and alarms • Chemical and utility flow control • On/off or variable position control valves • Leak detection • Alarms and Safety System Status		of process variables, alarms and safety systems is critical for safe and stable operation 	

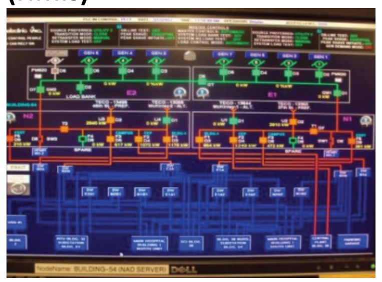
			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
Chemical Separation Units (e.g. distillation columns, flash drums, decanters, filters, screens, etc.)   	Separates mixtures of chemical products and/or wastes into separate streams. Separation of mixtures can involve separation by chemical state (gas, liquid, solid), or component properties (e.g. water and organic, solids size, etc.)	Local controls • Chemical transfer systems (pumps) • Manual valves • Local process indicators (e.g. temperature, pressure, flow, level, sight glasses, etc.) • Chemical separation unit(s) temperature, flow, pressure and chemical/gas composition monitoring and control systems • Utilities: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation, communications Protection controls: • Pressure Relief Safety Systems • Toxic / flammable release safety systems • Fire safety/suppression systems • Leak detection • Ventilation systems Operational Controls: • Chemical(s) and inert(s) flow control (pumps and control valves) • Chemical separation unit(s) temperature, flow, pressure and chemical/gas composition monitoring and control • Utilities needed to control chemical separation unit conditions: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation • Product outlet flow control	Upstream – Chemical and utility flow control • Storage level and flow Control and Alarms • Leak detection Local Communications: • Field devices at the process may communicate with a local controller or local safety system/ alarm • Local safety systems may be linked to control automatic valves, switches, pump relays or fire suppression systems. Downstream – Plant Operation Systems • PLC • Motor VSD, starters • Fuel Feeders • Balance of Plant Systems • Downstream product storage and chemical separation units. • Chemical separation unit area ventilation systems	Upstream • Chemical transfer systems. • Utilities: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation Downstream • Utilities: Cooling water, steam, compressed air/gas, fuel, electricity, ventilation • Product, waste and utilities (e.g. cooling water) outlet flows • Ventilation exhaust	Monetary – losses from nuisance failures and shut downs of subsystems or fines from operating outside of EPA and other regulatory requirements Physical Damage - depends upon the number and quantity of different chemicals in the process unit, chemical hazards (toxicity, reactivity, flammability, explosivity), chemical state (gas, liquid, solid) and system operating parameters (temperature, pressure) • Loss of process control • Fire or explosion • Loss of life or injury to personnel in the vicinity of the process unit • Collateral damage to nearby plant systems likely, but will be limited within any one plant, due to separation of hazardous systems and boundary protections Loss of Confidentiality - is low Loss of Integrity – can be low to high depending on the chemical and plant systems (e.g. integrity requirement can be medium to high for process safety systems, and air and water emissions monitoring systems) Loss of Availability – Timely status of process variables, alarms and safety systems is critical for safe and stable operation	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Chemical Plant Subsystem: Chemical Separator Unit % in Subsystem: much less than 10% of Chemical plants are both high risk for more than local damage <u>and</u> use digital systems from the same vendor N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
Bulk Chemical Storage   	Store bulk chemicals received (raw products) and chemicals produced (products and waste materials) until needed by the plant or transferred off-site Packaged chemicals may be stored in bulk tanks or in individual packaging ready for transportation (e.g. supersacks, drums, gas cylinders, totes)	Many industrial control and instrumentation systems. Primary plant controls • Data monitoring system Protection controls • Level, temperature, pressure, leak detection • Emissions monitoring for large storage areas	Upstream Communications: • Chemical Delivery and off-loading • Material movement controls (e.g. pumps, augers conveyer belt Local Communications: • Field devices at the bulk storage tanks or packaged chemical storage pads may communicate with a local controller or local safety system/ alarm • Local safety systems may be linked to control automatic valves, switches, pump relays or fire suppression systems. Downstream Communications: • Chemical storage level, flow control and alarms • Chemical and utility flow control • To Plant Control Room via ICS communication or TCP/IP protocols	Upstream • Chemical Delivery and off-loading • Transfer of bulk chemicals into containers or bulk storage (tanks, silos, etc.) • Container movement • Bulk material movement (e.g. pumps, augers, conveyer belts, piping, bins, etc.) Downstream • Chemical storage • Transfer of chemicals into containers or bulk chemical transport tanks/hoppers (rail, truck, barge, ship) • Transfer of chemical containers onto transportation systems (rail, truck, barge, ship, air)	Monetary – losses from nuisance failures and shut downs of subsystems or fines from operating outside of EPA and other regulatory requirements Physical Damage - depends upon the number and quantity of different bulk chemicals, chemical hazards (toxicity, reactivity, flammability, explosivity), chemical state (gas, liquid, solid, pressure/temperature) • Fire or explosion • Loss of life or injury to personnel • Physical damage to parts and equipment in balance of plant • Damage to the environment • Collateral damage to nearby plant systems likely, but will be limited within any one plant, due to separation of hazardous systems and boundary protections Loss of Confidentiality - is low Loss of Integrity – can be low to high depending on the chemical and plant systems (e.g. integrity requirement can be medium to high for process safety systems, and air and water emissions monitoring systems) Loss of Availability – Timely status of process variables, alarms and safety systems is critical for safe and stable operation	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Chemical Plant Subsystem: Bulk Chemical Storage % in Subsystem: <10% of chemical plants store enough hazardous chemicals and have digital systems from the same vendor N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

Applications on Specialized Equipment or Programmed into PLC or DCS

			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
Process Control Rooms 	A central location for operators to monitor and control plant and/or process operations for a facility or group of facilities. These are usually located outside the local zone of hazards for the processes being monitored and controlled.	Status received by other data sources and other DCSs which are displayed either on large visual boards or HMIs with many other sub displays to aid the operators including alarms and alerts. Controls are sent to process field devices directly or to local PLCs either via automatic scheduling/batching or operator action.	Upstream communications with local control rooms either from field devices or remote DCS, PLCs or smart field devices with embedded microprocessors depended on the size the type of plant or process. Data from RTUs is sent to substation control centers and personnel or automation systems at the center monitor the data from the RTUs and send control commands back to the RTU's if needed. Internal to the control room the low latency protocols are common (DNP, Modbus, Fieldbus), fiber media or twisted pair with considerations for electromagnetic interference and environmental conditions. Downstream communications are to data historians and business data users.	Operators maintain control of material flows within their process or plant from control rooms, and may have some monitoring and control over loading/unloading of material to/from transportation systems.	Monetary: s with potential wider impact if networked or coordinated attack Physical Damage: Cyber attackers who take control of systems in process control rooms may be able to cause physical damage to plant systems. Loss of Confidentiality - Low Loss of Integrity - may result in improper operations, reliability issues Loss of Availability: Chemical processes may become unstable leading to equipment failures, leaks, and worse within the plant, but only a small fraction of chemical plants are high risk for Reputation: Public loss of confidence in local systems or sector	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Chemical Plant Subsystem: Process Control Room % in Subsystem: +90% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

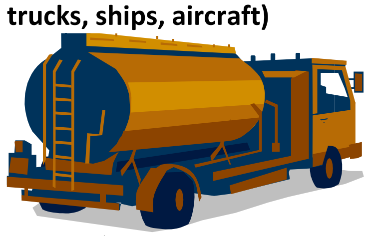
			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
Distributed Control Systems (DCSs) 	Used for more localized control of one or more process systems within a plant or compound. Common functions in a DCS include: 1) Human machine interface (HMI) for the operator human in the loop operations, 2) Historian for recording, 3) input and output to actuators, switches relays for actions, 4) data communication networks to and from the control and status components, 5) engineering workstations and/or non-production systems for design, development, updating and maintenance of the computer programs , 6) programs specific to the data for operational set points, alarm indicators, automatic actions for time sensitive critical operations; which may be layers upon layers of programs functioning on different platforms (i.e. PLCs, RTUs and other localized industrial control system).	Status received by other data sources and other DCSs which are displayed either on large visual boards or HMIs with many other sub displays to aid the operators including alarms and alerts. Controls sent to process or local PLCs either via automatic scheduling/batching or operator action.	Upstream Communications: Receive data from chemical process systems and field devices/monitors. Can be real-time or near-real-time Downstream Communications: Serve process data to remote locations for use by production planners, business, regulatory agencies, etc. Can also push data up to larger control centers, or SCADA systems using common ICS protocols on traditional networks (packet switched telephone modems, virtualized private networks isolated on the internet, private networks, cellular). Most networks will be IP (TCP/IP based and may tunnel in more ICS-specific protocols (DNP, Modbus) Inside the local area network for the control system connecting the HMI, historian, engineering workstations together may be a typical TCP/IP network but use more UDP or stateless communications for low latency protocols such as (DNP, Modbus, FieldBus). Down to the control devices, other embedded microcontrollers (PLC, IED, RTU) may be TCP/IP based but more commonly serial or low latency communications.	DCSs maintain control of material flows within their process or plant, and may have some control of transportation loading/unloading operations.	See consequences for Process Control Rooms	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: DCS Subsystem: All % in Subsystem: 100% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

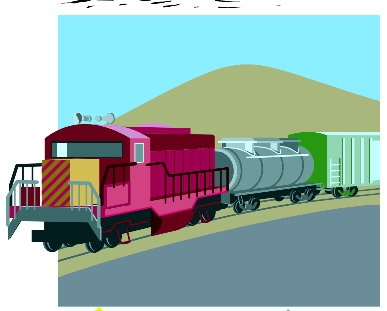
			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
Human Machine Interfaces (HMIs) 	HMIs are computers running software packages and are used as an interface between the operator and the Industrial Control Systems (SCADA systems, PLCs, DCSs, RTUs, etc.) controlling one or more process or system. HMIs perform the following tasks: • System visualization, • Operator control of the system, • Alarm display and acknowledgement, • System value and alarm archiving, and • Machine parameter management HMIs are used in nearly all industries with Industrial Control Systems, including power, water and wastewater, oil and gas, and chemical.				Refer to the Component or Subsystem which uses the affected HMI for consequences of loss of HMI view or control for that Component or Subsystem for additional consequences Successful exploitation of an HMI vulnerability could allow an attacker to log on to a vulnerable HMI as a user or administrator, where they would be able to perform any of the system tasks configured for that HMI. The attacker might also be able to execute arbitrary code or obtain full access to files on the HMI system.	

			Environmental Vectors			
Chemical Sector Component or Subsystem	Purposes	Status & Controls	Up/Down Stream Digital	Up/Down Stream Material Flows	Consequences	Environmental Factors
Programmable logic controllers (PLCs) 	PLCs generally have less computing power than DCSs and are more localized to the processes they monitor and control, but these distinctions are getting less with newer microprocessor capabilities. Normally communicate using copper conductors but many newer PLCs support wireless communications. Digital logic and signal processing systems for autonomous or aided control of process equipment, apparatus and data acquisition systems • Collect inputs from analog field devices, such as level, temperature, pressure, flow transmitters and digital field devices such as relays, , on/off, open/closed and the quality of power, system voltages, thermal conditions, switch positions • Collect inputs (analog/digital) for control algorithms of physical assets • Control process operations to maintain stable condition, and to maintain safe and stable conditions during and process upsets • Manage the sequence of operations for complex or batch process operations				Refer to the Chemical Sector Component or Subsystem which uses this component	

			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
Data Historians 	Collect and archive process data (analog/digital) and serve it back to upstream process users or downstream business users. Data historians are typically computers configured as servers and operate similar to other database servers with the exception that they may have a higher availability requirement.	Status and controls are similar to other database applications.	Upstream Communications: Receive data from chemical process systems. Can be real-time or near-real-time Downstream Communications: Serve process data to remote locations for use by production planners, business, regulatory agencies, etc.	Data historians generally have no direct impact on material flows.	Monetary: if fined for no logging data by regulatory agency Physical Damage, personal injury or pollution: unlikely Loss of Confidentiality: state based potential for energy market advantage Loss of Integrity: if spoofed, modified or erased by attackers; Spoofed situation awareness, state estimation feeds resulting in bad operator actions Loss of Availability: maybe all erased for difficult forensics Reputation: Public loss of confidence in local systems or sector	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Chemical Plant Subsystem: Data Historian % in Subsystem: 50% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

Transportation Systems

<table>
<tr><td></td><td></td><td></td><td colspan="4">Environmental Vectors</td></tr>
<tr><th>Chemical Sector Component or Subsystem</th><th>Purposes</th><th>Status & Controls</th><th>Up/Down Stream Digital</th><th>Up/Down Stream Material Flows</th><th>Consequences</th><th>Environmental Factors</th></tr>
<tr>
<td>Chemical Transport (rail, trucks, ships, aircraft)






</td>
<td>Move raw materials to the chemical facility.

Move chemical products to bulk storage warehouses, retail facilities and end users.

Move wastes to treatment, storage and disposal facilities or recycle facilities.

• Tracking inventory, storage, and movement of chemical products;
• Storing customer information, including products that are bought on a regular basis and the locations where they are typically sent;</td>
<td>Status:
• temperature
• flows
• Level monitoring
• Weight
• GPS location
• Radio communication with dispatchers

Controls:
• Protection systems, such as Leak detection</td>
<td>Upstream Communications
• Radio communication with dispatchers
• Chemical Storage (manufacturer, warehouse/tankage, retail sales)

Local Communications
• Local tank weighing systems
• GPS tracking of vehicles and/or chemical containers
• Radio communication with dispatchers

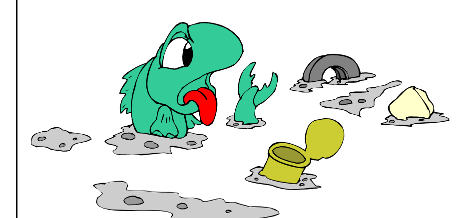
Downstream Communications
• Radio communication with dispatchers
• Chemical Storage inventory(warehouse/ tankage, retail sales
• Tracking inventory, storage, and movement of chemical products
• GPS tracking of vehicles and chemical containers</td>
<td>Upstream/Downstream:
• Transportation of bulk or small quantities
• Transportation to/from distribution centers
• Transportation to/from
• major industrial centers
• Transportation to
• retail centers</td>
<td>Monetary: if fined for no logging data

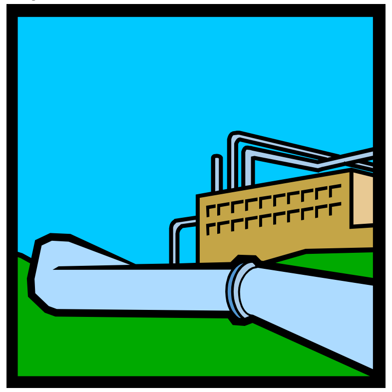
Physical Damage, personal injury or pollution: Wrecks leading to chemical spills may have collateral damage if material is flammable, toxic, pressurized, etc.

Loss of Confidentiality: low

Loss of Integrity: low

Loss of Availability: low

Reputation: Public loss of confidence in local systems or sector</td>
<td>CDP Collateral Damage Potential
N | L | LM | MH | H | ND
TD Target Distribution
Component: Chemical Plant
Subsystem: Data Historian
% in Subsystem: 50%
N | L | M | H | ND
CR System Confidentiality Requirement
L | M | H | ND
IR System Integrity Requirement
L | M | H | ND
AR System Availability Requirement
L | M | H | ND
</td>
</tr>
</table>

			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
Chemical Transportation Pipeline 	Chemical pipelines may be used to transport liquids, solids or gases from one chemical facility to another, or from a mine to a chemical facility. These are not as common as oil and gas pipelines and generally only extend to local areas rather than spanning across multiple states. These serve the same function as oil and gas pipelines and have similar digital communications and controls.	Status: • temperature • flows • valve positions • leak detection Controls: • remote pumping stations • remove valves	Upstream Communications: • With field devices using ICS protocols Downstream Communications: • With master control systems or SCADA systems using a combination of ICS and networking protocols • More likely to have wireless communication than in-plant chemical systems.	•	Monetary – losses from nuisance shut downs Physical Damage - depends upon the size of the pipeline, chemical hazards (toxicity, reactivity, flammability, explosivity), chemical state (gas, liquid, solid, pressure/temperature) • Fire or explosion • Loss of life or injury to personnel • Damage to the environment • Collateral damage to nearby areas likely, but will be limited to a local area Loss of Confidentiality - is low Loss of Integrity – can be low to high depending on the chemical and plant systems (e.g. integrity requirement can be medium to high for process safety systems, and air and water emissions monitoring systems) Loss of Availability – Timely status of process variables, alarms and safety systems is critical for safe and stable operation Reputation: Public loss of confidence in local systems or sector	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Chemical Transportation Subsystem: Chemical Pipelin % in Subsystem: <10% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND
Remote Terminal Units (RTU) manage digital and analog inputs/outputs from remote areas, such as pipeline pumping and monitoring stations, converting these signals to proper units for display at master control systems or SCADA systems at a control room. More likely to have wireless communication than in-plant chemical systems.	Digital logic and signal processing systems for autonomous or aided control of pipeline pumping station equipment, apparatus and data acquisition systems • Collect inputs (analog/digital) for control algorithms of physical assets • Control opening and closing of valves • Control operation of pumps • Monitor pressure, temperature,		Upstream Communications: • With field devices using ICS protocols Downstream Communications: • With master control systems or SCADA systems using a combination of ICS and networking protocols • More likely to have		Refer to the Chemical Pipeline Consequences	

			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
	flow and valve positions • Manage the sequence of operations for complex valving/ distribution arrangements		wireless communication than in-plant chemical systems.			

Warehousing and Storage Systems (aka Storage for Distribution and Sales)

<table>
<tr><th></th><th></th><th></th><th colspan="4">Environmental Vectors</th></tr>
<tr><th>Chemical Sector Component or Subsystem</th><th>Purposes</th><th>Status & Controls</th><th>Up/Down Stream Digital</th><th>Up/Down Stream Material Flows</th><th>Consequences</th><th>Environmental Factors</th></tr>
<tr>
<td>Distribution System and Sales Chemical Storage



</td>
<td>Large facilities that store or use bulk quantities of chemicals in sufficient quantities to pose risk to off-site facilities and personnel and the general public

These may be in other industry sectors, such as agriculture, food processing, and water/wastewater.

Packaged chemicals may be in bulk tanks or in individual packaging ready for transportation (e.g. supersacks, drums, gas cylinders, totes)</td>
<td>Status:
• Temperature, level and/or pressure monitors
• Flows into/out of bulk storage tanks.

Protection systems:
• Leak detection
• Level monitoring and alarm</td>
<td>Up/Down Stream
• Digital Communications: Likely to use few digital communications off-site

Local Communications:
• Field devices at the bulk storage tanks or packaged chemical storage pads may communicate with a local controller or local safety systems/ alarms
• Local safety systems may be linked to control automatic valves, switches, pump relays or fire suppression systems.</td>
<td>Upstream:
• Transportation System

Downstream:
End use application</td>
<td>Monetary: Low

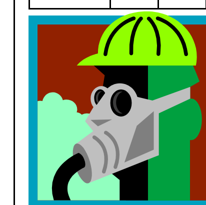
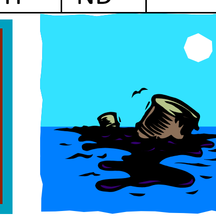
Physical Damage, personal injury or pollution: Low since only a small percentage of Warehousing and Storage facilities are expected to be impacted by cyber attack.

Target Distribution: Very low since only a small percentage of chemical users have sufficient quantities of hazardous chemicals to cause off-site consequences.

Loss of Confidentiality: Not defined for cyber impact

Loss of Integrity: Not defined for cyber impact

Loss of Availability: Not defined for cyber impact

Reputation: Public loss of confidence in local systems or sector</td>
<td>
<table>
<tr><td>CDP</td><td colspan="6">Collateral Damage Potential</td></tr>
<tr><td></td><td>N</td><td>L</td><td>LM</td><td>MH</td><td>H</td><td>ND</td></tr>
<tr><td>TD</td><td colspan="6">Target Distribution</td></tr>
<tr><td></td><td>N</td><td>L</td><td>M</td><td>H</td><td>ND</td><td></td></tr>
<tr><td>CR</td><td colspan="6">System Confidentiality Requirement</td></tr>
<tr><td></td><td>L</td><td>M</td><td>H</td><td>ND</td><td></td><td></td></tr>
<tr><td>IR</td><td colspan="6">System Integrity Requirement</td></tr>
<tr><td></td><td>L</td><td>M</td><td>H</td><td>ND</td><td></td><td></td></tr>
<tr><td>AR</td><td colspan="6">System Availability Requirement</td></tr>
<tr><td></td><td>L</td><td>M</td><td>H</td><td>ND</td><td></td><td></td></tr>
</table>


</td>
</tr>
</table>

Chemical End Users

			Environmental Vectors			
Chemical Sector Component or Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Material Flows**	**Consequences**	**Environmental Factors**
Large Scale Chemical User 	Large facilities that store or use bulk quantities of chemicals in sufficient quantities to pose risk to off-site facilities and personnel and the general public These may be in other industry sectors, such as agriculture, food processing, and water/wastewater.	Depends upon the sector.	Likely to use few digital communications	Upstream: • Transportation System Downstream: • End use application	Monetary: insignificant Physical Damage, personal injury or pollution: Low since only a small percentage of end user facilities are expected to be impacted by cyber attack. Target Distribution: Very low since only a small percentage of chemical users have sufficient quantities of hazardous chemicals to cause off-site consequences. Loss of Confidentiality: Not defined for cyber impact Loss of Integrity: Not defined for cyber impact Loss of Availability: Not defined for cyber impact Reputation: Not defined for cyber impact	**CDP** Collateral Damage Potential N, L, M, MH, H, ND **TD** Target Distribution N, L, M, H, ND **CR** System Confidentiality Requirement L, M, H, ND **IR** System Integrity Requirement L, M, H, ND **AR** System Availability Requirement L, M, H, ND
Small Scale Chemical User	Small facilities and consumers that use small quantities of chemicals where there is low risk to off-site facilities and personnel or the general public	Little or no digital monitoring or controls.	Little or no digital communications.	Upstream: • Storage for Distribution and Sales. • User transportation to usage location. Downstream: • Disposal of excess/Unused chemicals to disposal facilities or the environment.	Monetary: None for cyber impact. Physical Damage, personal injury or pollution: None for cyber impact. Target Distribution: Almost no small scale chemical users can be impacted by cyber vulnerabilities. Loss of Confidentiality: ND Loss of Integrity: ND Loss of Availability: ND Reputation: None	**CDP** Collateral Damage Potential N, L, LM, MH, H, ND **TD** Target Distribution N, L, M, H, ND **CR** System Confidentiality Requirement L, M, H, ND **IR** System Integrity Requirement L, M, H, ND **AR** System Availability Requirement L, M, H, ND

Critical Infrastructure: Water Sector

Water Sector includes both water supply and distribution systems (see Figure E-2) and wastewater collection and treatment systems (see Figure E-3). The water sector is one of the critical lifeline sectors due to the importance for the public to have a continuous supply of clean water for public health and safety.

This appendix contains a Water Sector Consequence Table for the each of the two main functional areas of the water sector and these tables list the major components and subsystems typically present in these systems.

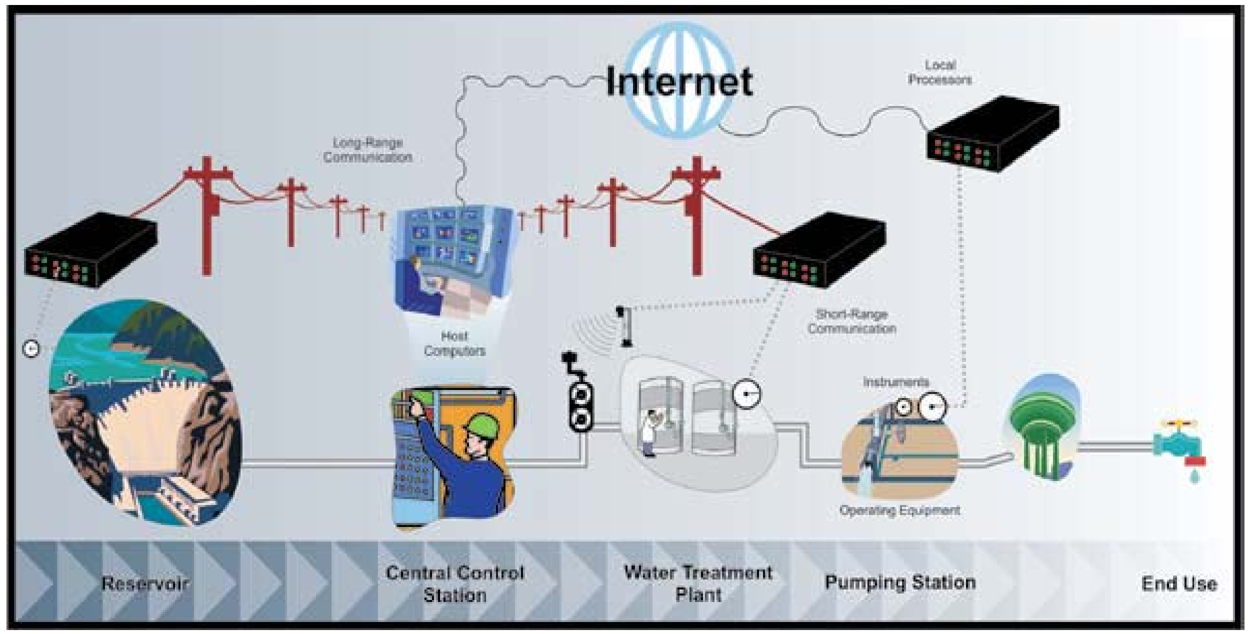


Figure E-2. Typical Components in a Water-Sector Control System (Courtesy GAO 07-1036)

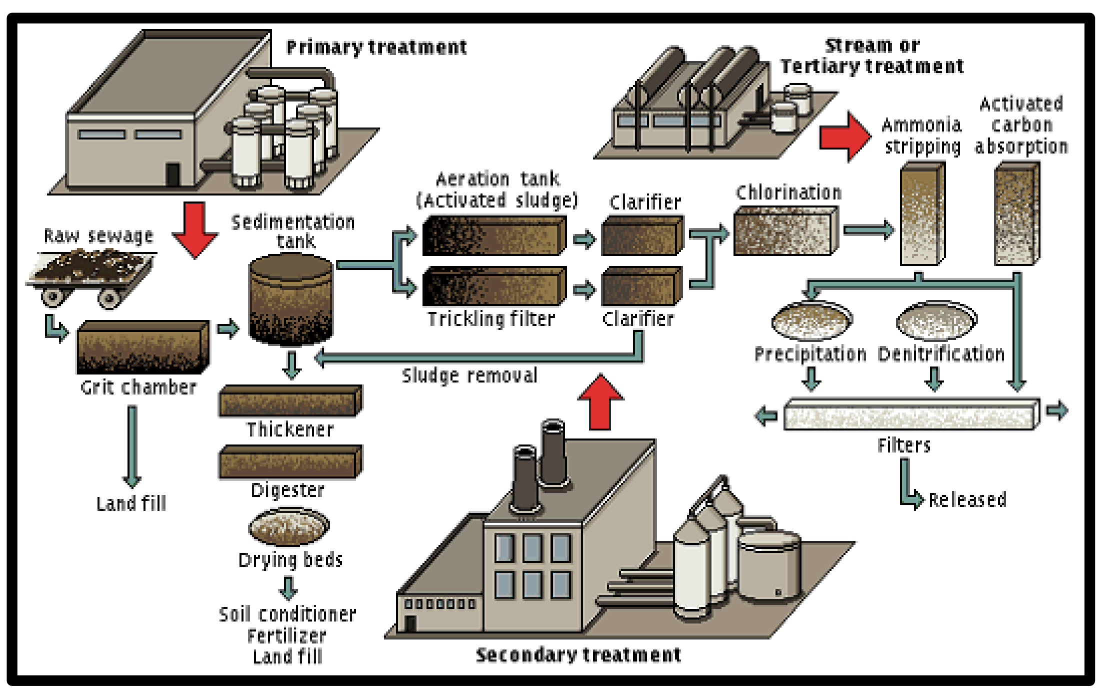


Figure E-3. Typical Components in a Wastewater-Treatment System (cityoflewisville.org)

The Applications subsection describes the functions that maybe implement in any other of the subsystems. Due to the nature of the nature of water systems, not all applications' status and control are digital. Older electro mechanical status and control are common on older subsystems and can still be found in some areas. Other newer components will be digital control and status. The headings of the Water Sector Consequence Table are described as follows:

- Water Sector Functional Area Component/Subsystem: Scope of apparatus discussed.
- Purpose: Descriptions of the functional roles the subsystems and components in water sector systems.
- Status & Controls: Distinction between typical status and control mechanisms. While no communications is strictly one way in a cyber security view (host computer someplace to impact communications), status is generally from the component into the larger subsystems, and control acts on the status(es) or a command from an operator from the subsystem to the component.
- Digital Flows: Show the data network connectivity between the component to other subcomponents to larger subsystems, and control centers. If other control is not digital, then manual functions or controls are provided to assist with determinations. Manual or local controls may work independently of a digital system, such as a pressure relief valve or float that shuts off valves on high tank level or a float sensor/valve and relay that turns on a sewage lift pump upon high level in a wastewater collection tank.
- Material Flows: Describes the physical connectivity of water systems independent from data communications.
- Consequences: This column follows the same logic as the Environmental Factors in the CVSS 2.0 with Monetary and Reputation also summarized for impact.

The CVSS 2.0 Environmental Factor categories scored in Table C-1 have the following options:

- **Metric:** CDP = Collateral Damage Potential (Organization specific potential for loss)
  Possible Values: N = None, L = Low, LM = Low-Medium, MH = Medium-High, H = High, ND = Not Defined
- **Metric:** TD = Target Distribution (Percentage of vulnerable systems)
  Possible Values: N = None (0%), L = Low (1-25%), M = Medium (26-75%), H = High (76-100%), ND = Not Defined
- **Metric:** CR = System Confidentiality Requirement (draft proposal)
  Possible Values: L = Low, M = Medium, H = High, ND = Not Defined
- **Metric:** IR = System Integrity Requirement (draft proposal)
  Possible Values: L = Low, M = Medium, H = High, ND = Not Defined
- **Metric:** AR = System Availability Requirement (draft proposal)
  Possible Values: L = Low, M = Medium, H = High, ND = Not Defined

Evaluation Assumptions for Environmental Factors are as follows, given that the highlighted scoring in the tables for the Water Sector are based upon worst case scenarios for a given subsystem or component:

- Collateral Damage Potential: The consequence discussion includes monetary and physical damage, which can be related to the subjective rating in collateral damage potential. Some components have large monetary value, the potential for causing illness in the general public or the potential for damage to the real world environment (e.g. pollution of surface water) if physically damaged, while other components may have little or no damage potential and be easier to replace (e.g. a water flow meter or a historian database). If the damage potential is very localized, then the rating would be lower (e.g. failure of a single controller or water treatment plant component versus major plant damage causing a major fire, explosion or toxic material leak that affects an entire plant, surrounding communities and waterways).
- Target Distribution: Not all subsystems and components are digital and will have a cyber impact (e.g. manual valves do not have an embedded digital system). To understand the Environmental Factors, the maximum impact based on the limited information available, is represented in the Target Distribution factor. For example, the number and extent of digital and cyber control systems versus manual operation of systems in a water system depends on numerous factors such as number of customers, size of regional area supported, ages of piping and control systems, process complexity and level of regulatory oversight. Small water or wastewater utilities are likely to use fewer digital systems than large, large utilities with widely distributed systems, so are less likely to be impacted by a cyber attack, and being smaller, are also less likely to have a regional impact in the case of a physical attack. Cyber system target distribution is also affected by the market penetration of a vendor in a particular critical infrastructure sector. For example, if an industrial control system component from vendor X that is found to have an exploitable vulnerability, then there would be a cyber impact on only the small portion of water utilities that use this vulnerable system component from vendor X. Government data on water and wastewater utilities, market surveys, installation specifics and subject matter experts will be needed to better understand and quantify the environmental factors.
- System Confidentiality: For the state and temporal nature of the chemical systems, confidentiality is a lesser concern unless dealing with customer data.
- System Integrity: The ability for operations to understand the correct state or situational awareness makes integrity a moderately important environmental factor for water sector systems.
- System Availability: Based on the need for people and industries to have a safe and reliable flow of potable water and to have a reliable means of treatment of sewage to protect people and the environment, availability an important environment factor for water sector control system components.

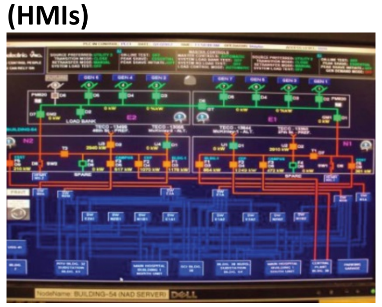
Water Treatment and Distribution

			Environmental Vectors			
Water Component / Subsystem	**Purpose**	**Status & Control**	**Digital Flows**	**Up/Down Stream Water Flows**	**Consequence**	**Environmental Factors**
Raw Water Supply  	The sources of water for human and industrial use include pumping from underground aquifers into storage tanks or collection from surface water, such as dams or rivers.	Raw water wells and pumping stations use industrial control systems to monitor and control inlet raw water flow and pressure. This includes: • Water quality monitoring (turbidity, pH, etc.) • Equipment status (On/off status, equipment failure, run hours, etc.) • Raw water piping monitoring including pressure, head loss, etc. • Well and transfer pump control • Pump on/off control •	Upstream Communications – • Reservoir, storage tank and river level monitoring • Raw water flow meters Downstream Communications – • Well and transfer pump local (pressure switch) or remote (control relay) on/off control • Outlet diversion valve controls • Pressure regulators/ controllers	Upstream – • Raw water collection from rivers, lakes, and/or wells Downstream – • Raw water transfer to a water treatment plant	Monetary – losses from nuisance shut downs Physical Damage – possible flooding from failures, with impact dependent upon storage capacity. For large systems, personnel injury or death is possible Loss of Confidentiality - is low Loss of Integrity – is low Loss of Availability – Timely status of process variables, alarms and safety systems is critical for maintaining a continuous supply of raw water to treatment systems Reputation: Public loss of confidence in local systems or sector	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Water Supply Subsystem: Raw Water Supply % in Subsystem: <25% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Water Component / Subsystem	**Purpose**	**Status & Control**	**Digital Flows**	**Up/Down Stream Water Flows**	**Consequence**	**Environmental Factors**
Water Treatment Plant  *Aerial of South Water Treatment Plant*	Water treatment is a series of processes that treats water for human consumption. Treatment processes include the removal of particulates, chemicals, heavy metals and microbes and other biological contaminants. Filtration and disinfection (sodium hypochlorite, chlorination, ozone, and ultraviolet) of water is a common treatment method to remove suspended particulates and destroy potentially harmful bacteria, respectively. However, there are many other processes including sedimentation, aeration, corrosion control and odor control. .	Water treatment facilities use industrial control systems to monitor and control plant processes. This includes: • Water quality monitoring (turbidity, pH, etc.) • Equipment status (On/off status, equipment failure, run hours, etc.) • Process monitoring (plant production, filter head loss, etc.) • Chemical feed pump control • Backwash control • Plant flow control.	Upstream Communications– • Pressure regulators/ controllers • Water flow meters • Status from upstream utilities/ water suppliers Downstream Communications – • Distribution valve controls • Pressure regulators/ controllers • Water flow meters • Status to downstream utilities or consumers	Upstream – • Raw water production from rivers, lakes, and wells Downstream – • Water distribution system	Monetary: Revenue loss and regulatory fines from water contamination Physical Damage: Disabling or damaging treatment systems or opening bypass valves may cause water supply contamination impacting the water supply for all customers. This could lead to to customer equipment damage or illnesses from use of contaminated water. Worst case is contamination of the water supply for a major region or large city. Most large systems have backup or alternate systems for this reason. Loss of Confidentiality- is low Loss of Integrity: system valve positions, equipment status or field sensors spoofed or overridden Loss of Availability: - is high based on the need for people and industries to have a safe and reliable source of potable water. Reputation: if major contamination or loss of service	**CDP** Collateral Damage Potential N | L | LM | **MH** | H | ND **TD** Target Distribution Component: Water Supply Subsystem: Water Treatment Plant % in Subsystem: <25% N | **L** | M | H | ND **CR** System Confidentiality Requirement **L** | M | H | ND **IR** System Integrity Requirement L | **M** | H | ND **AR** System Availability Requirement L | M | **H** | ND
Water Distribution 	Pumping stations and distribution lines deliver potable water from the treatment plant to industry and the public	Treated water wells and pumping stations use industrial control systems to monitor and control inlet treated water flow and pressure. This includes: • Water flow control • Water quality monitoring (turbidity, pH, etc.) • Equipment status (On/off status, equipment failure, run hours, etc.) • Treated water piping monitoring including pressure, head loss, etc. • Booster transfer pump on/off control	Upstream Communications– • Pressure regulation • Water flow Local communications – with RTUs or SCADA systems that provide both upstream or downstream communications for the local system. Downstream Communications – • Distribution valve controls • Pressure regulation	Upstream – • Treated water production from rivers, lakes, and wells Downstream – • Treated water transfer to a water treatment plant	Monetary: Revenue loss and regulatory fines from water contamination Physical Damage: Disabling or damaging pumping or water mains could cause loss of water supply for the public. Worst case is loss of the water supply for a major region or large city. Most large systems have backup or alternate systems for this reason. Loss of Confidentiality- is low Loss of Integrity: system valve	**CDP** Collateral Damage Potential N | L | LM | **MH** | H | ND **TD** Target Distribution Component: Water Supply Subsystem: Water Treatment Plant % in Subsystem: <25% N | **L** | M | H | ND **CR** System Confidentiality Requirement **L** | M | H | ND **IR** System Integrity Requirement L | **M** | H | ND **AR** System Availability Requirement

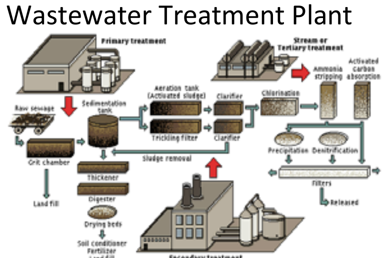
			Environmental Vectors			
Water Component / Subsystem	**Purpose**	**Status & Control**	**Digital Flows**	**Up/Down Stream Water Flows**	**Consequence**	**Environmental Factors**
		• Distribution valve controls • Pressure control •	• Booster transfer pump on/off control • Distribution valve controls • Pressure regulation		positions, equipment status or field sensors spoofed or overridden Loss of Availability: - is high based on the need for people and industries to have a safe and reliable source of potable water. Reputation: if major contamination or loss of service	L / M / H / ND
Remote Terminal Unit (RTU) 	Remote Terminal Units (RTU) manage digital and analog inputs/outputs converting these signals to proper units for display at a master control systems or SCADA systems. RTUs are normally located in remote locations so must have some type of long range communication system (wired or wireless).	Digital logic and signal processing systems for autonomous or aided control of substation equipment, apparatus and data acquisition systems • Collect inputs (analog/digital) for control algorithms of physical assets • Control reclosing and reconfiguration operations during and after a fault condition • Monitor power levels and the quality of power, system voltages, thermal conditions, switch positions • Operators can send control commands to RTUs to change water flow or pressure setpoint limits remotely to manage system upsets or in response to changes in supply or demand. • Manage the sequence of operations for complex switching arrangements	Upstream Communications: • With field devices using ICS protocols Downstream Communications: • With master control systems or SCADA systems using a combination of ICS and networking protocols • RTUs use a variety of communications media for communications to/from SCADA systems and control centers. Older systems will communication via traditional ICS protocols over one or more of leased telephone lines, public telephone lines, radio and/or satellite links. Newer systems may use protocol converters to ransmit traditional ICS/SCADA communications over TCP/IP-based networks.		Refer to the Consequences for Component or Subsystem which uses this component	**CDP** Collateral Damage Potential N / L / LM / MH / H / ND **TD** Component: Water Supply Subsystem: Water Treatment Plant % in Subsystem: <25% Component: Water Supply N / L / M / H / ND **CR** System Confidentiality Requirement L / M / H / ND **IR** System Integrity Requirement L / M / H / ND **AR** System Availability Requirement L / M / H / ND
Supervisory Control and Data Acquisition (SCADA) Systems	Collection of remote status from multiple locations normally report. The SCADA system has a situational status display, historian of statuses and operator actions, normally geolocation specifics of the remote components and serves as the overall operations of the complex systems	Status received by many digital control systems, RTUs, other data sources and other SCADAs which are displayed on large one-line or other visual board for operations with many other sub displays to aid the operators including alarms and alerts.	Upstream communications to control centers, or other SCADA systems may one or more traditional industrial control protocol over a mixture of communications media, such as packet switched telephone	SCADA control and provides operational status for the water distribution and wastewater collection systems	Monetary: Large potential impact if networked nature of SCADA used for wide impact. Physical Damage: Attacks on specific operations may cause physical damage (i.e. damage to pumping stations resulting in loss	**CDP** Collateral Damage Potential N / L / LM / MH / H / ND **TD** Target Distribution Component: Water Supply Subsystem: Water Treatment Plant % in Subsystem: <25%

			Environmental Vectors			
Water Component / Subsystem	**Purpose**	**Status & Control**	**Digital Flows**	**Up/Down Stream Water Flows**	**Consequence**	**Environmental Factors**
	upon systems operations very common in water distribution and wastewater collection systems. SCADA systems obtains information from other digital control systems, PLCs, RTUs, and other sources, resolves that data to the system's status, acts upon urgent needs for the health and ongoing operations (must times automatically), allows for operator control of the systems, sends control commands to remote systems, records actions, enables a human in the loop operations, uses status for predictive forecast allowing for more efficient control.	Control: Control pumps and valves to match water supply with demand.	modems, virtualized private networks isolated on the internet, private networks, cellular, radio, satellite. More modern systems will use protocol converters to transmit traditional ICS/SCADA communications protocols over TCP/IP-based networks. Local Communications - Local area network for the control system connecting the HMI, historian, engineering workstations together may use both TCP/IP and industrial control protocols (OPC, DNP, Modbus, FieldBus). Downstream communications - to the control devices, other embedded microcontrollers, PLCs, or RTUs may be TCP/IP based but more commonly serial or low latency communications.		of system pressure that may allow contamination to enter the water system or complete loss of the water supply Loss of Confidentiality: Markets, use supply and usage projections to determine prices Loss of Integrity: State estimation, contingency analysis, reliability systems require integrity of data Loss of Availability: potential loss of natural gas supply to users if degraded system is unnoticed by operations with potential for wide spread regional impact. Reputation: Public loss of confidence in water and wastewater utilities.	N L M H ND **CR** System Confidentiality Requirement L M H ND **IR** System Integrity Requirement L M H ND **AR** System Availability Requirement L M H ND
Water utility control centers  	Pipeline control centers have overall monitoring/control via SCADA, with DCS feedback controls internal to the center.	Status received by many digital control systems, RTUs, other data sources and other SCADAs which are displayed on large one-line or other visual board for operations with many other sub displays to aid the operators including alarms and alerts. Controls are sent to pumping stations and RTUs to match supply with demand. .	Upstream communications with remote SCADA systems, RTUs PLCs or smart field devices with embedded microprocessors. Local Communications - Inside the local area network for the control system connecting the HMI, historian, engineering workstations together may be a typical TCP/IP network but use more UDP or stateless communications for low latency protocols such as (DNP, Modbus, FieldBus).	Operators maintain control of water flows within their utility distribution area or region from local or remote control rooms.	Monetary: SCADA data feeds connect to energy markets providing potential for large monetary impacts; Large potential impact if networked nature of SCADA used for wide impact. Physical Damage: Attacks on specific operations will cause physical damage (i.e. damage resulting in fires or explosions at pumping stations. Loss of Confidentiality: Markets, use supply and usage projections to determine prices Loss of Integrity: State estimation,	**CDP** Collateral Damage Potential N L LM MH H ND **TD** Target Distribution Component: Water Supply Subsystem: Water Utility Control Center % in Subsystem: <25% N L M H ND **CR** System Confidentiality Requirement L M H ND **IR** System Integrity Requirement L M H ND **AR** System Availability Requirement L M H ND

			Environmental Vectors			
Water Component / Subsystem	**Purpose**	**Status & Control**	**Digital Flows**	**Up/Down Stream Water Flows**	**Consequence**	**Environmental Factors**
			Downstream communications –personnel or automation systems at the control center monitor the data from the RTUs and send control commands back to the RTU's if needed. Downstream communications - are to data historians and business data users.		contingency analysis, reliability systems require integrity of data Loss of Availability: potential loss of natural gas supply to users if degraded system is unnoticed by operations with potential for wide spread regional impact. Reputation: Public loss of confidence in natural gas utilities.	
Human Machine Interfaces (HMIs) 	HMIs are computers running software packages and are used as an interface between the operator and the Industrial Control Systems (SCADA systems, PLCs, DCSs, RTUs, etc.) controlling one or more process or system. HMIs perform the following tasks: • System visualization, • Operator control of the system, • Alarm display and acknowledgement, • System value and alarm archiving, and • Machine parameter management HMIs are used in nearly all industries with Industrial Control Systems, including power, water and wastewater, oil and gas, and chemical.				Refer to the Component or Subsystem which uses the affected HMI for consequences of loss of HMI view or control for that Component or Subsystem for additional consequences Successful exploitation of an HMI vulnerability could allow an attacker to log on to a vulnerable HMI as a user or administrator, where they would be able to perform any of the system tasks configured for that HMI. The attacker might also be able to execute arbitrary code or obtain full access to files on the HMI system. This could cause: • False view of the treatment system operations and equipment • Nuisance operation of pumps and valves, controlling water movement and treatment injection through the system • False view of the quality of the water; operators may over or undertreat water • Possible equipment failure • Production that does not meet water quality standards. • Depending on failure, potential impact to some industries from loss of water flow	Refer to the environment factor scores for the component or subsystem that uses the affected HMI.

Wastewater Collection and Treatment

			Environmental Vectors			
Wastewater Component / Subsystem	**Purpose**	**Status & Control**	**Digital Flows**	**Up/Down Stream Wastewater Flows**	**Consequence**	**Environmental Factors**
Wastewater Collection	Sumps and sewage piping collect wastewater from industry and the public in to main lines for gravity flow to lift stations and the wastewater treatment plant.	Sewage collection systems status is primarily monitoring of wastewater flows sump high level alarms This includes: • Wastewater flowrate monitoring and alarms • Sump high level alarms • Stormwater segregation and diversion control	Upstream Communications– • Pressure regulation • Water flow Local communications – with RTUs or SCADA systems that provide upstream and/or downstream communications for the local system. Downstream Communications – • Distribution valve controls • Pressure regulation • Booster transfer pump on/off control • Distribution valve controls • Pressure regulation	Upstream – • Treated water production from rivers, lakes, and wells Downstream – • Treated water transfer to a water treatment plant	Monetary: Cleanup costs and regulatory fines from wastewater contamination or physical damage to businesses or homes Physical Damage: Disabling protective sensors (sewage pressure and level rise) may cause wastewater contamination or physical damage to businesses or homes. Loss of Confidentiality- is low Loss of Integrity – is low Loss of Availability: - is high based on the continuous need for people and industries to have a means of sewage collection and transfer Reputation: if major contamination or loss of service	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Wastewater Subsystem: Wastewater Collection % in Subsystem: <25% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Wastewater Component / Subsystem	**Purpose**	**Status & Control**	**Digital Flows**	**Up/Down Stream Wastewater Flows**	**Consequence**	**Environmental Factors**
Sewage Lift Station  	Sewage lift stations with collection sumps are used to transfer wastewater from low-lying areas back into the main sewage lines where it can gravity flow to the wastewater treatment plant.	Sewage lift stations status monitoring includes: • Sump high level alarm • Lift pump manual or automatic on/off control	Upstream Communications – • Wastewater inlet flow Downstream Communications – • Sewage lift station controls • Stormwater overflow diversion control •	Upstream – • Sewage collection lines and sumps Downstream – • Wastewater flow into main sewage lines to wastewater treatment plant.	Monetary: Cleanup costs and regulatory fines from wastewater contamination or physical damage to businesses or homes Physical Damage: Disabling protective sensors (sewage pressure and level rise); or disabling lift pump controls may cause wastewater contamination or physical damage to businesses or homes Loss of Confidentiality- is low Loss of Integrity: system pressure or overflow sensors spoofed or overridden Loss of Availability: - is high based on the continuous need for people and industries to have a means of sewage collection and transfer Reputation: if major contamination or loss of service	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Wastewater Subsystem: Sewage Lift Station % in Subsystem: <25% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND
Wastewater Treatment Plant 	Wastewater treatment is a series of discrete types of processes that treat wastewater from industrial and human sources. Treatment processes include the removal of particulates, chemicals, heavy metals, microbes and other biological contaminants, removal of sediments. Sedimentation, aeration and filtration are common treatment methods to remove suspended particulates, break down biological wastes, control odors and remove contaminants. Final filtration is a common method to remove suspended particulates. Final disinfection of wastewater to destroy potentially harmful bacteria may be one or a combination of treatment with sodium hypochlorite, chlorine or ozone and/or exposure to ultraviolet light.	Wastewater treatment facilities use industrial control systems to monitor and control plant processes. This includes: • Equipment status (On/off status, equipment failure, run hours, etc.) • Process monitoring (plant production, unit to unit transfers, filter head loss, etc.) • Chemical feed pump control • Backwash control • Plant flow control • Wastewater discharge quality monitoring (turbidity, pH, metal and organic contaminants, etc.)	Upstream Communications – • Sewage lift station controls • Stormwater diversion control • Pressure regulation (generally for high-rise construction only) • Wastewater flow Downstream Communications – • Wastewater discharge flow and quality monitoring (turbidity, pH, BOD etc.) • Stormwater overflow diversion control • Data (usually not real time) to EPA, state or local regulators	Upstream – • Sewage collection lines and lift (pumping) stations Downstream – • Cleaned wastewater discharge • Treated wastewater solids disposal	Monetary: Cleanup costs and regulatory fines from surface water contamination Physical Damage: Disabling or damaging treatment systems or opening bypass valves will cause surface water contamination, and may impact downstream surface water users. Worst case is loss of sewage treatment for a major region or large city leading to a major sewage discharge Loss of Confidentiality- is low Loss of Integrity: system valve positions, equipment status or field sensors spoofed or overridden Loss of Availability: - is high based	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Wastewater Subsystem: Wastewater Treatment Plant % in Subsystem: <25% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Wastewater Component / Subsystem	**Purpose**	**Status & Control**	**Digital Flows**	**Up/Down Stream Wastewater Flows**	**Consequence**	**Environmental Factors**
					on the need for people and industries to have a safe and reliable means of treatment of sewage to protect people and the environment, availability an important environment factor for water sector control system components Reputation: if major contamination or loss of service	

The Natural Gas Industry in the U.S. consists of a large network of pipelines that collect raw natural gas from product areas, such as the Permian Basin in Texas, and distributes it by major region to large users, such as natural gas-fired power plants, and to smaller users, such as industries and homes. The figure below shows a basic representation of the major equipment and flow paths that make up the natural gas industry. The highly distributed nature of the systems require natural gas companies to rely on communications with a large number of remote systems to be able to monitor and control of the flow of natural gas.

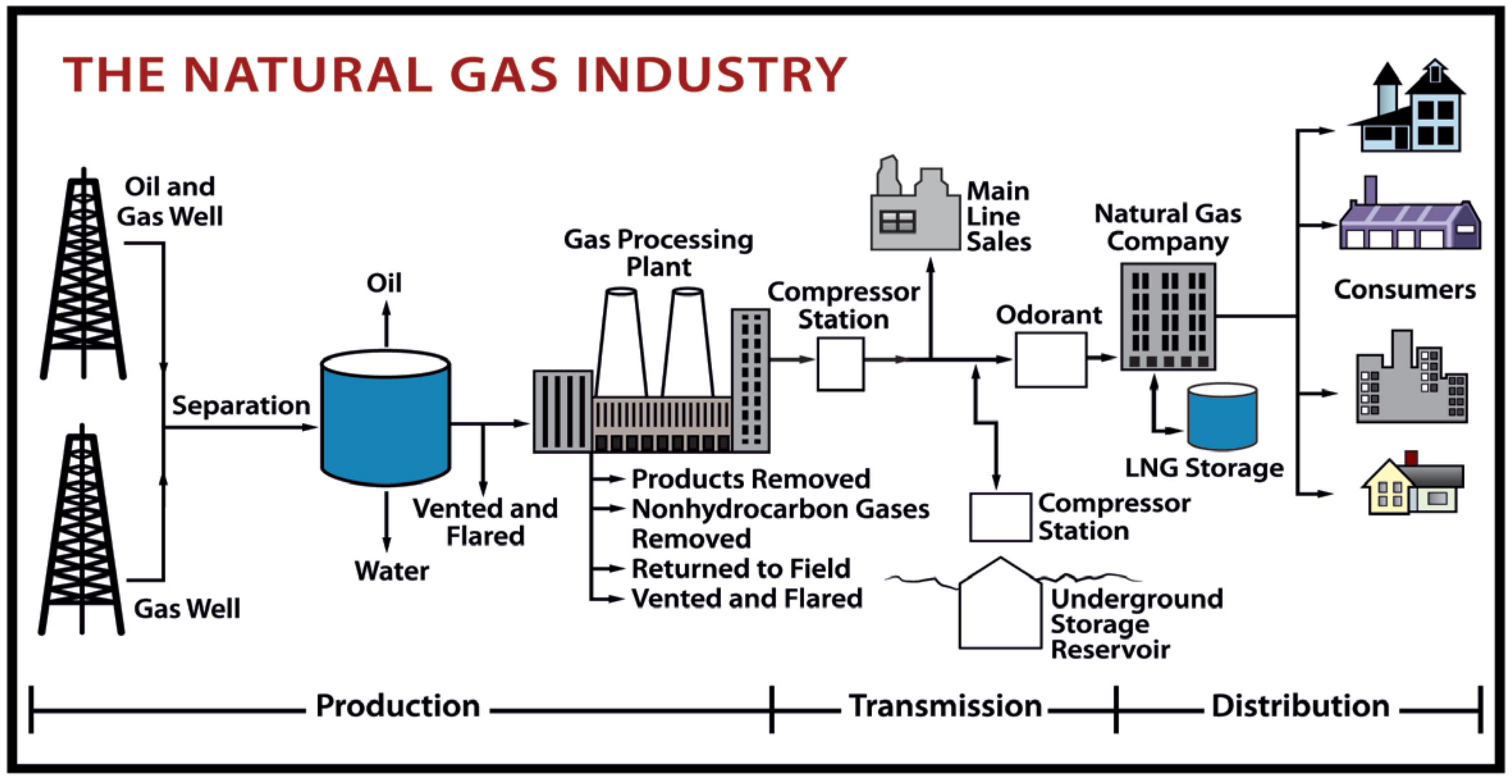


Figure E-4. Natural gas industry and its subsectors. (Courtesy: U.S. Energy Information Administration [EIA])

As depicted in the figure, the major components are:

- Production and Gas Processing
- Transmission
- Applications – SCADA, DCS, Specialized Equipment (RTU, PLC)
- Compressor Station(s)
- Main Line Sales
- Reservoir Storage
- Local Distribution Companies
- LNG Storage
- Consumers
- Energy Markets

The table in this appendix provides examples of vulnerability vectors and scoring for one major major component in the sector - natural gas transmission subsystems.. Tables for the other major components in the natural gas sector would be completed in a future effort, if desired by DHS. The Applications subsection describes the functions that maybe implement in any other of the subsystems.

The headings on the columns are described as follows:

- Natural Gas Component/Subsystem: Scope of apparatus discussed.
- Purpose: Role the component/subsystem provided in the natural gas industry.

- Status & Control: Distinction between typical status and control mechanisms. While no communications is strictly one way in a cyber security view (host computer someplace to impact communications), status is generally from the component into the larger subsystems, and control acts on the status(es) or a command from an operator from the subsystem to the component.
- Digital Flows: Show the data network connectivity from the component to subcomponents to larger subsystems, control centers, and SCADA/EMS. If other control is not digital, electro mechanical functions are noted to understand impact determinations. Electromechanical controls works on a level of voltage on a copper wire that when raised or decreased cause a mechanical function (i.e. tripping a breaker).
- Load/Utility Power Flow: Describes the connectivity of the electric grid physics independent from the data communications.
- Consequence: This column follows the same logic as the Environmental Factors in the CVSS 2.0 with Monetary and Reputation also summarized for impact.

Environmental Factor are listed from CVSS 2.0 below.

Common Vulnerability Scoring Systems Environmental Vectors

Metric: CDP = Collateral Damage Potential (Organization specific potential for loss)
Possible Values: N = None, L = Low, LM = Low-Medium, MH = Medium-High, H = High, ND = Not Defined

Metric: TD = Target Distribution (Percentage of vulnerable systems)
Possible Values: N = None (0%), L = Low (1-25%), M = Medium (26-75%), H = High (76-100%), ND = Not Defined

Metric: CR = System Confidentiality Requirement (draft proposal)
Possible Values: L = Low, M = Medium, H = High, ND = Not Defined

Metric: IR = System Integrity Requirement (draft proposal)
Possible Values: L = Low, M = Medium, H = High, ND = Not Defined

Metric: AR = System Availability Requirement (draft proposal)
Possible Values: L = Low, M = Medium, H = High, ND = Not Defined

Evaluation Assumptions for Environmental Factors

Collateral Damage Potential: The consequence discussion includes monetary and physical damage which can be related to the subjective rating in collateral damage potential. Some components have large monetary value if physically damaged (i.e. compressor stations), while other components may be easier to replace (i.e. historian database). If the damage potential is very localized, the rating would be lower (i.e. city distribution meter vs transmission breaker).

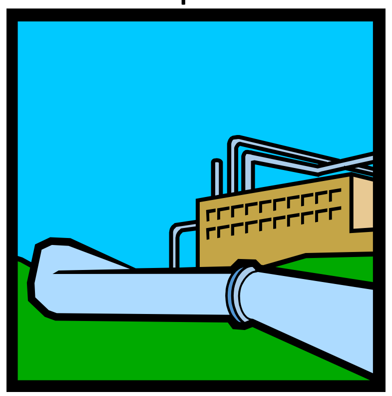
Target Distribution: Not all components are digital and will have a cyber impact (i.e manual pipeline valves do not have embedded processors). To understand the Environmental Factors, the maximum impact based on the limited information available, is represented in the Target Distribution factor. For example, SCADA systems are estimated to have a Target Distribution of nearly 100% since the distributed nature of the natural gas sector means that nearly all sector components have communications from remote SCADA systems to regional control centers and might have be vulnerable to cyber attack. However, there are a large number of vendors for SCADA systems, and if a SCADA system from vendor X had an exploitable vulnerability with an impact, then that would represent the small percentage of the industry that uses vendor X SCADA systems. Market surveys, installation specifics and subject matter experts will be needed to better understand the environmental factors.

System Confidentiality: For the state and temporal nature of the natural gas sector, confidentiality is a lesser concern unless dealing with customer data.

System Integrity: The ability for operations to understand the correct state or situational awareness makes integrity an important environmental factor for the natural gas sector.

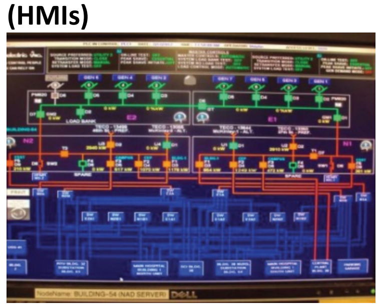
System Availability: Based on the safety and security needs of the natural gas sector, some command operations need to occur with minimum latency and in proper sequence with other actions making availability an important environment factor for control aspects of the natural gas sector.

Gas Transmission

			Environmental Vectors			
Natural Gas Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Gas Flows**	**Consequences**	**Environmental Factors**
Natural Gas Pipeline 	Natural Gas Pipelines transport bulk quantities of natural gas from producers to bulk users and local distributors. Oil and gas pipelines operations use have similar digital communications and controls.	Pipelines have remote terminal units at key locations along the pipeline. These contain industrial control systems that monitor and control the most important parameters Status: • temperature • pressure • flowrate • valve position • leak detection Controls: • remote monitoring • remove valves • manual valves	Upstream Communications: • With field devices using ICS protocols Downstream Communications: • With master control systems or SCADA systems using a combination of ICS and networking protocols • .	Upstream – • Gas processing plant • Additional Metering and Compressor Stations Downstream – • Additional Metering and Compressor Stations • Odorant insertion • Consumer distribution	Monetary – losses from nuisance shut downs Physical Damage - • Fire or explosion • Loss of life or injury to personnel • Collateral damage to nearby areas likely, but will be limited to a local area Loss of Confidentiality - is low Loss of Integrity –) Loss of Availability – Timely status of process variables, alarms and safety systems is critical for safe and stable operation Reputation: Public loss of confidence in local systems or sector	**CDP** Collateral Damage Potential N L LM MH H ND **TD** Target Distribution Component: Natural Gas Transmission Subsystem: Natural Gas Pipelin % in Subsystem: +50% N L M H ND **CR** System Confidentiality Requirement L M H ND **IR** System Integrity Requirement L M H ND **AR** System Availability Requirement L M H ND
Compressor Station 	Compressors act as "pumps" that provide additional internal pressure needed to maintain the flow of natural gas through a pipeline by controlling the pipeline pressure differential along the pipeline. Pipeline controllers set a desired pressure level and the compressor stations maintain that level without further intervention. Depending on the size or remoteness, compressor stations may be manned or unmanned.	Compressor stations contain industrial control systems that monitor and control the most important systems • Monitor pipe pressure • Monitor volumes through selected operational meters • Control the valves • Control number of compressors operating	Upstream Communications– • Pressure regulation • Scrubbing controls for sulfurous and other contaminants • Pipeline control center has overall monitoring/control via SCADA, with DCS feedback controls internal Downstream – • Distribution valves • Pressure regulation	Upstream – • Gas processing plant • Natural gas pipeline • Additional Metering and Compressor Stations Downstream – • Natural gas pipeline • Additional Metering and Compressor Stations • Odorant insertion • Consumer distribution	Monetary – losses from nuisance shut downs • Physical Damage - Fire or explosion • Nuisance failures and shut downs of subsystems • Operating outside of EPA and other regulatory requirements Loss of Confidentiality - is low Loss of Integrity – Loss of Availability – Timely status of process variables, alarms and safety systems is critical for safe and stable operation Reputation: Public loss of confidence in local systems or sector	**CDP** Collateral Damage Potential N L LM MH H ND **TD** Target Distribution Component: Gas Transmission Subsystem: Compressor Station % in Subsystem: 100% N L M H ND **CR** System Confidentiality Requirement L M H ND **IR** System Integrity Requirement L M H ND **AR** System Availability Requirement L M H ND
Remote Terminal Unit (RTU)	Remote Terminal Units (RTU) manage	Digital logic and signal processing	Upstream Communications:	RTUs collect operational	Refer to the Component or	**CDP** Collateral Damage Potential

			Environmental Vectors			
Natural Gas Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Gas Flows**	**Consequences**	**Environmental Factors**
	digital and analog inputs/outputs converting these signals to proper units for display at a master control systems or SCADA systems. RTUs are normally located in remote locations so must have some type of long range communication system (wired or wireless).	systems for autonomous or aided control of substation equipment, apparatus and data acquisition systems • Collect inputs (analog/digital) for control algorithms of physical assets • Control reclosing and reconfiguration operations during and after a fault condition • Monitor power levels and the quality of power, system voltages, thermal conditions, switch positions • Manage the sequence of operations for complex switching arrangements	• With field devices using ICS protocols Downstream Communications: • With master control systems or SCADA systems using a combination of ICS and networking protocols • RTUs use a variety of communications media for communications with SCADA systems and control centers. Older systems will use communications via traditional ICS protocols over leased telephone lines, public telephone lines, radio or satellite links. Newer systems may use conversion from ICS protocols to TCP/IP for communications.	status on gas flow and local control of systems. Operators can also change gas flow or pressure setpoints remotely to manage system upsets or in response to gas sales requests.	Subsystem which uses this component	N | L | LM | MH | H | ND **TD** Target Distribution Component: Gas Transmission Subsystem: RTU % in Subsystem: +90% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND

			Environmental Vectors			
Natural Gas Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Gas Flows**	**Consequences**	**Environmental Factors**
Supervisory Control and Data Acquisition (SCADA) Systems	Collection of remote status from multiple locations normally report. The SCADA system has a situational status display, historian of statuses and operator actions, normally geolocation specifics of the remote components and serves as the overall operations of the complex systems upon systems operations very common in natural gas transmission systems. SCADA systems obtains information from other digital control systems, PLCs, RTUs, and other sources, resolves that data to the system's status, acts upon urgent needs for the health and ongoing operations (must times automatically), allows for operator control of the systems, sends control commands to remote systems, records actions, enables a human in the loop operations, uses status for predictive forecast allowing for more efficient control.	Status received by many digital control systems, RTUs, other data sources and other SCADAs which are displayed on large one-line or other visual board for operations with many other sub displays to aid the operators including alarms and alerts. Control: Automatic Generation Control for generators, fault isolation, switching and breaker operations, operational set points for subsystems; status feed into the state estimators, contingency analysis systems, load balance calculations and energy markets which controls energy market decisions. Supervisory control for maintenance (i.e. taking asset offline for maintenance) or restoration.	Upstream communications to pipeline control centers, or other SCADA systems will include common protocols on traditional networks (packet switched telephone modems, virtualized private networks isolated on the internet, private networks, cellular, radio, satellite). Most networks will be IP (TCP/IP based and built on top of traditional ICS/SCADA communications protocols. Local Communications - Inside the local area network for the control system connecting the HMI, historian, engineering workstations together may be a typical TCP/IP network but use more UDP or stateless communications for low latency protocols such as (DNP, Modbus, FieldBus). Downstream communications - to the control devices, other embedded microcontrollers (PLC, RTU) may be TCP/IP based but more commonly serial or low latency communications.	SCADA control and provides operational status for the natural gas transmission systems	Monetary: SCADA data feeds connect to energy markets providing potential for large monetary impacts; Large potential impact if networked nature of SCADA used for wide impact. Physical Damage: Attacks on specific operations will cause physical damage (i.e. damage resulting in fires or explosions at pumping stations. Loss of Confidentiality: Markets, use supply and usage projections to determine prices Loss of Integrity: State estimation, contingency analysis, reliability systems require integrity of data Loss of Availability: potential loss of natural gas supply to users if degraded system is unnoticed by operations with potential for wide spread regional impact. Reputation: Public loss of confidence in natural gas utilities.	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Gas Transmission Subsystem: SCADA system % in Subsystem: +90% N | L | M | H | ND **CR** System Confidentiality Requirement L | M | H | ND **IR** System Integrity Requirement L | M | H | ND **AR** System Availability Requirement L | M | H | ND
Pipeline control centers 	Pipeline control centers have overall monitoring/control via SCADA, with DCS feedback controls internal to the center.	Status received by many digital control systems, RTUs, other data sources and other SCADAs which are displayed on large one-line or other visual board for operations with many other sub displays to aid the operators including alarms and alerts. Controls are sent to pumping stations and RTUs to match	Upstream communications with remoteSCADA systems, RTUs PLCs or smart field devices with embedded microprocessors. Local Communications - Inside the local area network for the control system connecting the HMI, historian, engineering	Operators maintain control of material flows within their pipeline segment or region from control rooms, and may have some monitoring and control over loading/unloading of material to/from transportation systems.	Monetary: SCADA data feeds connect to energy markets providing potential for large monetary impacts; Large potential impact if networked nature of SCADA used for wide impact. Physical Damage: Attacks on specific operations will cause physical damage (i.e. damage resulting in fires or explosions at	**CDP** Collateral Damage Potential N | L | LM | MH | H | ND **TD** Target Distribution Component: Chemical Plant Subsystem: Process Control Room % in Subsystem: +90% N | L | M | H | ND **CR** System Confidentiality Requirement

			Environmental Vectors			
Natural Gas Component / Subsystem	**Purposes**	**Status & Controls**	**Up/Down Stream Digital**	**Up/Down Stream Gas Flows**	**Consequences**	**Environmental Factors**
		supply with demand. .	workstations together may be a typical TCP/IP network but use more UDP or stateless communications for low latency protocols such as (DNP, Modbus, FieldBus). Downstream communications –personnel or automation systems at the control center monitor the data from the RTUs and send control commands back to the RTU's if needed. Downstream communications - are to data historians and business data users.		pumping stations. Loss of Confidentiality: Markets, use supply and usage projections to determine prices Loss of Integrity: State estimation, contingency analysis, reliability systems require integrity of data Loss of Availability: potential loss of natural gas supply to users if degraded system is unnoticed by operations with potential for wide spread regional impact. Reputation: Public loss of confidence in natural gas utilities.	L M H ND **IR** System Integrity Requirement L M H ND **AR** System Availability Requirement L M H ND
Human Machine Interfaces (HMIs) 	HMIs are computers running software packages and are used as an interface between the operator and the Industrial Control Systems (SCADA systems, PLCs, DCSs, RTUs, etc.) controlling one or more process or system. HMIs perform the following tasks: • System visualization, • Operator control of the system, • Alarm display and acknowledgement, • System value and alarm archiving, and • Machine parameter management HMIs are used in nearly all industries with Industrial Control Systems, including power, water and wastewater, oil and gas, and chemical.				Refer to the Component or Subsystem which uses the affected HMI for consequences of loss of HMI view or control for that Component or Subsystem for additional consequences Successful exploitation of an HMI vulnerability could allow an attacker to log on to a vulnerable HMI as a user or administrator, where they would be able to perform any of the system tasks configured for that HMI. The attacker might also be able to execute arbitrary code or obtain full access to files on the HMI system.	