CyTRICS Impact-Based Prioritization Process

February 8, 2023

CyTRICS™ Cyber Testing for Resilient Industrial Control Systems

U.S. DEPARTMENT OF ENERGY
OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Executive Summary

Cyber Testing for Resilient Industrial Control Systems™ (CyTRICS™) is the Department of Energy's (DOE's) program for cybersecurity vulnerability testing, digital subcomponent enumeration, and forensic assessment. CyTRICS leverages best-in-class test facilities and analytic capabilities at six DOE National Laboratories and strategic partnerships with key stakeholders including technology developers, manufacturers, asset owners and operators, and interagency partners.

During the program's development, CyTRICS established a unique methodology for prioritizing digital components within operational technology (OT) and industrial control systems (ICS) in the Energy Sector Industrial Base (ESIB) for cyber vulnerability testing. The CyTRICS prioritization process leverages multiple characteristics of systems, components, and their contextual deployment to calculate a quantification of individual digital components for CyTRICS testing. The initial version of the CyTRICS prioritization process was premised largely upon the impact which could result to an energy sector industrial control system if the digital component under testing was compromised, either through malicious means, faulty engineering, or other modes. CyTRICS has termed this process the "CyTRICS Impact-based Prioritization Process."

This paper describes the factors identified for use in the Impact-based Prioritization process and identifies the rationale for inclusion. During development, three National Laboratories piloted this prioritization process and generated prioritization scores for seven systems. Following the piloting of the process, laboratory subject matter experts (SME) validated that the numerical scores generated by the prioritization process were consistent with their knowledge of the impact that may occur should any of these systems be disrupted.

The following document explains how to perform the prioritization process to generate prioritization scores for energy sector systems. After outlining assumptions required to conduct the process, it describes how to identify and elicit data which can be leveraged to evaluate a system and assign numerical values for each factor. The prioritization process uses different weights on different factors; rationale for each weight is included within the paper. Additionally, the paper includes some recommendations for future enhancements to prioritization, including lessons learned from developing and piloting the process. Finally, a comprehensive appendix includes example documents to be leveraged by those looking to execute the prioritization process.

Acknowledgements

The Idaho National Laboratory and U.S. Department of Energy (DOE) acknowledges all stakeholders who participate in the CyTRICS program and who contributed input used in the development of this report.

Authors

Kent Orange Warner, Control Systems Cybersecurity Analyst, Idaho National Laboratory,

Anna Skelton, Control Systems Cybersecurity Analyst, Idaho National Laboratory,

Lori Ross O'Neil, Digital Cyber Security Project Manager, Pacific Northwest National Laboratory

Quinn Wright-Mockler, Cybersecurity Engineer, Pacific Northwest National Laboratory,

Rachel Samuels, Global Security Systems Analyst, Lawrence Livermore National Laboratory,

Alex Campbell, Systems Analyst, Lawrence Livermore National Laboratory,

Tom Edmunds, Principal Investigator, Systems and Decisions Sciences, Lawrence Livermore National Laboratory,

Virginia Wright, Energy Cyber Portfolio Manager, Idaho National Laboratory,

Adam Hahn, Principal Critical Infrastructure Security Engineer, MITRE Corporation,

Marie Collins, Manager, Mobile & Cyber-Physical Systems Technology, MITRE Corporation,

Deb Bodeau, Senior Principal Security Engineer, MITRE Corporation.

Contributors

Jeff Mitchell, Program Manager, Idaho National Laboratory,

Jessica Smith, Senior Cybersecurity Research Scientist, Pacific Northwest National Laboratory,

Robert Hanson, Deputy Associate Program Leader for Defense Infrastructure, Lawrence Livermore National Laboratory,

Lucas Tate, Data Scientist, Pacific Northwest National Laboratory,

Sean Gordon, National Security Systems Analyst, Lawrence Livermore National Laboratory,

Andrew Murray, Intern, Pacific Northwest National Laboratory.

Acknowledgements

Stephanie Johnson, Program Manager, Supply Chain Cyber Risk Management Program, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy

Cherylene Caddy, Senior Advisor for Cybersecurity, Office of Cybersecurity, Energy Security, and Emergency Response, U.S. Department of Energy,

Samuel Chanoski, Technical Relationship Manager, Idaho National Laboratory,

Carla Heathman, Electrical Engineer, Idaho National Laboratory,

Briam Johnson, Power Engineer, Idaho National Laboratory,

Robert Erbes, Senior Computer Security Researcher, Idaho National Laboratory.

Table of Contents

Terms and Definitions

Prioritization – the process of evaluating a system to determine its potential impact to overall energy stability, thereby establishing if CyTRICS should test a system and, if so, how soon.

Score – The process of compiling values provided by the SMEs for a system under consideration into the scoring instrument to generate a prioritization score.

Acronyms

CESER – Office of Cybersecurity, Energy Security, and Emergency Response

CFT – CyTRICS Facilitation Team

CyTRICS– Cyber Testing for Resilient Industrial Control Systems

DOE – Department of Energy

SME – Subject Matter Expert

Overview of Document

This document provides an overview of the Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) Impact-based Prioritization process. Prior to explaining the process, this document introduces CyTRICS and explains how Impact-based Prioritization fits into the objectives of CyTRICS. The document explains how to perform Impact-based Prioritization and presents the scales and definitions for each criteria used to generate a prioritization score. The appendices provide the tools necessary to conduct a prioritization session, calculate a score, and produce a prioritization report.

CyTRICS Introduction

The CyTRICS program is a DOE program to perform cybersecurity vulnerability testing and subsystem enumeration for equipment in the energy sector. Created in 2018, CyTRICS enhances the cyber resilience of highly critical equipment in the energy sector by partnering with stakeholders to identify high priority OT systems, perform expert testing, share information about vulnerabilities in the supply chain, and inform improvements in system design and manufacturing. The program leverages best-in-class test facilities and analytic capabilities across multiple DOE National Laboratories, as well as strategic partnerships with technology developers, manufacturers, asset owners and operators, and interagency partners. CyTRICS is led by the DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

The CyTRICS program's primary purpose is to perform testing to identify common mode vulnerabilities in high-impact energy sector systems[1] and responsibly disclose them to manufacturers who can develop patches or mitigations before adversaries can exploit them. Because testing is a time- and resource-intensive process, it is important for CyTRICS to test systems that are uniquely important to the security and reliability of the energy grid. The purpose of prioritization is to provide a repeatable methodology for identifying and ranking such systems.

Purpose

The purpose of this document is to describe the CyTRICS prioritization process, illustrating how CyTRICS executes a repeatable methodology to determine testing priorities. With this document, readers should have enough information to understand and perform the CyTRICS prioritization process. Researchers designed this process specifically for CyTRICS; CyTRICS makes no claim for applicability or transferability of this process to other programs or uses.

1. Section 1: Overview of Impact-based Prioritization

This section provides an overview of Impact-based Prioritization:

- Assumptions
- The prioritization process

[1] CyTRICS uses the term system as an all-encompassing term for hardware systems, software systems, and firmware as they are used throughout the energy sector.

- The prioritization team roles
- Assumptions
- Instruments and templates used for prioritization
- Value scales used for prioritization.

The CyTRICS program developed two methods for prioritizing systems for testing. the first method prioritizes OT systems based on the worst-case possible impacts to energy stability and is detailed in this paper. The second method prioritizes systems based on the potential for adversaries to gain strategic advantage, including process insights or system impact through unauthorized access, and will be addressed in a future paper. Both methods were developed in collaboration with MITRE. Impact-based prioritization allows systems to be evaluated without assuming actual or hypothetical adversary capabilities and attack methods.

1.1. Assumptions

This initial CyTRICS Prioritization process is built on a series of assumptions that must be addressed to accurately understand it's outputs. For example, CyTRICS Prioritization operates under the assumption that only first-order impacts are in scope for Prioritization. This assumption is communicated to SMEs prior to the scoring process. If a SME feels inclusion of second- or third- order impacts is needed to accurately score a system, they may make notation of this in the "notes" section; however, including this SME's score in the broader group of scores changes the model under which the score was developed, making direct comparisons between scores problematic. As a result, scores should not be directly compared, but rather used with context to frame the vitality of a system within a given environment. Ultimately, each scoring factor includes inherent assumptions that may affect scoring significantly. While the CyTRICS Prioritization is designed as a quantitative score, it is a score of a qualitative topic and process.

SMEs are chosen based on experience integrating and using the system being scored. They will have practical experience and knowledge of configuration details that are not accessible through desk research into the prioritization process. The CyTRICS process assumes selected SMEs are qualified to provide accurate scoring across all factors, which will not always be true, i.e. the knowledge of a power engineer in regards to the cyber security measures in place withing a system. In the electric sector, SMEs will be needed within power system operations, specifically engineers within protection and control groups. In the Oil and Natural Gas (ONG) sector, SMEs will be needed within operations, controls engineering, and automation engineering groups. CyTRICS conducts Prioritization with the assumption SMEs are more than tangentially familiar with the system.

As presented in this paper, the prioritization process does not leverage computer security subject matter experts. CyTRICS acknowledges the inclusion of computer security SMEs will influence the results of scoring. As the prioritization process continues to develop, CyTRICS will be looking at adding additional SME groups in the future.

To help SMEs document assumptions needed to contextualize the environment a system is being scored in, a reference architecture is used to define the presumed installation environment. Examples include distribution substations, transmission substations, and compressor stations. Operational use case assumptions define expected system functions, such as data aggregators in a control station or protective relays that monitor voltage and current.

For prioritization, CyTRICS assumes the more complex a system is, the higher potential for that system to contain vulnerabilities, which is tangentially related to impact. However, systems which support multiple configuration options which can increase or decrease complexity of a given deployment within the defined scenario should be evaluated by SMEs in a consistent manner. To achieve this, the prioritization team must assume a system to have the maximum number of capabilities possible enabled for that system.

For Impact-based Prioritization, CyTRICS does not assess feasibility or capabilities of threat actors. Instead, the process focuses on the impacts that could result from a failure regardless of the root cause. CyTRICS operates under the assumption that threat actors have the resources necessary to compromise any target, regardless of level of complexity. This assumption aims to focus SMEs on assessing the severity of the impacts as opposed to deliberating feasibility of a given attack.

Further assumptions will be documented and added to this document as Prioritization matures.

1.2. Prioritization Process

A CyTRICS Facilitation Team (CFT) performs the steps of the prioritization process shown in Figure 1 below.

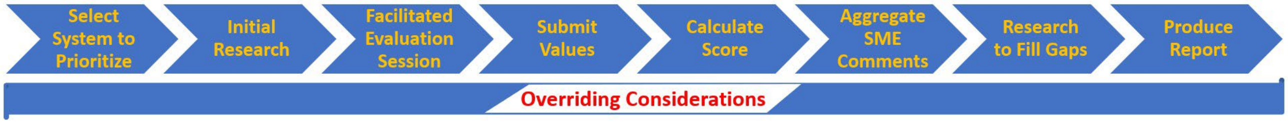


Figure 1: Diagram showing the flow of the prioritization process.

1. **Select System to Prioritize:** The CyTRICS program generally predicates the system for the CFT to prioritize based on needs of the program. CyTRICS uses the term “system” to describe the entity being prioritized, regardless of size or complexity.
2. **Initial Research:** The CFT performs initial desk research and gathers data to develop assumptions about how the system is typically used. This includes market data, installation and configuration details, and system use cases.
3. **Facilitated Evaluation Session:** During the facilitated evaluation session, the CFT will present the information gathered during research to the SMEs. The CFT will also explain the prioritization rubric to the SMEs. Next, SMEs provide values for each factor, ask questions, and state assumptions they make as they assign values to each factor. The SMEs record their provided values and assumptions in a fillable worksheet. The CFT also asks follow-up questions to draw out underlying assumptions that the SMEs may not have stated, focusing on assumptions that may be considered standard within an industry but foreign to outsiders.
4. **Submit Values:** The SMEs submit their values and assumptions for each factor via a fillable worksheet to the CFT.
5. **Calculate Score:** After all SMEs submit their worksheets to the CFT, the CFT uses a formula that weights the factors to calculate the system prioritization score. It is essential that the original

SME inputs are preserved so different formulas can be applied in the future if assumptions or priorities change, without requiring an additional evaluation session.

6. **Aggregate SME Comments:** The CFT summarizes SME comments made during the facilitated evaluation session and draws out key themes or gaps.
7. **Research to Fill Gaps:** If the SMEs ask questions the original assumptions around system use case, installation, and configuration did not cover, the CFT performs a second round of desk research to cover any gaps and, if necessary, consults again with the SMEs for any resulting revisions to their assigned values.
8. **Produce Report:** The CFT summarizes the system score and assumptions in a report. The purpose of the report is to contextualize the numerical system score with the aggregated SME assumptions and comments. The CFT then disseminates the report to the CyTRICS analysis team and any other relevant audiences, potentially including system manufacturers, utilities, or asset owners.
9. **Overriding Considerations:** Overriding considerations are considered separate from the process because they do not apply for each system selected for prioritization. In situations where overriding considerations apply, they could interrupt the prioritization process or impact the score by changing assumptions used at the time the system was prioritized.

1.3. Prioritization Team Roles

The prioritization team comprises one or more facilitators, a panel of SMEs, and a market research company. The facilitators work with a Lead SME from the SME team to narrow a vast number of possible use cases of a system down to a specific use case that can be evaluated against the prioritization factors. Additionally, the CFT may appoint a designated record keeper to document key discussion points during the facilitated evaluation session for further analysis by the CFT during report generation. The facilitators lead an evaluation session with the SMEs to elicit values from the SMEs for nine defined factors. Finally, market research companies help provide vital market data used during prioritization.

1. **Facilitator / CyTRICS CFT (CFT):**
   a. Oversees prioritization
   b. Perform initial research and information gathering
   c. Ensure market data for the system to be scored is procured from market research company
   d. Establish reference architecture and operational use case assumptions

      Note: The operational use case is important to establish because it helps SMEs estimate potential consequences that could occur if the system were interdicted.

   e. Gather a comprehensive team of SMEs, to potentially include participants from industry
   f. Appoint a Lead SME

      Note: The Lead SME should be an expert experienced with the system selected for prioritization or a similar system. The Lead SME has field experience in the subdomain where the system is assumed to be installed for the purpose of the prioritization.

   g. Appoint a record keeper (optional)

   h. Conduct facilitated evaluation session
   i. Collect SME inputs
   j. Generate prioritization report.

2. **SMEs:**
   a. Evaluate system selected for prioritization
   b. Provide values for each evaluated factor
   c. Document assumptions used to assign values to each factor
   d. Provide values and assumptions to the CFT.

      Note: The SME team should be comprised of experts experienced with the system selected for prioritization or a similar system. Ideally, the SME team can provide a depth and breadth of knowledge of the system being prioritized.

3. **Market Research Company**:
   a. Provide market data for systems selected for prioritization to the CFT.

Figure 2 shows the relationship between the prioritization process steps, the roles, and instruments used to evaluate a system and generate a prioritization score.

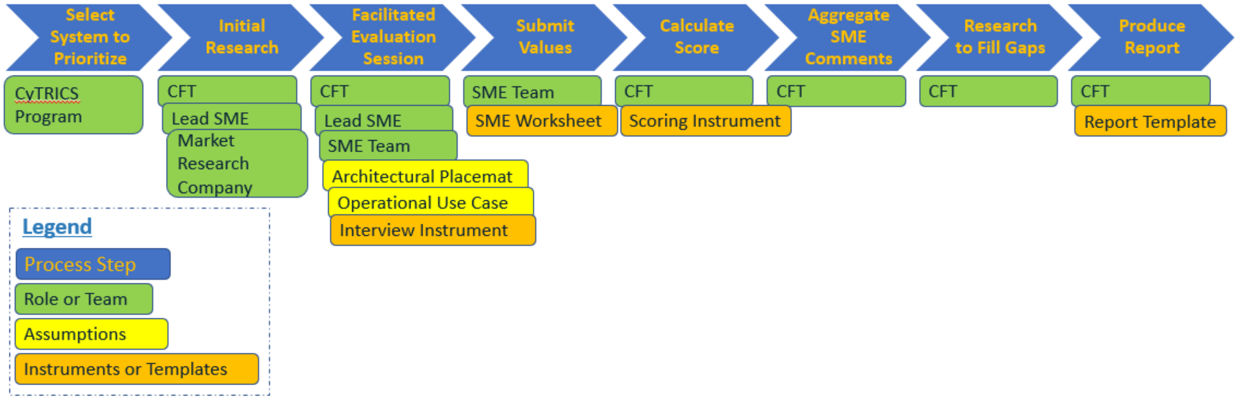


Figure 2: Prioritization steps shown in relation to roles, assumptions, and tools used to generate a prioritization score.

1.4. Instruments and Templates Used for Prioritization

1.4.1- Prioritization Instruments

Several instruments help the CFT successfully conduct facilitated evaluation sessions with SMEs, collect SME inputs, and calculate the prioritization score for a system.

1.4.1.1- CFT Interview Instrument

The CFT Interview Instrument contains an overview of the prioritization process, the system to be prioritized, and the assumptions necessary to complete a prioritization session. It also contains definitions for each category and factor and visually presents the scales to the SMEs. The CFT will use the interview instrument to keep the scoring session focused on the specific topic the team is scoring. The interview instrument is a Microsoft PowerPoint and is shown as screen captures in the CFT Interview Instrument section of Appendix B: Instruments Used for Prioritization.

1.4.1.2- SME Prioritization Worksheet

The SME prioritization worksheet is an instrument used to capture the SMEs' numeric values and their notes substantiating each value they provide. It also captures their areas of experience and expertise. The prioritization worksheet currently exists in fillable Microsoft Word and fillable PDF formats. Screen captures of the scoring worksheet are shown in the SME Prioritization Worksheet section of Appendix B: Instruments Used for Prioritization.

Value scales are the measures SMEs can select for each factor on the prioritization worksheet. The values range from one to five for each factor. In addition to the range of values, definitions for each possible value are provided. These definitions keep the score consistent when working with different SMEs across multiple facilitated evaluation sessions. The scales and definitions are provided in Section 2, as each factor is discussed more in depth. For instances where the scales are not fully defined, SMEs can interpolate scores; for example, if a scale has definitions for a 1, 3, and 5 and SMEs deem it appropriate, they can assign a value of a 2 or 4 if they assess the appropriate response to fall between defined ranges.

1.4.1.3- CFT Scoring Instrument

The scoring instrument helps the CFT manage SME inputs and performs all the calculations from the raw integer values provided by the SMEs. The scoring instrument is currently a Microsoft Excel workbook. See the CFT Scoring Instrument section in Appendix B: Instruments Used for Prioritization.

1.4.2- Prioritization Report Template

The prioritization report documents the prioritization score as well as assumptions and considerations SMEs made as they assigned values calculated in the prioritization score. The report template is in Microsoft Word and screen captures of several prioritization reports are provided in Appendix C: Prioritization Report Template.

Section 2: Impact-based Prioritization

This section explains:

- The Prioritization Framework
- The rationale behind why each category was chosen
- Where the CFT should look for information to score each factor
- What CyTRICS is measuring with each factor
- The definitions for the scoring range of each factor
- How to calculate scores for each factor.

2.1. Prioritization Framework

Impact-based prioritization considers five categories, shown below in Figure 3. Each category is divided into factors with framing questions and evaluation criteria. The categories of Impact, Prevalence, Technical Characteristics, and Maintainability are evaluated with the help of SMEs, market research firms, and technical data produced by system manufacturers. The overriding considerations category is analyzed outside of the prioritization process on an ad hoc, as-needed basis.

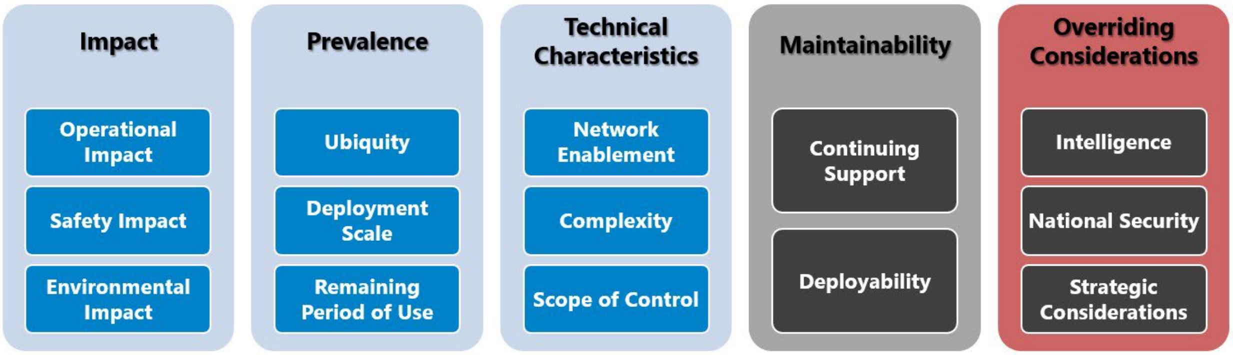


Figure 33: Categories and factors used for the Impact-based Prioritization process.

2.2. Impact

The Impact category captures the extent to which the misuse of a system could degrade or deny operational capabilities or could result in harm to human safety or the environment. Impact is evaluated by using input from SMEs who understand the system's use within the architecture of an organization and the negative impacts misuse could present.

Impact
Operational Impact
Safety Impact
Environmental Impact

2.2.1- Operational Impact

Operational Impact is evaluated by using input from energy sector SMEs who have a detailed understanding of the application of the system within an organization. This evaluation requires SMEs who have extensive operational knowledge of the system (i.e., performing equivalent roles within architectures supporting critical systems within the energy sector).

The evaluation of Operational Impact is based on the system's functions and roles within the architecture, including any information stored on or processed by the system, the systems it controls, and the communications it supports with other systems. For consistency across Impact assessments, SMEs will be asked to assess the impact of only one compromised system. SMEs should assess the impact of a misuse of the primary system and any similar backup systems for that specific function within the architectures. SMEs should only assess first-order impacts of the system under evaluation; additional impacts beyond the system being evaluated are not within the scope of the prioritization process.

2.2.1.1- Rationale

Systems that have greater impact to energy stability present more serious risks.

2.2.1.2- Electric Sector

2.2.1.2.1- Scoring

Impact within the electric sector is evaluated based on the unique operational requirements across electricity generation, transmission, and distribution. Examples of how impact is assessed include damage to critical equipment and replacement time, attacks causing direct loss-of-load or generation,, and misleading or erroneous information (due to loss or manipulation of information) impacting situational awareness and operator decision-making.

Level	Value	Description
Very High Consequence	5	The misuse, malfunction, or loss of this system alone could cause a wide-area loss of electricity for days or more.
High Consequence	4	The misuse, malfunction, or loss of this system alone could cause a wide-area loss of electricity for hours, up to one day.
Medium Consequence	3	The misuse, malfunction, or loss of this system alone could cause localized outages.
Low Consequence	2	The misuse, malfunction, or loss of this system in combination with others could cause localized outages.
Very Low Consequence	1	The misuse, malfunction, or loss of this system would not likely cause loss of power under any circumstances.

2.2.1.2.2- Information Sources

In the electric sector, scoring will require utility SMEs in power system operations. Engineers within power system planning and protection/control groups are required to assess potential impacts to various critical utility functions.

2.2.1.2.3- Framing Questions

Below are example questions the CFT can ask SMEs during a facilitated scoring session. Additional questions are included in a scoring worksheet. These questions are tailored for effectiveness when analyzing the electric sector:

- How severe would the operational consequences be?
- How badly would the utilities' ability to deliver energy be affected?
- For how long?
- What are the worst-case Operational Impacts of malicious mis-operation of the system?
- Record what factors contribute to the Operational Impacts, e.g.:
    - Damage to critical equipment and replacement time
    - Attacks causing direct loss-of-load/generation
    - Ability to induce cascading failures
    - Misleading or erroneous information (due to loss or manipulation of information) impacting situational awareness and operator decision-making
- Describe what built-in resilience is in place (e.g., spares, backups) that may affect the Operational Impact described.

2.2.1.3- ONG Sector

2.2.1.3.1- Scoring

Impact within the ONG sectors is evaluated based on the unique operational requirements across ONG systems including, processing, transportation, and storage. Examples of how impact is assessed include: damage to critical equipment and replacement time; direct loss of oil or gas supply to users (e.g., electric utilities using ONG for generation, refineries or processing plants, and household or commercial customers in a geographic area); loss of systemion or wells; ability to cause ripple effects (e.g., by storage reaching capacity and thus precluding further input); and misleading or erroneous information (due to loss or manipulation of information) impacting situational awareness and operator decision-making.

Level	Value	Description
Very High Consequence	5	The misuse, malfunction, or loss of this system would result in an immediate wide spread demand loss (e.g., metropolitan area, pipelines feeding multiple generators) or wide-area supply loss (e.g., multiple refineries or processing plants) for an extended period (e.g., >7 days).
High Consequence	4	The misuse, malfunction, or loss of this system would result in a loss of critical ONG capabilities of facilities (e.g., systemion, processing, transportation, storage) for a long period (e.g., 2-7 days).
Medium Consequence	3	The misuse, malfunction, or loss of this system would result in a loss of critical ONG capabilities of facilities (e.g., systemion, processing, transportation, storage) for a moderate period (e.g., 1-2 days).

Low Consequence	2	The misuse, malfunction, or loss of this system would result in a loss of critical ONG capabilities of facilities (e.g., systemion, processing, transportation, storage) for a short period (e.g., hours).
Very Low Consequence	1	Little to no impacts to oil/gas refinement or delivery; the system is not needed for real-time operation of the oil/gas domain.

2.2.1.3.2- Framing Questions

Below are example questions the CFT can ask SMEs during a facilitated scoring session. Additional questions are included in a scoring worksheet. These questions are tailored for effectiveness when analyzing the oil and gas sector:

- What are the worst-case Operational Impacts of malicious mis-operation of the system?
- Record what factors contribute to the Operational Impacts, e.g.:
    - Damage to critical equipment and replacement time
    - Attacks causing direct loss of oil or gas supply to users (e.g., electric utilities using ONG for generation, refineries or processing plants, and household or commercial customers in a geographic areas)
    - Loss of systemion or wells
    - Ability to cause ripple effects (e.g., storage reaching capacity and precluding further input)
    - Misleading or erroneous information (due to loss or manipulation of information) impacting situational awareness and operator decision-making
- Describe what built-in resilience is in place (e.g., spares, backups) that may affect the Operational Impact described.

2.2.1.3.3- Information Sources

In the ONG sector, SMEs will be needed within operations, controls engineering, and automation engineering groups.

2.2.2- Safety Impact

This factor reflects the impact a malicious system could have on human safety. Human safety, in this context, includes both the general public and employees of the utility or organization.

2.2.2.1- Rationale

In addition to operational and environmental impacts, the risk from a compromised system can also result in safety impacts. Safety impacts encompass the harm the energy source or associated equipment could cause to plant employees and the general public. This factor includes only the first-order safety impacts, not second-order impacts resulting from loss of energy (e.g., by hospitals or other lifeline services).

2.2.2.2- Scoring

Level	Value	Description
Very High Consequence	5	The misuse, malfunction, or loss of this system alone could cause loss of life.
High Consequence	4	The misuse, malfunction, or loss of this system, in conjunction with multiple human errors or failures of redundant systems, could cause loss of life.
Medium Consequence	3	The misuse, malfunction, or loss operation of this system alone could cause injury.

Low Consequence	2	The misuse, malfunction, or loss of this system, in conjunction with multiple human errors or failures of redundant systems, could cause injury.
Very Low Consequence	1	The misuse, malfunction, or loss of this system could not cause impacts to safety under any circumstances.

2.2.2.3- Information Sources

In addition to SMEs, when available, documented historical events are also valuable reference points to assist the CFT in understanding the scope and scale of potential impacts.

2.2.2.4- Framing Questions

Below are example questions the CFT can ask SMEs during a facilitated scoring session. Additional questions are included in a scoring worksheet:

- How severe would the safety consequences be?
- How many people could be harmed?
- Could lives be lost?
- What is the worst-case safety impact of malicious mis-operation of the system?
- Who would be injured?
- What events should need to occur to induce a safety hazard?

2.2.3- Environmental Impact

This factor reflects the impact a malicious system could have on the environment. This factor is situationally dependent on the sector and types of effects that a malicious system could create (e.g., wildfires, oil spills, explosions).

Data Source(s):	SME evaluation, documented historical events (where available), etc.
Scale for Evaluation:	1, 2, 3, 4, 5

2.2.3.1- Rationale

In addition to operational and safety impacts, the risk from a compromised system can also result in environmental impacts. The Environmental impacts factor focuses on damage caused by inadequate control of energy sources (e.g., fires, spills).

2.2.3.2- Scoring

Level	Value	Description
Very High Consequence	5	Catastrophic: The malicious operation of this system would result in a wide-area (e.g., regional) and significant (e.g., requiring environmental remediation and/or behavioral changes on the part of the affected human population) environmental impact for a period of time (i.e., at least five years).
High Consequence	4	Severe: The malicious operation of this system would result in a wide-area and significant environmental impact for a period of time (i.e., more than one year).
Medium Consequence	3	Significant: The malicious operation of this system would result in localized or time-bounded environmental impacts (i.e., no more than one year), which could require short-term behavioral changes on the part of the affected human population.
Low Consequence	2	Minor: The malicious operation of this system would result in a localized and time-bounded environmental impact.
Very Low Consequence	1	Negligible: No credible scenario exists where the misuse of the system contributes to marginal environmental impacts.

2.2.3.3- Information Sources

In the electric sector, SMEs will have extensive knowledge of power system operations, specifically within protection and control groups. In the ONG sector, SMEs will be knowledgeable about operations, controls engineering, and automation engineering groups. When available, documented historical events are also valuable reference points to assist the CFT in understanding the scope and scale of potential impacts.

2.2.3.4– Framing Questions

Below are example questions the CFT can ask SMEs during a facilitated scoring session. Additional questions are included in a scoring worksheet:

- How severe would the environmental consequences be?
- How much mitigation or environmental remediation would be needed, and for how long?
- What is the worst-case Operational Impact of malicious mis-operation of the system?
- What would the environmental consequence be?
- What errors/failures would have to occur to enable that impact?

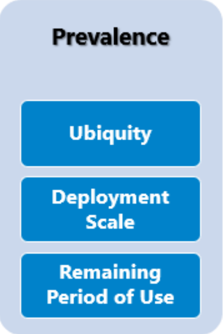
2.2.4- Impact Sub-score Calculation

The score for Impact will be produced by determining the maximum value of the Operational Impact, Safety Impact, and Environmental Impact scores, as systems can score high in one criteria but may have a low score in another. Also, subsectors may naturally face more risks in one of these areas (e.g., ONG may present greater opportunities for safety or environmental impacts). Changes to the prioritization process necessary for implementation in other energy sectors is included in Section 3.1., opportunities for improvement.

$$\textit{Impact} = \textit{Max}(\textit{Operational Impact, Safety Impact, \& Environmental Impact})$$

2.3. Prevalence

The Prevalence of a system captures the extent to which a vulnerability could impact national energy delivery by affecting multiple systems across different organizations. It also reflects the risk presented by a vulnerability enabling a coordinated attack to multiple instances of a system, thereby causing greater impacts. Prevalence incorporates how broadly the system is used within the sector or subsector, the system's overall lifespan, and the number of systems deployed. Prevalence operates on the assumption that a higher score indicates a larger disruption.



The scores for these factors are determined by SMEs and the CFT based on information procured from market research firms, data collected from Internet searches, and practical knowledge of the SMEs based on their field observations. The SME team evaluates the data available and assigns scores for each Prevalence factor.

2.3.1- Ubiquity

The Ubiquity of the system determines how common the vendor system is amongst systems that perform similar functions across the sector for which it was identified, or across similar subsectors for systems that perform more tailored, sector-specific functions.

2.3.1.1- Rationale

Functional application of market share data is leveraged to determine Ubiquity. The market share is determined specific to the system's function within the sector or subsector. For example, a programmable logic controller (PLC) may be compared across the energy sector, while a digital relay may be compared only within its subsector.

2.3.1.2- Scoring

Level	Value	Description
High	5	26%+ market share.
Medium High	4	19-25% market share.
Medium	3	13-18% market share.
Medium Low	2	6-12% market share.
Low	1	0-5% market share.

2.3.1.3- Information Sources

Market research reports provide information regarding the market share of that system. SMEs validate the numbers provided by market research reports with their observations.

2.3.1.4- Framing Questions

The interview instrument and scoring worksheet pose these questions:

- How common is the vendor system amongst systems that perform similar functions across the sector for which it was identified?
- What is its market share?

2.3.2- Deployment Scale

The Deployment Scale of the system attempts to estimate the total number of systems in use within the U.S. energy sector. For newly emerging systems, this factor could also represent the number of potential deployments expected to be fielded.

2.3.2.1- Rationale

Systems with a high number of deployed instances present more opportunities for intrusions, coordinated attacks, or supply chain manipulation with significant impacts. While the Ubiquity factor prioritizes systems with high market adoption, this factor prioritizes systems that may have large deployments, but, due to the scale at which certain systems are deployed, may not have a major market share. Furthermore, this factor helps to prioritize emerging systems that do not have known market adoption information but have potential for large adoption.

2.3.2.2- Scoring

Level	Value	Description
Very High	5	Over 100,000 deployed nationally: The energy sector either currently includes (or has the potential to adopt) over 100,000 systems nationally. The number of systems in the field scales with the number of consumers. Examples include smart meters (e.g., electric or gas) and smart inverters.

Medium High	4	1,001-9,999 deployed nationally.
Medium	3	Over 1,000 deployed nationally: The energy sector currently includes (or has the potential to adopt) over 1,000 systems nationally. The number of systems scales with the number of field systems. Examples include digital relays, PLCs, remote terminal units (RTUs), etc.
Medium Low	2	11-999 deployed nationally.
Low	1	10s deployed nationally: The energy sector currently includes (or has the potential to adopt) over ten instances of the system. The number of system scales with the number of utilities. Examples include control center software or specially tailored controllers for equipment generators, transformers, or refineries.

2.3.2.3- Information Sources

Market research reports provide information regarding the number of systems deployed, along with emerging trends for predicted deployments. SMEs validate the numbers provided by market research reports with their observations.

2.3.2.4- Framing Questions

The interview instrument and scoring worksheet pose this question:

- How many of these systems are deployed nationally?

2.3.3- Remaining Period of Use

This factor captures the length of time the system is expected to be used (for new or future deployments) or will continue to be used (for current deployments) operationally by an organization in the energy sector (e.g., an electric utility, an ONG pipeline operator) to support an energy delivery function. Information on lifespan should be obtained from industry SMEs that have the experience managing these systems. A system's remaining period of use may be organizationally dependent; therefore, these values may need to be averaged to accurately represent the energy sector's overall expected remaining period of use.

2.3.3.1- Rationale

Assets with a long remaining period of use will be part of the energy sector's attack surface for an extended timeframe.

2.3.3.2- Scoring

Level	Value	Description
Long	5	The life expectancy or expected deployment (whichever is shorter) is more than 15 years from today.
Medium	3	The life expectancy or expected deployment (whichever is shorter) is from 6 to 15 years from today.
Low	1	The life expectancy or expected deployment (whichever is shorter) is less than 6 years from today.

2.3.3.3- Information Sources

Organizational SMEs with asset management experience and organizational knowledge regarding the expected lifespan of systems are information sources. Alternatively, when organizational SMEs are not available, the CFT and SMEs evaluate the market research and SMEs use their experience to evaluate this factor.

2.3.3.4- Framing Questions

The interview instrument and scoring worksheet pose this question to the prioritization team as they assess market data:

- How long is the expected operational remaining period of use of this system?

2.3.4- Prevalence Sub-score Calculation

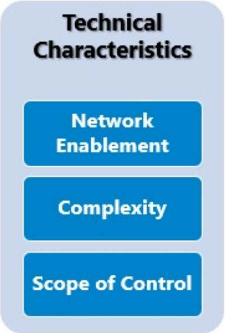
The scoring for Prevalence will be computed by the following equation:

Prevalence =.8 x Max(Ubiquity,Deployment Scale) +.2 x Remaining Period of Use

The scoring will more heavily weight Ubiquity and Deployment Scale, as these provide more immediate information regarding the degree to which the system supports energy delivery functions. Furthermore, Ubiquity and Deployment Scale will be combined with the Max function, which returns the maximum of the two values. This will prioritize systems that are key within their market segment, but have minimal deployments (i.e., have High Ubiquity) and systems that are deployed at large scales but may not be an industry market leader (i.e., High Deployment Scale).

2.4. Technical Characteristics

This category identifies technical characteristics of a system and is predicated on the underlying assumption that the more complex a system is, the more likely that system is to have impactful vulnerabilities. While this may or may not be true in every situation, CyTRICS Prioritization is attempting to quantify these factors. Many technical characteristics present challenges for repeatably and objectively collecting the relevant information to effectively score. The set of characteristics in the prioritization process was selected because the information needed to score the criteria can be derived from or based on objective and repeatable sources, such as product documentation.



Technical Characteristics

Network Enablement

Complexity

Scope of Control

2.4.1- Network Enablement

This factor represents the degree to which a system supports network connectivity, both within the organization and remotely. It includes the physical medium for connection (wired vs. wireless), the exposure of the system based on the supported network protocols, and architectural properties that are common based on the system's design and intended use.

2.4.1.1- Rationale

Vulnerabilities discovered in systems with increased network access present greater risk and could either be directly exploited to impact operations or used as a stepping-stone within a larger attack. Additionally, systems with greater connectivity may be used to compromise multiple connected systems. Although a system may have different network capabilities, these may be either disabled or blocked (i.e., through other network-based filtering techniques) so that deployed risks may differ from the system's default capabilities. However, these features will more broadly contribute to the system's risk when viewed across the sector, as they are likely used in many installations.

2.4.1.2- Scoring

Level	Value	Description

Very High Accessibility	5	The system includes default functionality and dependencies to communicate with third parties. This includes systems that require communication with manufacturers, such as for over-the-air patching, remote diagnostics, or monitoring.
High Accessibility	4	The system uses routable communication (i.e., IP) to interconnect with multiple systems, including across layers/boundaries. Examples may include SCADA Servers, Front End Processors, RTUs, substation gateways. This also includes wide-area wireless mediums, such as microwave and cellular communications (e.g., LTE, CDMA).
Medium Accessibility	3	The system supports routable communications (i.e., IP) to provide connectivity throughout the utility and introduces the possibility of Internet accessibility. This also includes local-area wireless communication protocols (e.g., 802.11, 802.15.4) that could be accessible by an attacker within local proximity to the system.
Low Accessibility	2	The system only includes local, non-routable, wired communications. It is not accessible remotely and requires physical proximity (e.g., Serial port, optical port).
No Accessibility	1	None: the system has no known support for network communication.

2.4.1.3- Information Sources

Scoring information should be obtained from vendor documentation that identifies the networking features of the system. Depending on non-disclosure agreements (NDAs), this information could also be obtained from vendor SMEs.

2.4.1.4- Framing Questions

The interview instrument and scoring worksheet pose these questions to the prioritization team:

- To what degree does the system support network connectivity, both within the organization and remotely?
- Consider wired and wireless connections. What is the exposure of the system based on the supported network protocols, and what are the architectural properties that are common based on the system's design and intended use?

2.4.2- Complexity

This factor explores the complexity and technical functionality of the system. Some systems perform static/preprogrammed functions, while other systems support broad programmability to perform organization-specified functions. Further, systems with greater programmability and interoperability may require greater networking capabilities, interfacing, and security requirements.

2.4.2.1- Rationale

Systems with greater complexity present broader opportunities for security vulnerabilities and require more sophisticated protection mechanisms to ensure secure operations.

2.4.2.2- Scoring

Note though the scale below contains values for 1, 3, and 5, SMEs may choose to select a 2 or 4 at their discretion if it is assessed the system qualifies for such a value.

Level	Value	Description
High Complexity	5	Generalized Multi-Purpose Device: Highly configurable system, with potentially high modularity. Will typically allow for operation in multiple environments, and will interact with several disparate other systems. Typically will make use of general purpose operating systems and deep technology or protocol stacks. High Complexity

		systems tend to support or include many individual components, communication pathways, or "moving parts". Examples include several different kinds of application servers, distributed control systems, etc.
Medium Complexity	3	Constrained Multi-Purpose System: The system can perform more than one function, but number of functions is highly constrained by controls which cannot be bypassed. Examples include processing constrained Programmable Logic Controllers (PLCs), automation controllers, and purpose built computer systems built from limited application-specific integrated circuits (ASICs).
Low Complexity	1	Limited Purpose System: The system provides a singular function, with limited configurability or modularity. Examples may include sensors/actuators, simple GPS clocks, or fault recorders.

2.4.2.3- Information Sources

Scoring information should be obtained from vendor documentation that identifies the system functions. This may include information obtained from vendor SMEs.

2.4.2.4- Framing Questions

The interview instrument and scoring worksheet pose these questions to the prioritization team:

- What is the complexity and technical functionality of the system?
- Does the system perform static/preprogrammed functions, or does it support broad programmability to perform organization-specified functions?
- Does the system support broad interoperability functions (which typically require greater networking capabilities, interfacing, and security requirements)?

2.4.3- Scope of Control

The Scope of Control factor reflects the degree to which the system can control operational equipment. Control in this context includes actions that directly actuate a physical system (e.g., pump, circuit breakers), as well as actions that provide processed data or communications that directly cause another system to be controlled (e.g., SCADA server, a distributed control system [DCS]).

2.4.3.1- Rationale

Systems with a larger Scope of Control are more likely to have a greater impact if misused, due to the large number of systems they control. Furthermore, these systems are more likely to be more highly connected to other systems within the organization, increasing their exposure to compromise. This factor may have overlap with both Impact and Complexity. For example, a High-Impact score is typically assigned because the system can control multiple actuators, while more complex systems are often needed to support a broader set of control functions. However, the Impact factor is heavily organizationally specific, while Scope of Control focuses on the technical capabilities and should more consistently contribute to the score regardless of a specific organization's use. Furthermore, higher Scope of Control scores may not always directly correlate with higher Complexity scores, especially in cases where a system may perform a key control role, but has limited features or configurability (e.g., front end processor).

2.4.3.2- Scoring

Note: though the scale below contains values for 1, 3, and 5, SMEs may choose to select a 2 or 4 at their discretion if it is assessed the system qualifies for such a value.

Level	Value	Description
Wide Control	5	The system uses remote communication to control a wide-area (e.g., distribution feeders, transmission system). Examples may include SCADA/EMS/DMS platforms.
Control of Limited Systems	3	The system either directly controls an actuator (e.g., breaker, switch, transformer tap, valve), or provides telemetry to another system that directly influences a control decision. This also includes systems that use remote communication to control an actuator.
No Control	1	The system does not directly control any equipment but may inform control decisions. For example, the system may provide telemetry that is used in aggregate and does not directly dictate a control decision.

2.4.3.3- Information Sources

Scoring information should be obtained from vendor documentation that identifies the system functions. This could also include information obtained from vendor or organizational SMEs.

2.4.3.4- Research Question

The interview instrument and scoring worksheet pose these questions to the prioritization team:

- To what degree can the system control operational equipment by directly actuating a physical system (e.g., pump, circuit breakers), or controlling processed data or communications that directly causes another system to be controlled (e.g., SCADA server, a DCS)?

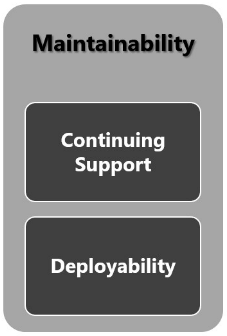
2.4.4- Technical Characteristics Sub-score Calculation

The various technical factors are weighted together to produce a single score. Network Enablement is given the largest weight (.5) as this is the factor that reflects how easily the system could be directed to operate incorrectly. The Complexity score is given a lower weight (.3); while this factor contributes to the number of potential systems, it also has more overlap with Impact. Finally, Scope of Control aims to estimate how many subsystems a system can potentially control, as this factor may also overlap with Impact and Complexity, this factor is assigned a weight of (.2).

Technical Characteristics =.5 x Network Enablement +.3 x Complexity +.2 x Scope of Control

2.5. Maintainability

While mitigations could be deployed through varying techniques, the factors identified in this category will focus on system-based techniques, such as updates, patches, or configuration changes that can potentially impact a vulnerability. Mitigations that require architecture or environmental context are not considered due to a lack of consistency regarding their broad deployment. While the factors in this category are not scored, the information provided during the facilitation session assists those testing the system in identifying potential vulnerabilities.



2.5.1- Continuing Support

This factor evaluates whether the vendor provides patches or updates for systems when needed.

2.5.1.1- Rationale

Vulnerabilities identified by the CyTRICS program can be more efficiently mitigated in systems that are actively supported by the vendor.

2.5.1.2- Scoring

This factor is not scored; the data is collected for CyTRICS Test Planning and CyTRICS Test Operations.

2.5.1.3- Information Sources

The CFT can look to market data, vendor support webpages, technical documentation, and SMEs for input to this factor.

2.5.1.4- Framing Questions

Facilitators ask SMEs these question during a facilitated scoring session. The questions are included in the scoring worksheet:

- Does the vendor provide patches or updates for the system when needed, especially as mitigations are identified for vulnerabilities?
- If a mitigation to a vulnerability detected in the system is developed, can it be deployed?

2.5.2- Deployability

This factor evaluates difficulties with installing an update or patch for a system. This includes both the technical and operational constraints associated with the deployment. Examples of technical constraints include the type of testing needed before the patch can be trusted within an operational setting and cases where the deployment is dependent on the manufacturer performing the installation. Examples of operational constraints include the need to physically install patches at geographically remote locations and the inability to remove the system from service to deploy the patch.

2.5.1.1- Rationale

Vulnerabilities identified by the CyTRICS program can be more efficiently mitigated in systems that are actively supported by the vendor.

2.5.1.2- Scoring

This factor is not scored; the data is collected for CyTRICS Test Planning and CyTRICS Test Operations.

2.5.1.3- Information Sources

The CFT can look to market data, vendor support webpages, technical documentation, and SMEs for input to this factor.

2.5.1.4- Framing Questions

Facilitators ask SMEs this question during a facilitated scoring session. Tthe questions are included in the scoring worksheet:

- How soon can a patch or update be deployed in a typical installation?
- Can the system be easily removed from service without impact to the process it performs?
- Does a patched system require testing or customization before being reinstalled?
- Are instances of the system geographically remote?
- Can an update be made in real-time, using a network connection?
- How difficult is obtaining the vendor update and deploying to the system?

2.5.3- How CyTRICS uses Maintainability Information

The CFT captures the discussion points surrounding continuing support and deployability and document it for use by the CyTRICS Test Operations teams when they perform enumerations and testing of systems. The intent of collecting this information is to assist test operations in identifying vulnerabilities, creating awareness of how supported systems are, and understanding how difficult it could be to deploy updates and recommended security enhancements.

2.6. Overriding Considerations

Overriding Considerations includes three factors that CyTRICS will consider outside of the quantitative scoring process. These factors are not quantifiable and emerge from research performed outside of the prioritization process. CyTRICS uses overriding considerations, when they are present, to provide alternative insights beyond the quantitative score, which may influence CyTRICS decisions to test the systems under consideration. These factors may not be described in the prioritization report.

Overriding Considerations
Intelligence
National Security
Strategic Considerations

2.6.1- Intelligence

This factor reflects information from intelligence sources detailing adversarial threat events, intentions, or capabilities regarding the system being prioritized. Intelligence could include information regarding the compromise of a system's supply chain or information regarding capabilities to exploit a system. Some additional intelligence examples are information about:

- A specific vendor, system, or system that allows remote access by a country/state
- A system includes malicious functionality that could manipulate system operations

- A system has known dependencies on hardware or software systems from concerning countries, and if there are known attempts to exploit these
- Known attempts to infiltrate the supply chains for a system or systems whether they are attempting to directly target the U.S. energy sector or not
- A country of concern has future potential for leverage over a vendor
- Open-source software packages with known contributors from countries of concern are integrated into a system
- Vendors not adequately enforcing strong supply chain security practices, perhaps leading to susceptibility to supply chain tampering
- Adversary group access to unpublished vulnerabilities on a specific system that grants them remote access to systems
- Adversary groups have known capabilities or tools that can manipulate a system

2.6.1.1- Information Sources

DOE/IN, threat intelligence reports from Government agencies or their partners, the Electricity ISAC (E-ISAC), the ONG-ISAC (ONG-ISAC), and open-source threat reporting.

2.6.2- National Security

This factor allows the CyTRICS program to consider potential specific National Security impacts that could result from interdiction of the system being prioritized. Systems supporting energy delivery functions to critical installations may be of particular concern to CyTRICS. Additional National Security examples include:

- A system performing critical or essential roles in supplying energy to a facility of National Security concern (e.g., a military base), as identified by DoD. Such a facility could experience significant or lasting Operational Impacts due to the system's malfunction, denial, or malicious operation. For example, the ability of the facility to perform its missions could be reduced below the mission-acceptable minimum threshold (significant impact), or the mission capability could be reduced for a period longer than the duration of a specific mission operation (lasting impact).
- A system performing a significant role in supplying energy to a facility of National Security (e.g., a military base), homeland security (e.g., a FEMA operations center), or lifeline (e.g., a major medical center) concern. Such a facility could experience significant short-term or moderate long-term impacts on its ability to perform mission tasks due to the system's malfunction, denial, or malicious operation.
- A system performing a role in supplying energy to a facility of National Security, homeland security, or lifeline concern. Such a facility could experience significant short-term or moderate long-term impacts on its ability to perform mission tasks due to the system's malfunction, denial, or malicious operation.

2.6.2.1- Information Sources

DOE-IN or other federal intelligence or law enforcement sources such as DoD, DOJ, or DHS.

2.6.3- Strategic Considerations

This factor allows CyTRICS to reflect considerations related to evolving trends within energy sector technologies, the role of a system across multiple subsectors, and the extent of prior testing or vulnerability discovery. CyTRICS may want to test systems incorporating novel technologies that previously have not been used in or tested by the energy sector, even if the quantitative scores for such systems are low. These new technologies could present new supply chain risks or introduce new vulnerabilities to existing control systems.

This factor also accounts for systems used across many subsectors where the prioritization of said system is relatively low in any or perhaps all given subsectors. However, when considering the breadth of subsectors where the system is used and their relative value to the resilience to U.S. energy delivery, the prioritization score needs to be elevated. Another facet this factor considers is previously discovered vulnerabilities in similar systems or within the same system family.

2.6.3.1- Information Sources

Vendor manuals, National Laboratories, utilities, industry organization, etc.

2.7. Scoring

The SME worksheets are aggregated and the SME scores for each factor are averaged. The average for each value is then used to calculate category sub-scores and the overall prioritization score. To assist in performing calculations, a Microsoft Excel workbook titled, “CFT Scoring Instrument” is provided in Appendix B: Instruments Used for Prioritization.

2.8. Weighting

Note the scoring system applies weights to categories and factors. This weighting is intended to allow factors that could have a greater impact to energy delivery to account for a greater percentage of the overall prioritization score.

The relative weights of each category (Impact = 39%, Prevalence = 39%, and Technical Characteristics = 22%) were selected to ensure that systems with greater overall importance to national energy delivery are given higher scores. The score range for the scoring instrument is 1.0-5.0.

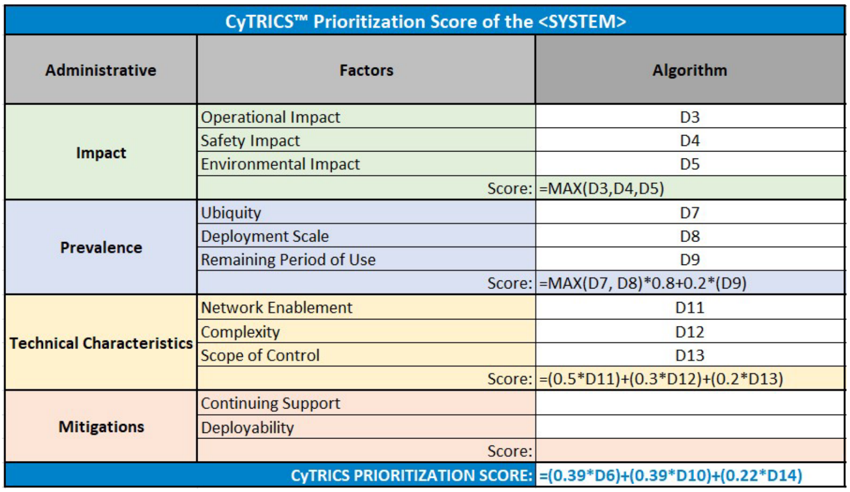
Default weights for the final prioritization score are:

Score= (.39 x Impact +.39 x Prevalence +.22 x Technical Characteristics)

A potential benefit to using weighting to calculate prioritization scores versus tabulating raw values for each factor allows future use of the scores to be changed, based on updated threat behavior, without creating a need to conduct additional facilitated scoring sessions with the SMEs. For example, this allows the CFT to adjust the weight of a score if current threat intelligence suggests cyber adversaries are targeting OT equipment based on safety features. In the event weights are adjusted, it is imperative for the team conducting the scoring to document all justifications and substantiating evidence in the prioritization report.

2.9. Prioritization Algorithm

The Impact-based Prioritization algorithm applies weighted percentages to categories and factors. The prioritization algorithm is best summarized below in Figure .



CyTRICS™ Prioritization Score of the <SYSTEM>		
Administrative	**Factors**	**Algorithm**
Impact	Operational Impact	D3
	Safety Impact	D4
	Environmental Impact	D5
	Score:	=MAX(D3,D4,D5)
Prevalence	Ubiquity	D7
	Deployment Scale	D8
	Remaining Period of Use	D9
	Score:	=MAX(D7, D8)*0.8+0.2*(D9)
Technical Characteristics	Network Enablement	D11
	Complexity	D12
	Scope of Control	D13
	Score:	=(0.5*D11)+(0.3*D12)+(0.2*D13)
Mitigations	Continuing Support	
	Deployability	
	Score:	
	CyTRICS PRIORITIZATION SCORE:	=(0.39*D6)+(0.39*D10)+(0.22*D14)

Figure 4: CyTRICS Impact-based Prioritization Score algorithm.

2.10. Prioritization Report

The results of Impact-based Prioritization are recorded in a prioritization report. The intent of the report is to document key assumptions with direct impact on the score as well as to capture key discussion with SMEs as the system is evaluated and scored. The report contains the following sections:

- Executive Summary – for a High-level one-page summary of the prioritization results.
- CyTRICS Overview – the report is expected to stand alone; the overview explains the purpose of CyTRICS and prioritization.
- Prioritization Report Overview – the report is approximately ten pages; this section provides a brief roadmap of the report.
- Results of Prioritization – a bottom-line up-front approach containing more details about the result of prioritization.
- System Overview – brief overview of the system, capabilities, and how it is leveraged in the energy sector.
- Operational Context Assumptions – this is where the prioritization team documents the sector and subsector, the representative architecture, and the operational use case assumptions. The intent is to specify where in a larger system the system being prioritized is assumed to be installed. This section also states which connections the system maintains and what control functions the system is assumed to have.
- Prioritization Score – this section is a deeper dive into the prioritization score. The total score was already presented in the executive summary section. This section contains the individual scores for each factor, the sub-scores for each category, and how all those scores aggregate into the overall prioritization score. The easiest way to display this information is in a table.
- Score Rationale – this section documents the key assumptions SMEs considered as they assigned their scores. It also contains the most important discussion points the scoring team considered as they performed research, conducted the facilitated scoring session, and followed up with SMEs to ensure all the SMEs perspectives and assumptions were clearly understood by the CFT.

The comments for this section are organized by category (e.g., Impact, Prevalence, Technical Characteristics) and by factor (e.g., Operational Impact, Deployment Scale, Scope of Control).

- Conclusion – a concise summary of the prioritization report.
- References – any documents used to generate a prioritization score, create the reference architecture, or add graphical enhancements to the report need to be properly documented in MLA format in the reference section.

Reports will be critical to capture the assumptions that directly impact the scores provided for each category and factor. As future research is performed and new vulnerabilities are discovered, CyTRICS researchers can refer to data collected during prioritization sessions and determine if prioritization scores should be re-evaluated. Prioritization reports can serve as justification as to why CyTRICS tests one vendor's system over a competitor's similar system. A sample report template is provided in Appendix B: Prioritization Report Template.

2.11. Pilot Testing

2.11.1- Electric Sector

Impact-based prioritization has been tested within the electric sector. While working with SMEs to conduct prioritization sessions, SMEs helped develop reference architectures that can be reused in future prioritization sessions. SMEs also helped capture use case assumptions for scored systems. As SMEs not directly involved with pilot prioritization sessions reviewed the results, they report that the results align with what they would expect. The systems scoring higher are the systems SMEs would expect to have a greater negative impact on energy stability if the system failed or was interdicted by cyber adversaries.

2.11.2- Oil and Natural Gas Sectors

CyTRICS made a deliberate decision to start prioritizing systems used primarily in the electric sector; however, CyTRICS has tested the prioritization process on systems used in the ONG sectors and determined the process returns repeatable results and is applicable for prioritizing systems used in the ONG sectors.

Since CyTRICS focused efforts on the electric sector, reference architectures and use case assumptions are not as mature and will require additional development and adjustments when scoring systems in ONG.

3. Future Work

3.1. Opportunities for Improvement

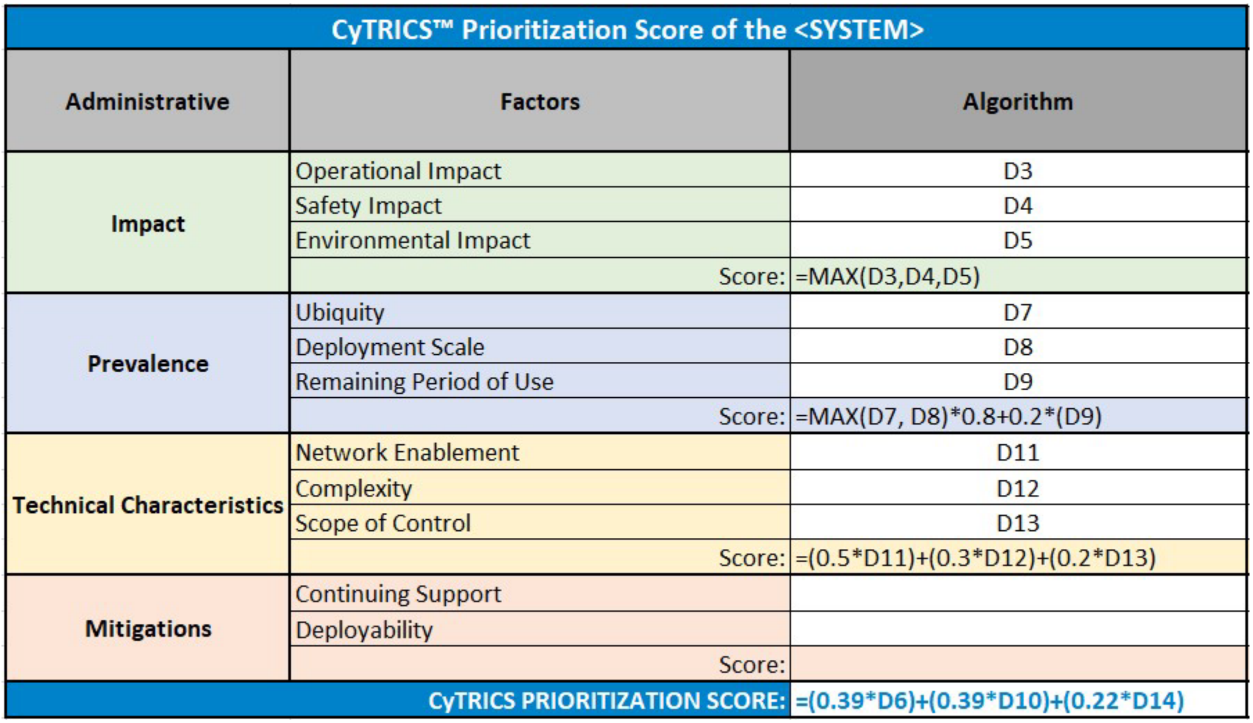
The CyTRICS team has identified several areas where future work could further validate and continuously improve the prioritization process. For example, the existing process could be applied to other energy subsectors by identifying and modifying modular systems of the existing process. These systems could include the required qualifications for SMEs, questions that are asked by the CFT to the SMEs, definitions in relevant scales, and reference architecture examples.

Elicitation of information from SMEs is a foundational element of the Prioritization process. Future improvements to the elicitation process may include a more technically sophisticated feedback collection tool, allowing higher efficiency for both SMEs providing feedback and facilitators processing the data for the prioritization report. For example, this could take the form of an online data repository accessible by SMEs on the front end and facilitators on the back end.

3.2. Next Steps in CyTRICS Prioritization

The scales for factors and scoring algorithms to combine them, shown In Table 4, reflect extensive deliberation among SMEs to characterize risk associated with deployment of a wide range of communication and control technologies on the grid. Although the prioritization system is functional and can be used to score technology risks, some improvements in the system could be made.

Table 4 CyTRICS Factors and Algorithms Used to Combine Factor Scores



CyTRICS™ Prioritization Score of the <SYSTEM>		
Administrative	**Factors**	**Algorithm**
Impact	Operational Impact	D3
	Safety Impact	D4
	Environmental Impact	D5
	Score:	=MAX(D3,D4,D5)
Prevalence	Ubiquity	D7
	Deployment Scale	D8
	Remaining Period of Use	D9
	Score:	=MAX(D7, D8)*0.8+0.2*(D9)
Technical Characteristics	Network Enablement	D11
	Complexity	D12
	Scope of Control	D13
	Score:	=(0.5*D11)+(0.3*D12)+(0.2*D13)
Mitigations	Continuing Support	
	Deployability	
	Score:	
	CyTRICS PRIORITIZATION SCORE:	**=(0.39*D6)+(0.39*D10)+(0.22*D14)**

3.3. Algorithms for Combining Factor Scores

After a scoring and ranking system has been developed, it is useful to look for examples that confirm intuition or may result in a counterintuitive ranking. To this end, consider the Impact factors: Operational, Safety, and Environmental. As indicated in the table, the algorithm used to combine these three factors is a maximum of the scores, Max(Operational, Safety, Environment).

Consider an example ranking of two systems. One system is a SCADA system deployed in an electric transmission environment. Assume an attack on this system would have a **High** Operational Impact. Further assume that the Safety Impact would be **Low** and Environmental Impact would be **Low**.

The second system is a SCADA system in a midstream pipeline environment. Assume an attack on this system would have a **High** Operational Impact, a **High** safety Impact and a **High** Environmental Impact.

The algorithm to score the systems is the Max of the three scores. Hence, the smart meter would score Max (High, Low, Low) = High and the transformer monitor would score Max (High, High, High) = High. This result of equal overall Impact scores seems counterintuitive. The two additional high scores for the transformer temperature monitor have no impact on the ranking.

In addition, there is a general ambiguity about the calculus for combining discrete levels of different factors. Some examples are shown below. It is not clear which system should be ranked higher. Explicit elicitation of the inequalities could be conducted, but a large number of elicitations would be required. For example, for scales with five discrete levels, each inequality would require up to 15,625 elicitations from SMEs [2].

System 1(Low, Low, High) <? System 2(Med, Med, Med)

System 3(Low, High, High) <? System 4(Med, Med, Med)

In contrast, such counterintuitive and ambiguous results are not possible using the weighted sum algorithm shown in the table for technical characteristics. Using the weighted sum algorithm used for technical characteristics guarantees that all factors are important to a greater or lesser degree. Furthermore, the weights that capture the relative importance of factors can be assessed through tradeoff questions. Tradeoff questions can be elicited from stakeholders using standard, well known, and accepted techniques. Finally, using numerical scales for each factor and a weighted sum algorithm to combine them would eliminate the need for the explicit inequality elicitations described above.

3.4. Numerical Scales for Factors

Factor scores need not take the form of discrete levels. Some factors could be expressed as continuous scales and the values normalized to the range 0-1. The Deployment Scale factor would be a good candidate to change from a discrete to continuous scale. The functional form of the Deployment Scale could take different mathematical forms depending upon the assumed relationship between the

[2] Five possible levels for each of three factor scores for the two systems being compared would be required to define the results for one inequality. One system could have 5^3 = 125 possible combinations of factor scores. The other system could also have 125 possible combinations. The total number of possible comparisons of the two system scores would be 125 x 125 = 16, 625.

number of systems deployed on the grid and the risk of discovery and compromise of a vulnerability in the system.

To illustrate these relationships, consider three deployment examples below.

1. If there are only 1,000 systems on the grid and they are easy for the adversary to find and attack. Assume that compromise of 100 would result in catastrophic grid failure. Under these conditions, having an additional 1,000 deployed would not increase risk significantly. Label this case "Beachhead."
2. If the system discovery and attack process is random, then the risk scales with the number of systems deployed. Label this case "linear."
3. If the systems are difficult to find and attack, a large population would be needed to present a significant risk. Label this case "need many."

The scoring functions for each of these three cases are shown by the orange, blue, and grey curves in Figure 5. The number of systems deployed has been normalized to (0-1) on the x axis and the score has been normalized to (0-1) on the y axis.

As indicated by the green "Beachhead" curve, the score or risk initially increases rapidly but then levels off because additional systems deployed on the grid do not significantly increase the risk. The blue "Linear" curve reflects a linear increase in risk in proportion to the number of systems deployed. The grey "Need many" curve shows a low risk until a significant number of systems are deployed on the grid. During elicitation, SMEs would be asked to identify which one of the three forms is appropriate. The decision analyst would change a parameter in the function to increase or decrease the curvature as directed by the SMEs.

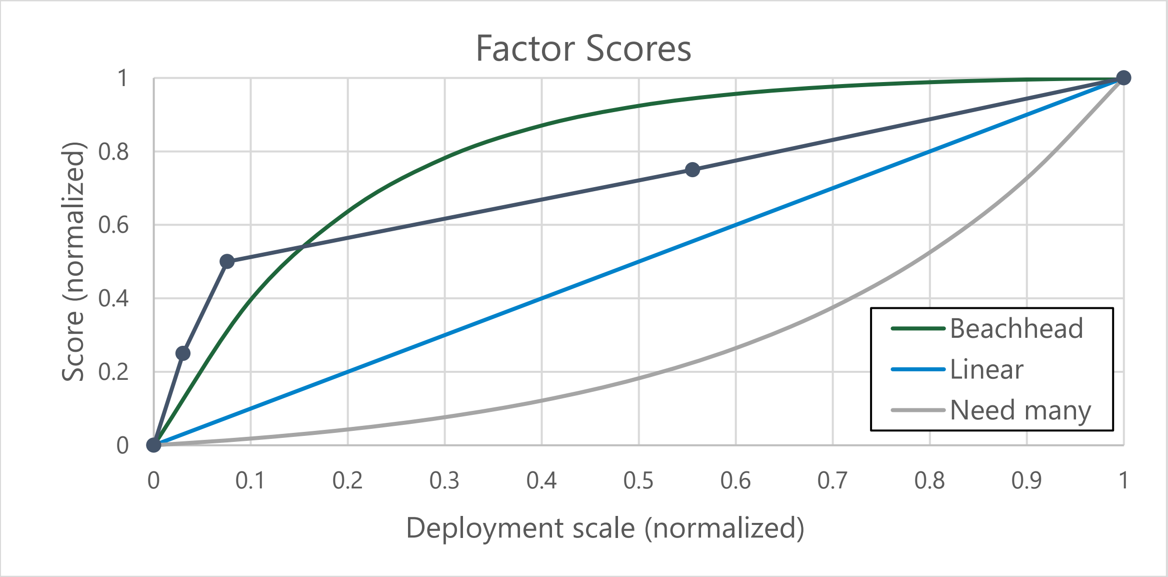


Figure 5 Alternative Forms of Factor Scores

The dark grey "Deployment" curve in the figure corresponds to the values currently used for the Deployment Scale. It reflects the beachhead property where only a few systems are needed to start and propagate an attack on the grid. The points for the five discrete levels in the scale are (1k,1), (1k-5k,2), (5k-10k,3), (10k-100k,4), and (100k,5). Using the midpoints of the ranges, the normalizing number deployed, and 1-5 values in scale, the corresponding points would be: (0,0), (0.030,0.25), (0.076,0.5), (0.56,0.75), (1.0,1.0). These data correspond to the dark grey curve in the figure.

3.5. Application of Scores

The scores will ultimately be used to determine which systems are selected for testing. Two basic approaches could be used: testing capacity-driven, or threshold-driven. If testing capacity is limited to x systems per period, the numerical scores could be used to identify the top x systems. These systems would then be tested. Alternatively, SME input could be used to establish a threshold for testing. SMEs would be shown a ranked list of systems. The SMEs would identify the dividing line between systems that posed a significant risk (and must be tested promptly) and the remaining systems that posed a lesser risk. The numerical score associated with this dividing line would be used as the threshold for testing in subsequent rankings.

3.6. Definition of System to be Scored

The challenge of defining systems to be scored has been previously discussed. Systems of different sizes must be mapped onto the same Deployment Scale to be compared. The deployment metric would suggest that a widely used system, smaller system is a much larger potential risk. In this example we could consider decomposing; the large, low deployment system would be decomposed into smaller subsystems or individual systems for scoring.

Another approach is to seek to reach a consensus among SMEs during the elicitation. For example, during elicitation, SME opinions may cluster into two or more groups. SMEs from different clusters could state the logic and evidence they used to reach the value they provided. Opposing opinions could be offered and debated until a consensus or impasse is reached. Elicitation systems are available that allow SMEs to vote autonomously using their phone to communicate their choice to the facilitator. The facilitator then displays the distribution of results to the group and outliers in the distribution are offered the chance to explain their reasoning if they choose to reveal themselves. A second or third anonymous vote can sometimes converge to a consensus opinion.

Appendices

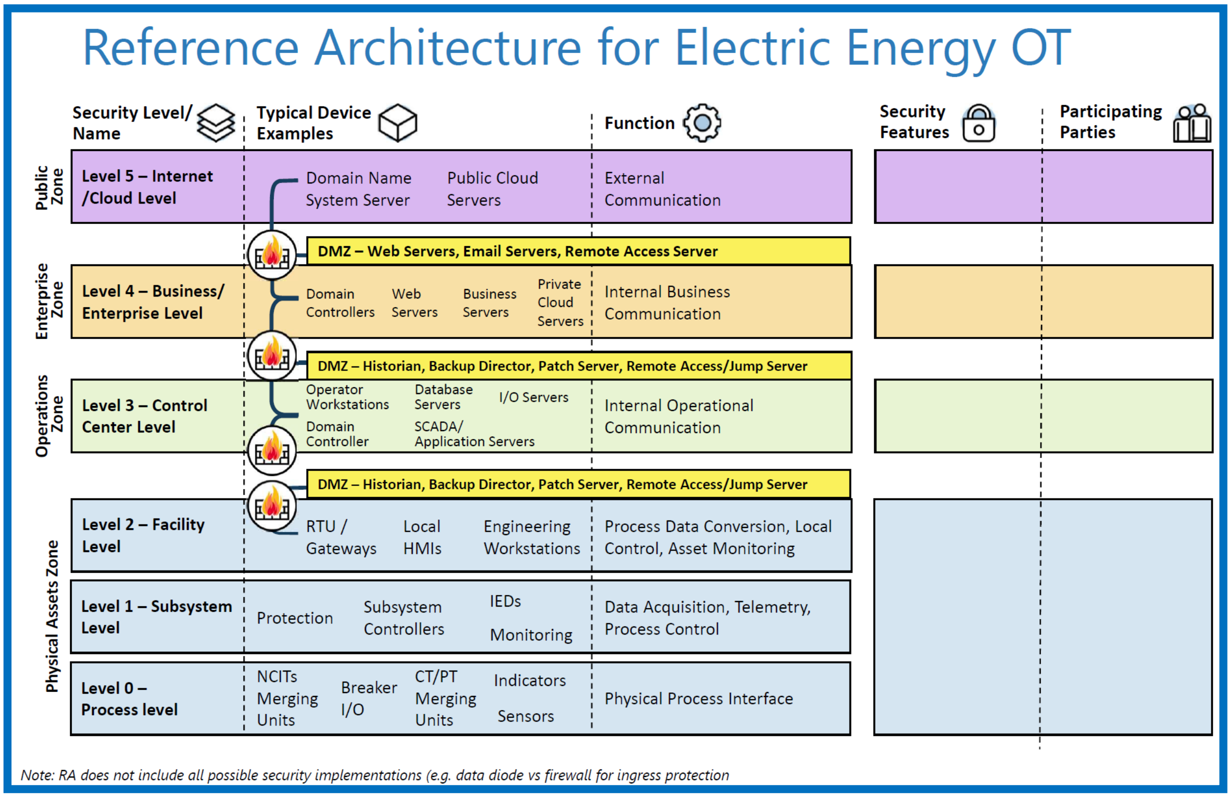
5. Appendix A: Examples of Assumptions Necessary for Scoring

Reference Architecture Examples

Reference architectures are helpful in framing the prioritization discussion. They help visually convey communications and control connectivity that systems have based on where they are installed. A challenge with reference architectures is finding one that includes sufficient detail but does not contain information that may make vendor partners uncomfortable.

Reference Architectures for the Electric Sector

The following reference architectures were developed by the Securing Energy Infrastructure Executive Task Force.

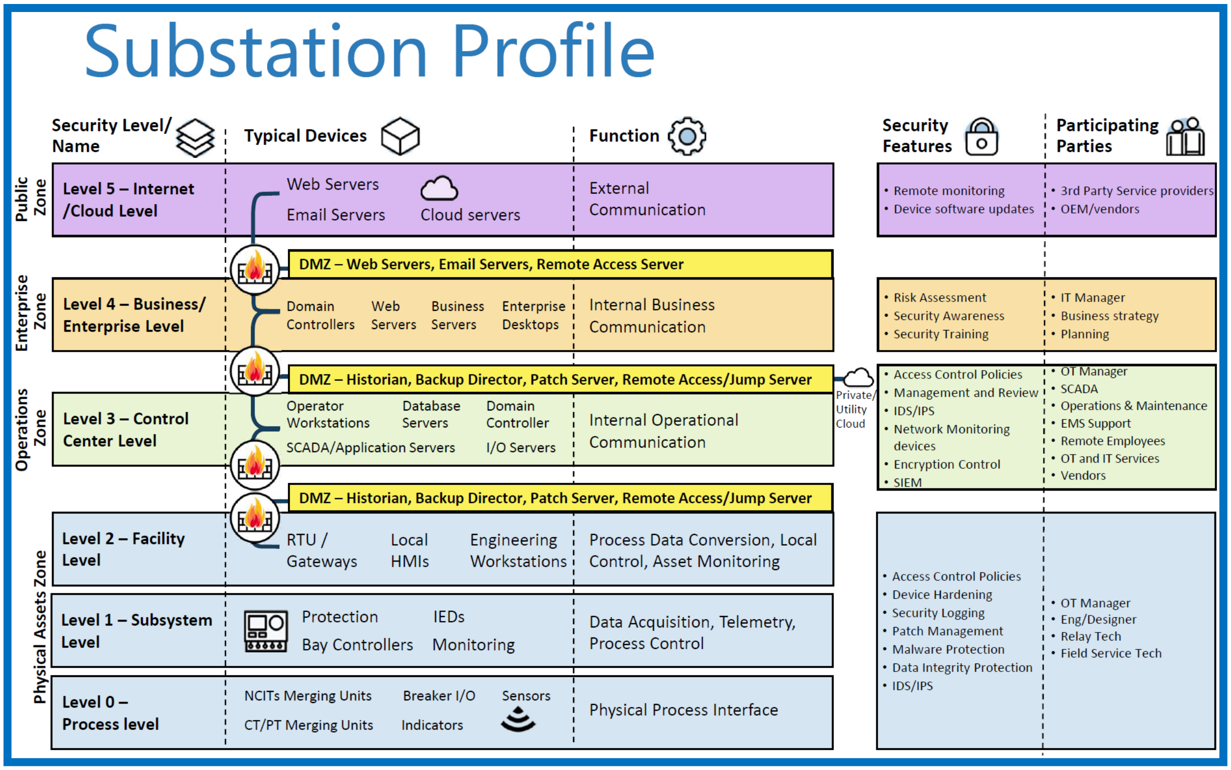


Reference Architecture for Electric Energy OT

	Security Level/ Name	Typical Device Examples	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet /Cloud Level	Domain Name System Server Public Cloud Servers	External Communication		
	DMZ – Web Servers, Email Servers, Remote Access Server				
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Web Servers Business Servers Private Cloud Servers	Internal Business Communication		
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server				
Operations Zone	Level 3 – Control Center Level	Operator Workstations Database Servers I/O Servers Domain Controller SCADA/ Application Servers	Internal Operational Communication		
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server				
Physical Assets Zone	Level 2 – Facility Level	RTU / Gateways Local HMIs Engineering Workstations	Process Data Conversion, Local Control, Asset Monitoring		
	Level 1 – Subsystem Level	Protection Subsystem Controllers IEDs Monitoring	Data Acquisition, Telemetry, Process Control		
	Level 0 – Process level	NCITs Merging Units Breaker I/O CT/PT Merging Units Indicators Sensors	Physical Process Interface		

Note: RA does not include all possible security implementations (e.g. data diode vs firewall for ingress protection

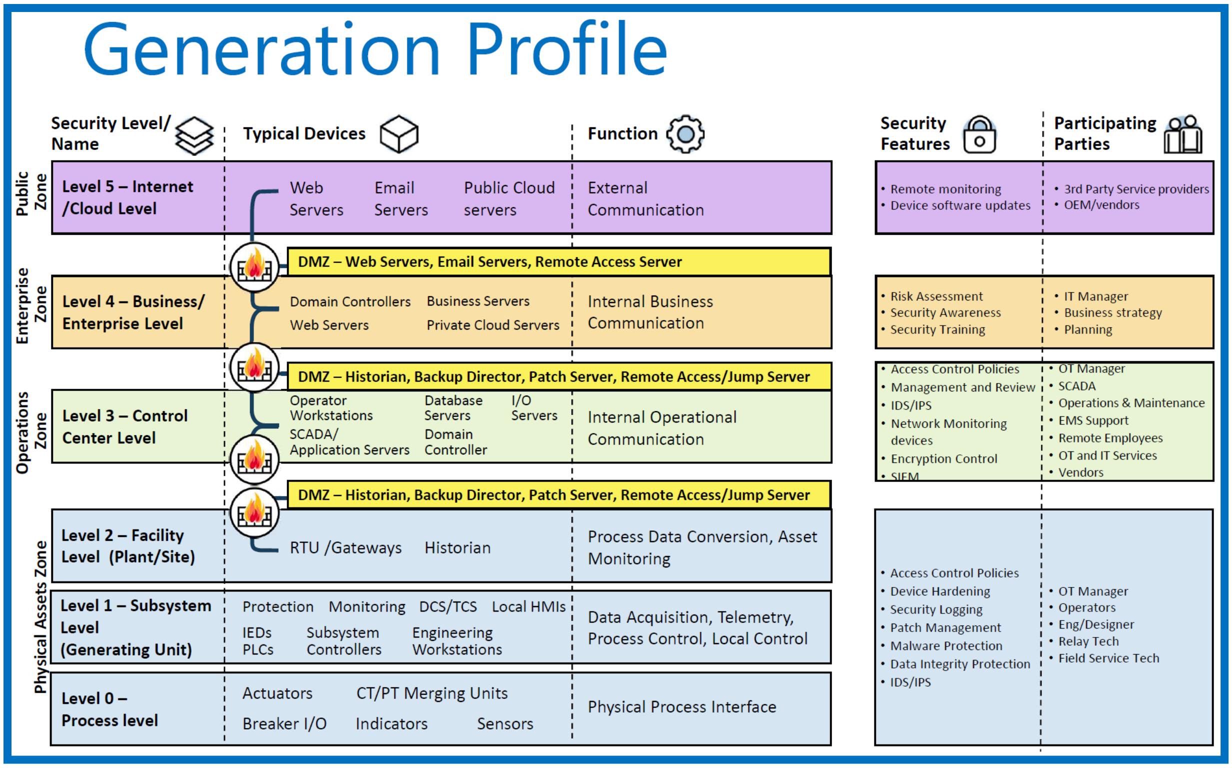
Figure 15: Reference architecture for generic electric sector operational technology.[i]



Substation Profile

Zone	Security Level/ Name	Typical Devices	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet /Cloud Level	Web Servers Email Servers Cloud servers	External Communication	• Remote monitoring • Device software updates	• 3rd Party Service providers • OEM/vendors
	DMZ – Web Servers, Email Servers, Remote Access Server				
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Web Servers Business Servers Enterprise Desktops	Internal Business Communication	• Risk Assessment • Security Awareness • Security Training	• IT Manager • Business strategy • Planning
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server		Private/ Utility Cloud		
Operations Zone	Level 3 – Control Center Level	Operator Workstations Database Servers Domain Controller SCADA/Application Servers I/O Servers	Internal Operational Communication	• Access Control Policies • Management and Review • IDS/IPS • Network Monitoring devices • Encryption Control • SIEM	• OT Manager • SCADA • Operations & Maintenance • EMS Support • Remote Employees • OT and IT Services • Vendors
	DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server				
Physical Assets Zone	Level 2 – Facility Level	RTU / Gateways Local HMIs Engineering Workstations	Process Data Conversion, Local Control, Asset Monitoring	• Access Control Policies • Device Hardening • Security Logging • Patch Management • Malware Protection • Data Integrity Protection • IDS/IPS	• OT Manager • Eng/Designer • Relay Tech • Field Service Tech
	Level 1 – Subsystem Level	Protection IEDs Bay Controllers Monitoring	Data Acquisition, Telemetry, Process Control		
	Level 0 – Process level	NCITs Merging Units Breaker I/O Sensors CT/PT Merging Units Indicators	Physical Process Interface		

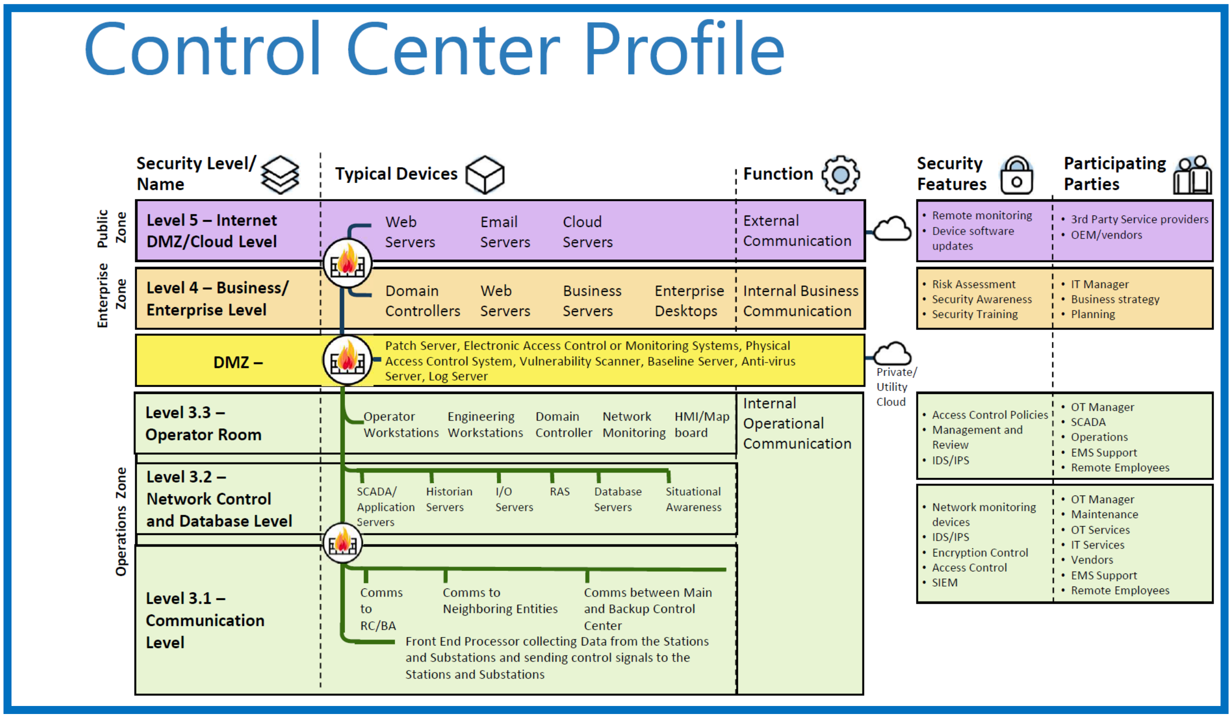
Figure 26: Reference architecture for an electric sector substation.[ii]



Generation Profile

Zone	Security Level/ Name	Typical Devices	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet /Cloud Level	Web Servers Email Servers Public Cloud servers	External Communication	• Remote monitoring • Device software updates	• 3rd Party Service providers • OEM/vendors
		DMZ – Web Servers, Email Servers, Remote Access Server			
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Business Servers Web Servers Private Cloud Servers	Internal Business Communication	• Risk Assessment • Security Awareness • Security Training	• IT Manager • Business strategy • Planning
		DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server			
Operations Zone	Level 3 – Control Center Level	Operator Workstations Database Servers I/O Servers SCADA/ Application Servers Domain Controller	Internal Operational Communication	• Access Control Policies • Management and Review • IDS/IPS • Network Monitoring devices • Encryption Control • SIEM	• OT Manager • SCADA • Operations & Maintenance • EMS Support • Remote Employees • OT and IT Services • Vendors
		DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server			
Physical Assets Zone	Level 2 – Facility Level (Plant/Site)	RTU /Gateways Historian	Process Data Conversion, Asset Monitoring	• Access Control Policies • Device Hardening • Security Logging • Patch Management • Malware Protection • Data Integrity Protection • IDS/IPS	• OT Manager • Operators • Eng/Designer • Relay Tech • Field Service Tech
	Level 1 – Subsystem Level (Generating Unit)	Protection Monitoring DCS/TCS Local HMIs IEDs PLCs Subsystem Controllers Engineering Workstations	Data Acquisition, Telemetry, Process Control, Local Control		
	Level 0 – Process level	Actuators CT/PT Merging Units Breaker I/O Indicators Sensors	Physical Process Interface		

Figure 37: Reference architecture for an electric sector generation site.[iii]



Control Center Profile

Zone	Security Level/ Name	Typical Devices	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet DMZ/Cloud Level	Web Servers Email Servers Cloud Servers	External Communication	• Remote monitoring • Device software updates	• 3rd Party Service providers • OEM/vendors
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Web Servers Business Servers Enterprise Desktops	Internal Business Communication	• Risk Assessment • Security Awareness • Security Training	• IT Manager • Business strategy • Planning
	DMZ –	Patch Server, Electronic Access Control or Monitoring Systems, Physical Access Control System, Vulnerability Scanner, Baseline Server, Anti-virus Server, Log Server	Private/ Utility Cloud		
Operations Zone	Level 3.3 – Operator Room	Operator Workstations Engineering Workstations Domain Controller Network Monitoring HMI/Map board	Internal Operational Communication	• Access Control Policies • Management and Review • IDS/IPS	• OT Manager • SCADA • Operations • EMS Support • Remote Employees
	Level 3.2 – Network Control and Database Level	SCADA/ Application Servers Historian Servers I/O Servers RAS Database Servers Situational Awareness		• Network monitoring devices • IDS/IPS • Encryption Control • Access Control • SIEM	• OT Manager • Maintenance • OT Services • IT Services • Vendors • EMS Support • Remote Employees
	Level 3.1 – Communication Level	Comms to RC/BA Comms to Neighboring Entities Comms between Main and Backup Control Center Front End Processor collecting Data from the Stations and Substations and sending control signals to the Stations and Substations			

Figure 48: Reference architecture for an electric sector control center.[iv]

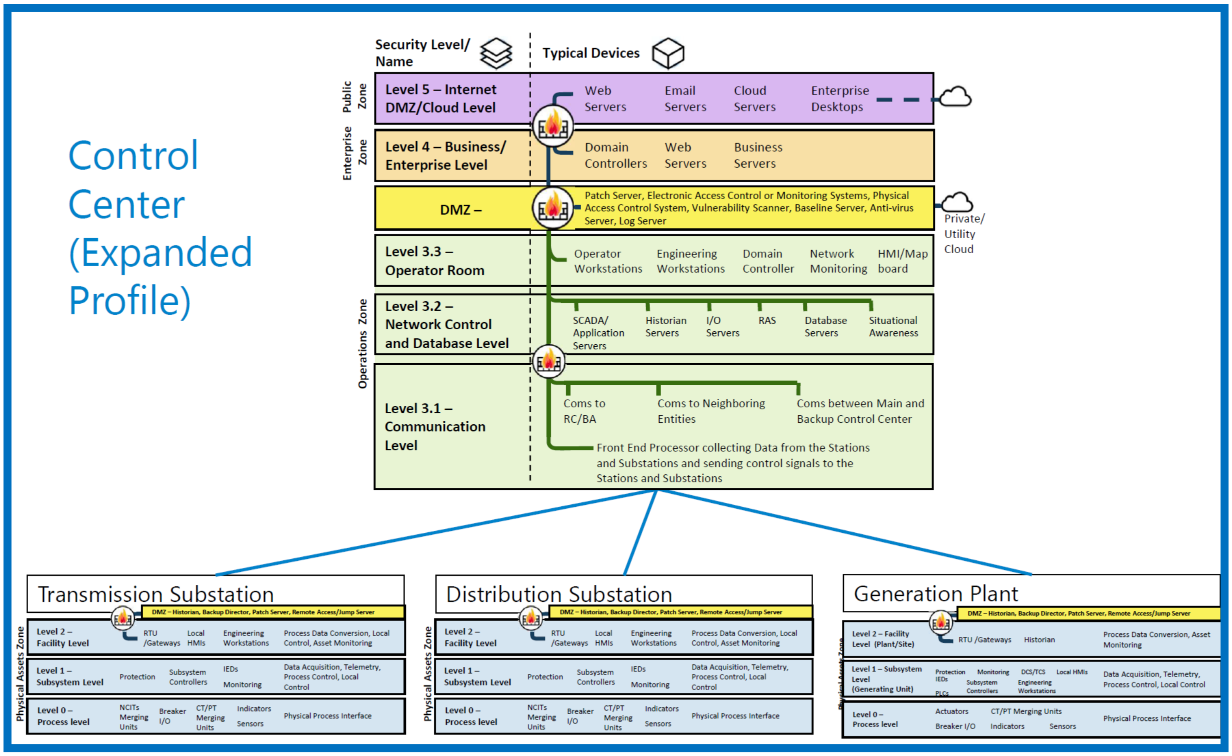

Control Center (Expanded Profile)
Security Level/ Name
Typical Devices
Public Zone
Level 5 – Internet DMZ/Cloud Level
Web Servers
Email Servers
Cloud Servers
Enterprise Desktops
Enterprise Zone
Level 4 – Business/ Enterprise Level
Domain Controllers
Web Servers
Business Servers
DMZ –
Patch Server, Electronic Access Control or Monitoring Systems, Physical Access Control System, Vulnerability Scanner, Baseline Server, Anti-virus Server, Log Server
Private/ Utility Cloud
Operations Zone
Level 3.3 – Operator Room
Operator Workstations
Engineering Workstations
Domain Controller
Network Monitoring
HMI/Map board
Level 3.2 – Network Control and Database Level
SCADA/ Application Servers
Historian Servers
I/O Servers
RAS
Database Servers
Situational Awareness
Level 3.1 – Communication Level
Coms to RC/BA
Coms to Neighboring Entities
Coms between Main and Backup Control Center
Front End Processor collecting Data from the Stations and Substations and sending control signals to the Stations and Substations
Transmission Substation
DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server
Physical Assets Zone
Level 2 – Facility Level
RTU /Gateways
Local HMIs
Engineering Workstations
Process Data Conversion, Local Control, Asset Monitoring
Level 1 – Subsystem Level
Protection
Subsystem Controllers
IEDs
Monitoring
Data Acquisition, Telemetry, Process Control, Local Control
Level 0 – Process level
NCITs Merging Units
Breaker I/O
CT/PT Merging Units
Indicators
Sensors
Physical Process Interface
Distribution Substation
DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server
Physical Assets Zone
Level 2 – Facility Level
RTU /Gateways
Local HMIs
Engineering Workstations
Process Data Conversion, Local Control, Asset Monitoring
Level 1 – Subsystem Level
Protection
Subsystem Controllers
IEDs
Monitoring
Data Acquisition, Telemetry, Process Control, Local Control
Level 0 – Process level
NCITs Merging Units
Breaker I/O
CT/PT Merging Units
Indicators
Sensors
Physical Process Interface
Generation Plant
DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server
Physical Assets Zone
Level 2 – Facility Level (Plant/Site)
RTU /Gateways
Historian
Process Data Conversion, Asset Monitoring
Level 1 – Subsystem Level (Generating Unit)
Protection IEDs
PLCs
Monitoring
Subsystem Controllers
DCS/TCS
Engineering Workstations
Local HMIs
Data Acquisition, Telemetry, Process Control, Local Control
Level 0 – Process level
Actuators
Breaker I/O
CT/PT Merging Units
Indicators
Sensors
Physical Process Interface

Figure 59: Expanded reference architecture for an electric sector control center.[v]

Reference Architectures for Oil and Gas Sectors

The oil and gas sectors require different reference architectures due to their unique functionality.

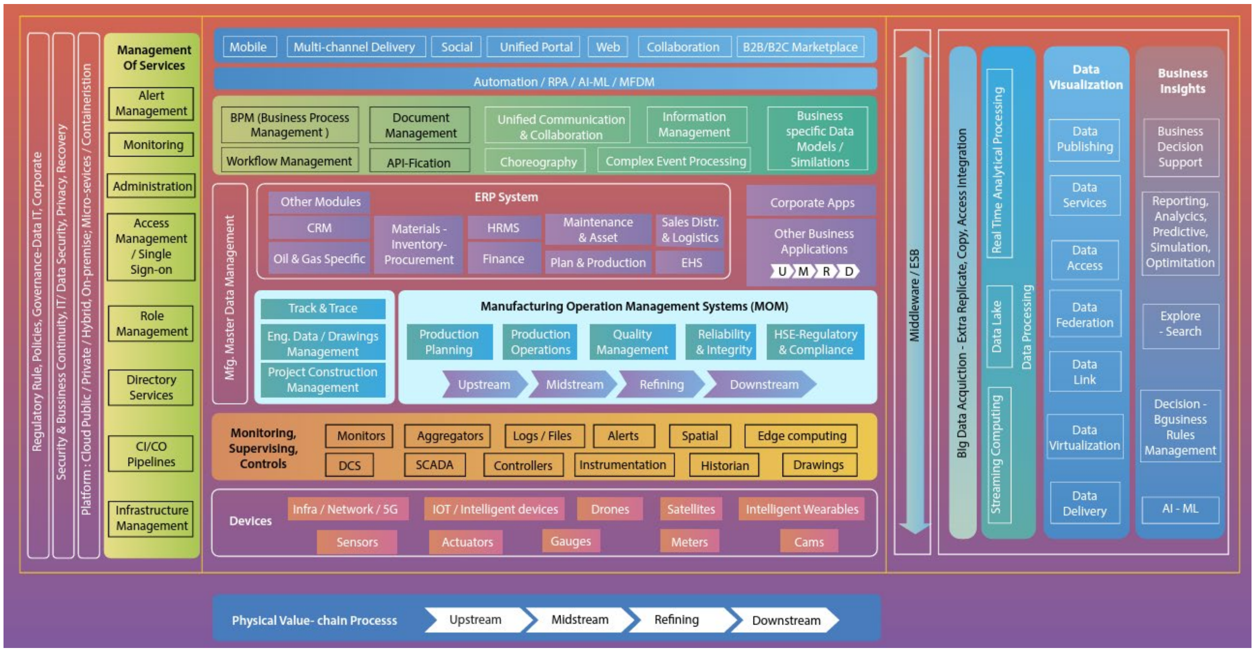


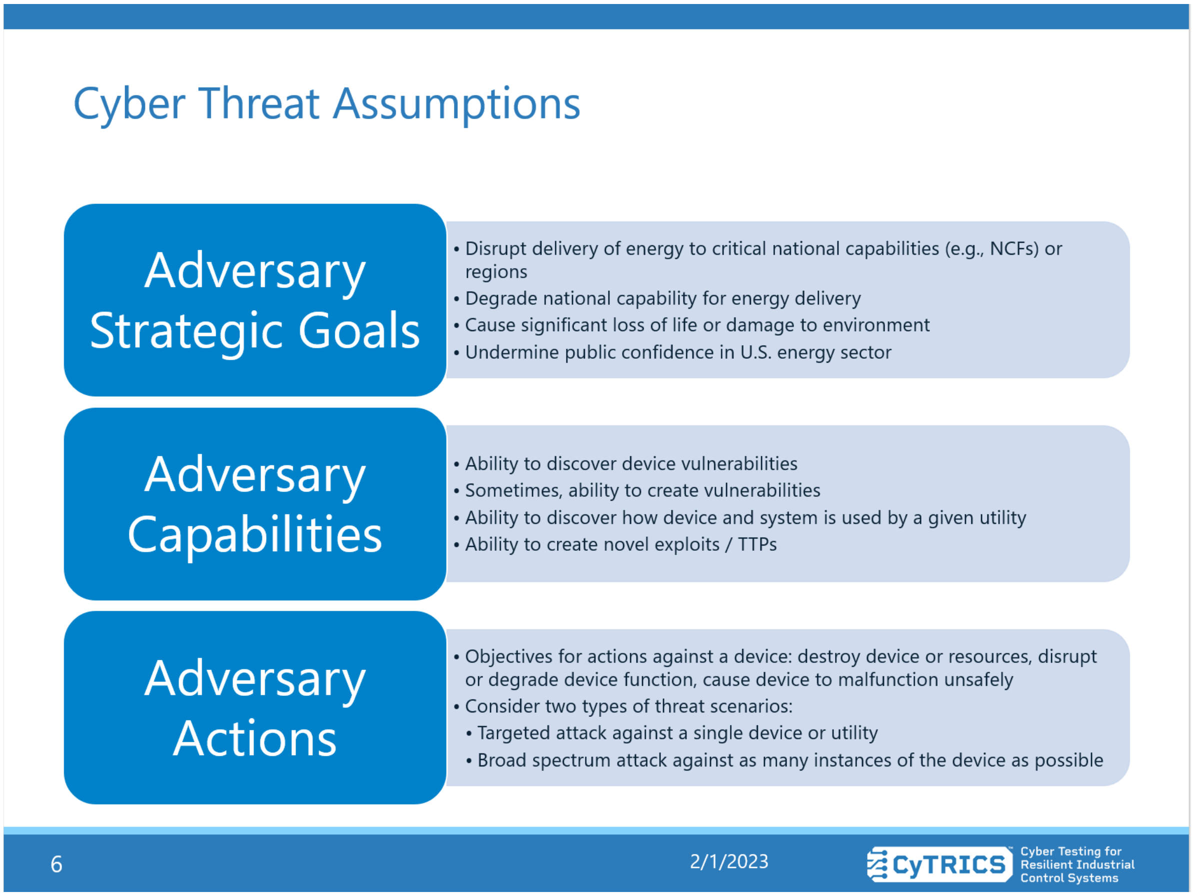
Figure 610: Reference architecture for oil and gas.[vi]

Operational Use Case Examples

Operational use cases are dependent on the system being prioritized, including capabilities and the reference architecture it is assumed to be installed in. The CFT and SMEs should determine the functionality of the system during the facilitation session. For example, is the system being used as a data concentrator, a protocol converter, or does it possess control functionality over other systems installed in the same reference architecture?

Threat Assumption Discussion

The CyTRICS Prioritization process makes a series of assumptions regarding adversary goals, capabilities, and actions.



Cyber Threat Assumptions

Adversary Strategic Goals

- Disrupt delivery of energy to critical national capabilities (e.g., NCFs) or regions
- Degrade national capability for energy delivery
- Cause significant loss of life or damage to environment
- Undermine public confidence in U.S. energy sector

Adversary Capabilities

- Ability to discover device vulnerabilities
- Sometimes, ability to create vulnerabilities
- Ability to discover how device and system is used by a given utility
- Ability to create novel exploits / TTPs

Adversary Actions

- Objectives for actions against a device: destroy device or resources, disrupt or degrade device function, cause device to malfunction unsafely
- Consider two types of threat scenarios:
  - Targeted attack against a single device or utility
  - Broad spectrum attack against as many instances of the device as possible

6

2/1/2023

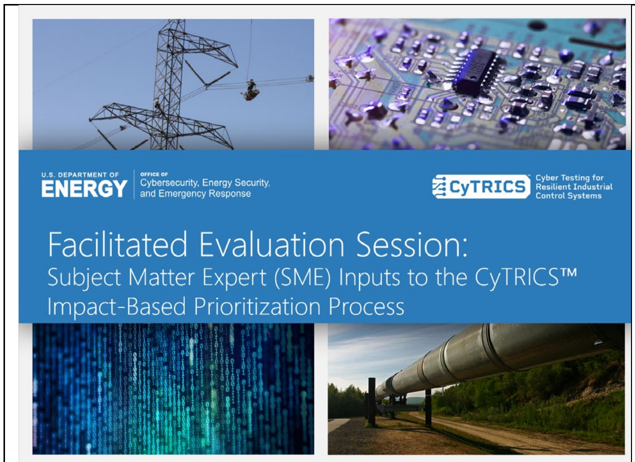
CyTRICS™ Cyber Testing for Resilient Industrial Control Systems

Figure 711: Cyber Threat Assumptions slide from the CFT Interview Instrument.

6. Appendix B: Instruments Used for Prioritization

CFT Interview Instrument

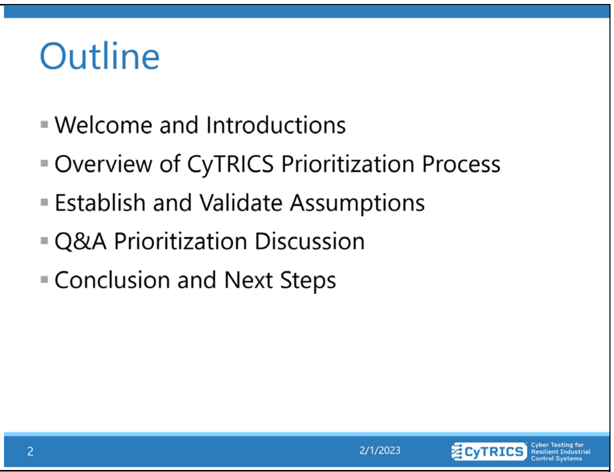
This is an example of a PowerPoint slide deck used to guide the facilitated evaluation session with the SMEs. It is provided as an example of how to frame discussions and elicit values and assumptions from SMEs.



U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response
CyTRICS Cyber Testing for Resilient Industrial Control Systems

Facilitated Evaluation Session:
Subject Matter Expert (SME) Inputs to the CyTRICS™ Impact-Based Prioritization Process

Slide 1 of the SME Interview Instrument.

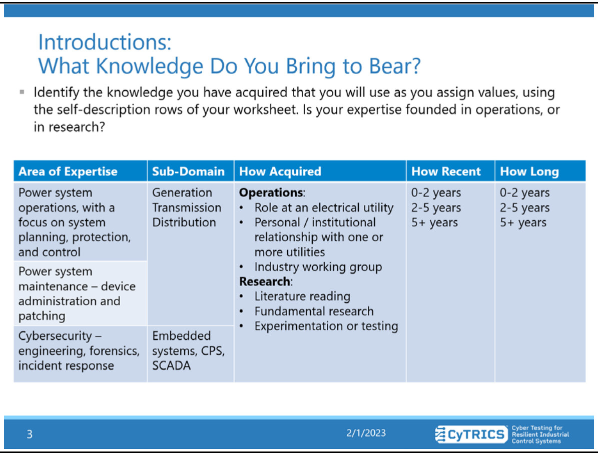


Outline

- Welcome and Introductions
- Overview of CyTRICS Prioritization Process
- Establish and Validate Assumptions
- Q&A Prioritization Discussion
- Conclusion and Next Steps

2 2/1/2023 CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 2 of the SME Interview Instrument.



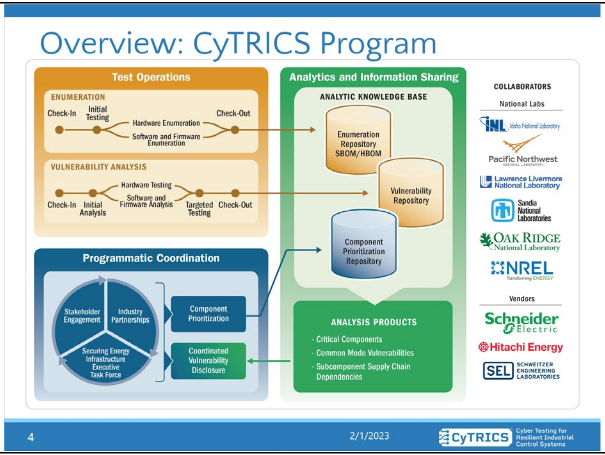
Introductions:
What Knowledge Do You Bring to Bear?

- Identify the knowledge you have acquired that you will use as you assign values, using the self-description rows of your worksheet. Is your expertise founded in operations, or in research?

Area of Expertise	Sub-Domain	How Acquired	How Recent	How Long
Power system operations, with a focus on system planning, protection, and control	Generation Transmission Distribution	**Operations**: • Role at an electrical utility • Personal / institutional relationship with one or more utilities • Industry working group **Research**: • Literature reading • Fundamental research • Experimentation or testing	0-2 years 2-5 years 5+ years	0-2 years 2-5 years 5+ years
Power system maintenance – device administration and patching				
Cybersecurity – engineering, forensics, incident response	Embedded systems, CPS, SCADA			

3 2/1/2023 CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 3 of the SME Interview Instrument.

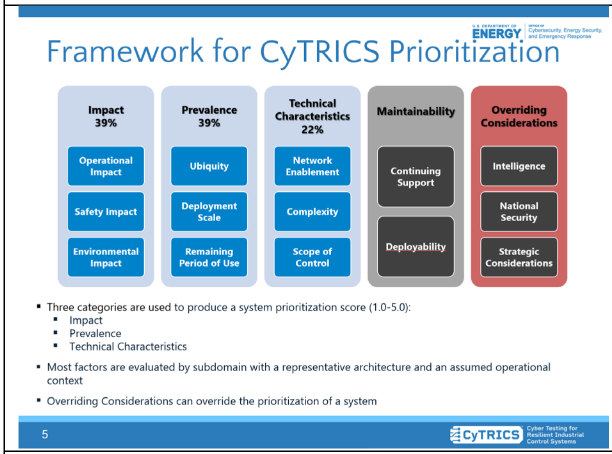


Overview: CyTRICS Program

Test Operations
ENUMERATION
Check-In
Initial Testing
Hardware Enumeration
Software and Firmware Enumeration
Check-Out
VULNERABILITY ANALYSIS
Check-In
Initial Analysis
Hardware Testing
Software and Firmware Analysis
Targeted Testing
Check-Out
Programmatic Coordination
Stakeholder Engagement
Industry Partnerships
Securing Energy Infrastructure Executive Task Force
Component Prioritization
Coordinated Vulnerability Disclosure
Analytics and Information Sharing
ANALYTIC KNOWLEDGE BASE
Enumeration Repository SBOM/HBOM
Vulnerability Repository
Component Prioritization Repository
ANALYSIS PRODUCTS
· Critical Components
· Common Mode Vulnerabilities
· Subcomponent Supply Chain Dependencies
COLLABORATORS
National Labs
INL Idaho National Laboratory
Pacific Northwest National Laboratory
Lawrence Livermore National Laboratory
Sandia National Laboratories
Oak Ridge National Laboratory
NREL Transforming ENERGY
Vendors
Schneider Electric
Hitachi Energy
SEL Schweitzer Engineering Laboratories

4 2/1/2023 CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 4 of the SME Interview Instrument.



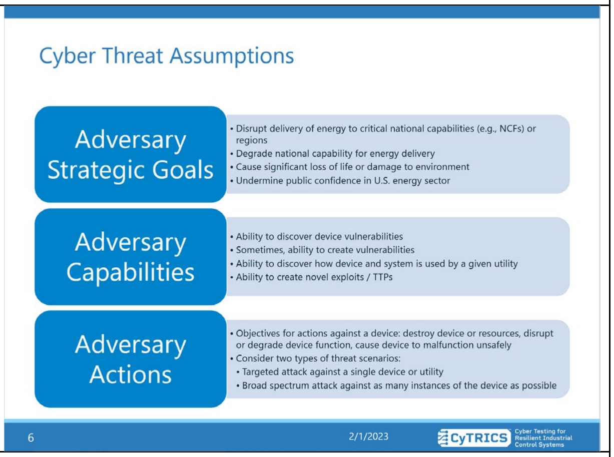
U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Framework for CyTRICS Prioritization

- Three categories are used to produce a system prioritization score (1.0-5.0):
  - Impact
  - Prevalence
  - Technical Characteristics
- Most factors are evaluated by subdomain with a representative architecture and an assumed operational context
- Overriding Considerations can override the prioritization of a system

5 CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 5 of the SME Interview Instrument.



Cyber Threat Assumptions

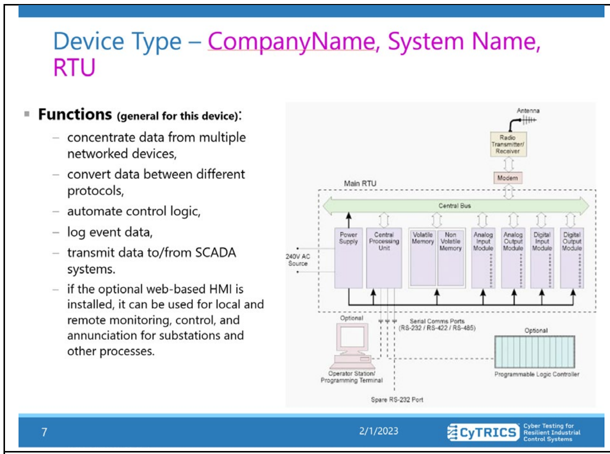
Adversary Strategic Goals
- Disrupt delivery of energy to critical national capabilities (e.g., NCFs) or regions
- Degrade national capability for energy delivery
- Cause significant loss of life or damage to environment
- Undermine public confidence in U.S. energy sector

Adversary Capabilities
- Ability to discover device vulnerabilities
- Sometimes, ability to create vulnerabilities
- Ability to discover how device and system is used by a given utility
- Ability to create novel exploits / TTPs

Adversary Actions
- Objectives for actions against a device: destroy device or resources, disrupt or degrade device function, cause device to malfunction unsafely
- Consider two types of threat scenarios:
  - Targeted attack against a single device or utility
  - Broad spectrum attack against as many instances of the device as possible

6 2/1/2023 CyTRICS Cyber Testing for Resilient Industrial Control Systems

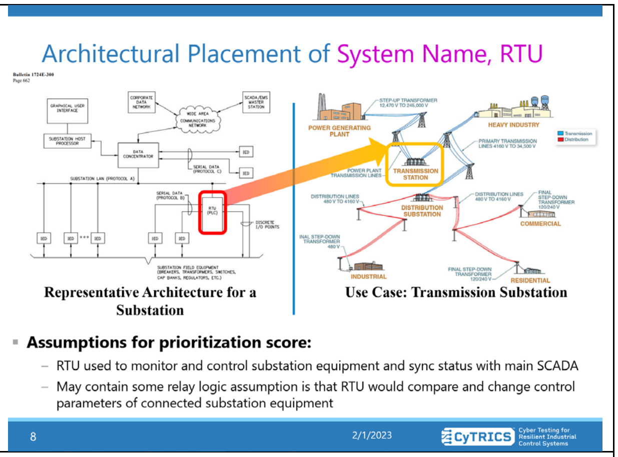
Slide 6 of the SME Interview Instrument.



Device Type – CompanyName, System Name, RTU

- **Functions** (general for this device):
  - concentrate data from multiple networked devices,
  - convert data between different protocols,
  - automate control logic,
  - log event data,
  - transmit data to/from SCADA systems.
  - if the optional web-based HMI is installed, it can be used for local and remote monitoring, control, and annunciation for substations and other processes.

Slide 7 of the SME Interview Instrument.



Architectural Placement of System Name, RTU

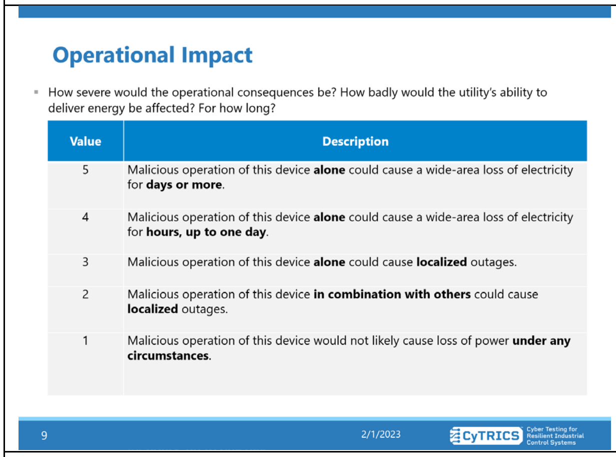
Bulletin 1724E-300
Page 662
GRAPHICAL USER INTERFACE
CORPORATE DATA NETWORK
SCADA/EMS MASTER STATION
WIDE AREA COMMUNICATIONS NETWORK
SUBSTATION HOST PROCESSOR
DATA CONCENTRATOR
IED
SERIAL DATA (PROTOCOL C)
IED
SUBSTATION LAN (PROTOCOL A)
SERIAL DATA (PROTOCOL B)
RTU (PLC)
DISCRETE I/O POINTS
IED
IED
IED
IED
IED
SUBSTATION FIELD EQUIPMENT (BREAKERS, TRANSFORMERS, SWITCHES, CAP BANKS, REGULATORS, ETC.)
STEP-UP TRANSFORMER 12,470 V TO 245,000 V
POWER GENERATING PLANT
HEAVY INDUSTRY
Transmission
Distribution
PRIMARY TRANSMISSION LINES 4160 V TO 34,500 V
POWER PLANT TRANSMISSION LINES
TRANSMISSION STATION
DISTRIBUTION LINES 480 V TO 4160 V
DISTRIBUTION SUBSTATION
DISTRIBUTION LINES 480 V TO 4160 V
FINAL STEP-DOWN TRANSFORMER 120/240 V
COMMERCIAL
INAL STEP-DOWN TRANSFORMER 480 V
INDUSTRIAL
FINAL STEP-DOWN TRANSFORMER 120/240 V
RESIDENTIAL

Representative Architecture for a Substation

Use Case: Transmission Substation

- **Assumptions for prioritization score:**
  - RTU used to monitor and control substation equipment and sync status with main SCADA
  - May contain some relay logic assumption is that RTU would compare and change control parameters of connected substation equipment

Slide 8 of the SME Interview Instrument.

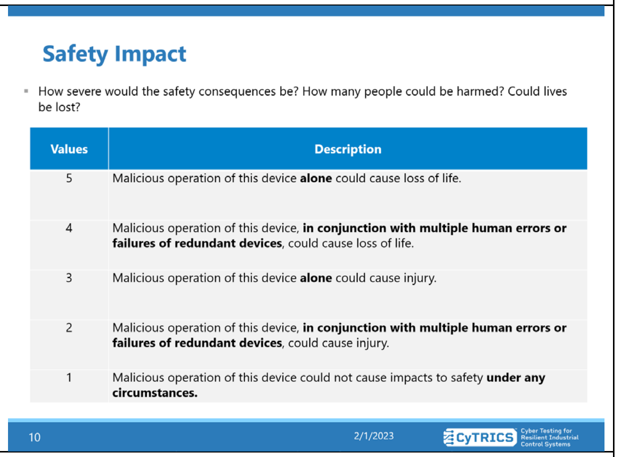


Operational Impact

- How severe would the operational consequences be? How badly would the utility's ability to deliver energy be affected? For how long?

Value	Description
5	Malicious operation of this device **alone** could cause a wide-area loss of electricity for **days or more**.
4	Malicious operation of this device **alone** could cause a wide-area loss of electricity for **hours, up to one day**.
3	Malicious operation of this device **alone** could cause **localized** outages.
2	Malicious operation of this device **in combination with others** could cause **localized** outages.
1	Malicious operation of this device would not likely cause loss of power **under any circumstances**.

Slide 9 of the SME Interview Instrument.

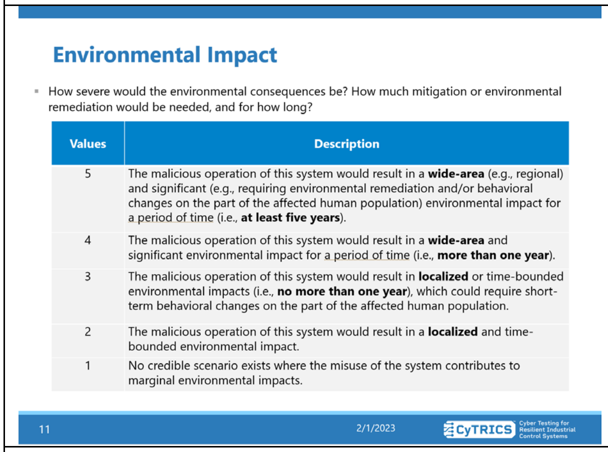


Safety Impact

- How severe would the safety consequences be? How many people could be harmed? Could lives be lost?

Values	Description
5	Malicious operation of this device **alone** could cause loss of life.
4	Malicious operation of this device, **in conjunction with multiple human errors or failures of redundant devices**, could cause loss of life.
3	Malicious operation of this device **alone** could cause injury.
2	Malicious operation of this device, **in conjunction with multiple human errors or failures of redundant devices**, could cause injury.
1	Malicious operation of this device could not cause impacts to safety **under any circumstances**.

Slide 10 of the SME Interview Instrument.

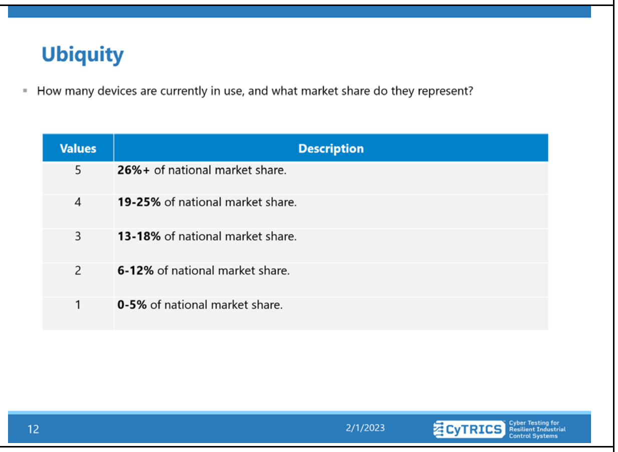


Environmental Impact

- How severe would the environmental consequences be? How much mitigation or environmental remediation would be needed, and for how long?

Values	Description
5	The malicious operation of this system would result in a **wide-area** (e.g., regional) and significant (e.g., requiring environmental remediation and/or behavioral changes on the part of the affected human population) environmental impact for a period of time (i.e., **at least five years**).
4	The malicious operation of this system would result in a **wide-area** and significant environmental impact for a period of time (i.e., **more than one year**).
3	The malicious operation of this system would result in **localized** or time-bounded environmental impacts (i.e., **no more than one year**), which could require short-term behavioral changes on the part of the affected human population.
2	The malicious operation of this system would result in a **localized** and time-bounded environmental impact.
1	No credible scenario exists where the misuse of the system contributes to marginal environmental impacts.

Slide 11 of the SME Interview Instrument.

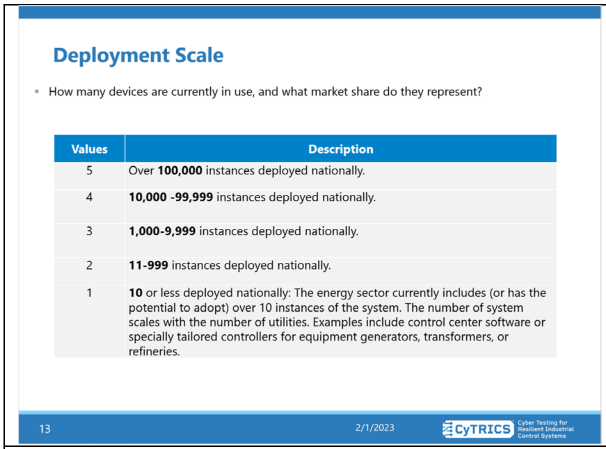


Ubiquity

- How many devices are currently in use, and what market share do they represent?

Values	Description
5	**26%+** of national market share.
4	**19-25%** of national market share.
3	**13-18%** of national market share.
2	**6-12%** of national market share.
1	**0-5%** of national market share.

Slide 12 of the SME Interview Instrument.



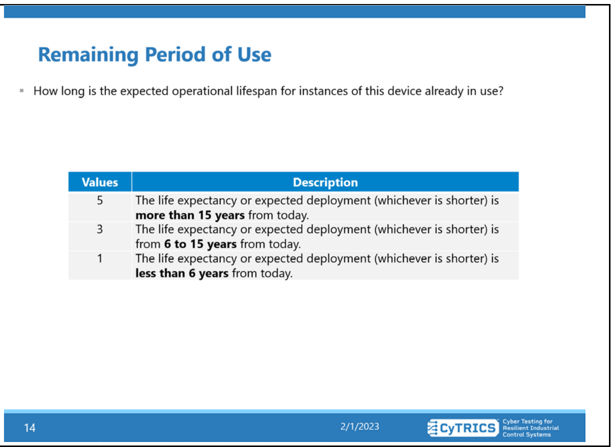
Deployment Scale

- How many devices are currently in use, and what market share do they represent?

Values	Description
5	Over **100,000** instances deployed nationally.
4	**10,000 -99,999** instances deployed nationally.
3	**1,000-9,999** instances deployed nationally.
2	**11-999** instances deployed nationally.
1	**10** or less deployed nationally: The energy sector currently includes (or has the potential to adopt) over 10 instances of the system. The number of system scales with the number of utilities. Examples include control center software or specially tailored controllers for equipment generators, transformers, or refineries.

13 2/1/2023 CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 13 of the SME Interview Instrument.



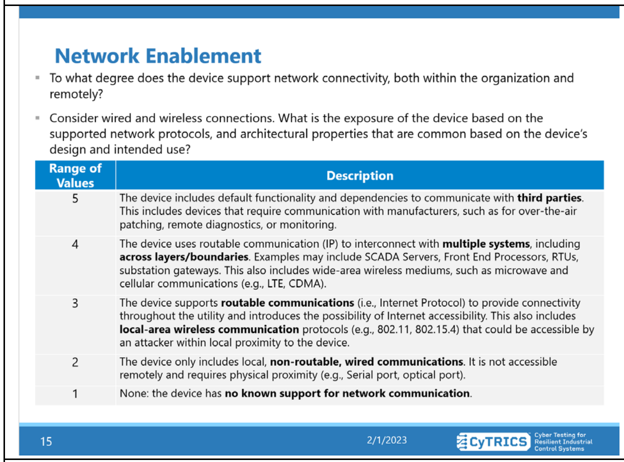
Remaining Period of Use

- How long is the expected operational lifespan for instances of this device already in use?

Values	Description
5	The life expectancy or expected deployment (whichever is shorter) is **more than 15 years** from today.
3	The life expectancy or expected deployment (whichever is shorter) is from **6 to 15 years** from today.
1	The life expectancy or expected deployment (whichever is shorter) is **less than 6 years** from today.

14 2/1/2023 CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 14 of the SME Interview Instrument.



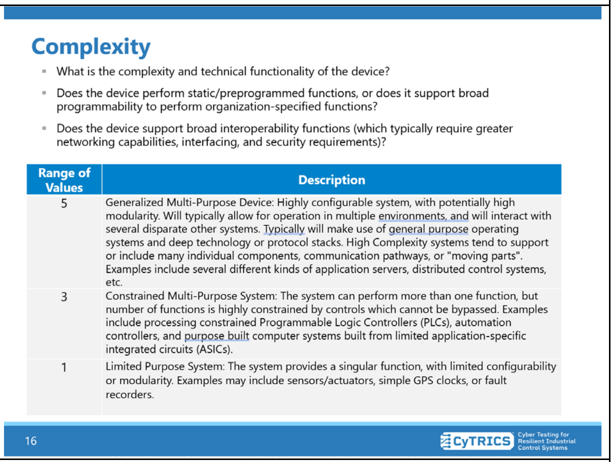
Network Enablement

- To what degree does the device support network connectivity, both within the organization and remotely?
- Consider wired and wireless connections. What is the exposure of the device based on the supported network protocols, and architectural properties that are common based on the device's design and intended use?

Range of Values	Description
5	The device includes default functionality and dependencies to communicate with **third parties**. This includes devices that require communication with manufacturers, such as for over-the-air patching, remote diagnostics, or monitoring.
4	The device uses routable communication (IP) to interconnect with **multiple systems**, including **across layers/boundaries**. Examples may include SCADA Servers, Front End Processors, RTUs, substation gateways. This also includes wide-area wireless mediums, such as microwave and cellular communications (e.g., LTE, CDMA).
3	The device supports **routable communications** (i.e., Internet Protocol) to provide connectivity throughout the utility and introduces the possibility of Internet accessibility. This also includes **local-area wireless communication** protocols (e.g., 802.11, 802.15.4) that could be accessible by an attacker within local proximity to the device.
2	The device only includes local, **non-routable, wired communications**. It is not accessible remotely and requires physical proximity (e.g., Serial port, optical port).
1	None: the device has **no known support for network communication**.

15 2/1/2023 CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 15 of the SME Interview Instrument.



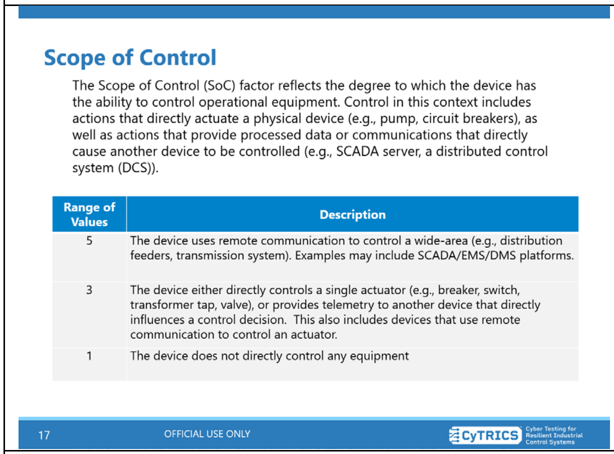
Complexity

- What is the complexity and technical functionality of the device?
- Does the device perform static/preprogrammed functions, or does it support broad programmability to perform organization-specified functions?
- Does the device support broad interoperability functions (which typically require greater networking capabilities, interfacing, and security requirements)?

Range of Values	Description
5	Generalized Multi-Purpose Device: Highly configurable system, with potentially high modularity. Will typically allow for operation in multiple environments, and will interact with several disparate other systems. Typically will make use of general purpose operating systems and deep technology or protocol stacks. High Complexity systems tend to support or include many individual components, communication pathways, or "moving parts". Examples include several different kinds of application servers, distributed control systems, etc.
3	Constrained Multi-Purpose System: The system can perform more than one function, but number of functions is highly constrained by controls which cannot be bypassed. Examples include processing constrained Programmable Logic Controllers (PLCs), automation controllers, and purpose built computer systems built from limited application-specific integrated circuits (ASICs).
1	Limited Purpose System: The system provides a singular function, with limited configurability or modularity. Examples may include sensors/actuators, simple GPS clocks, or fault recorders.

16 CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 16 of the SME Interview Instrument.



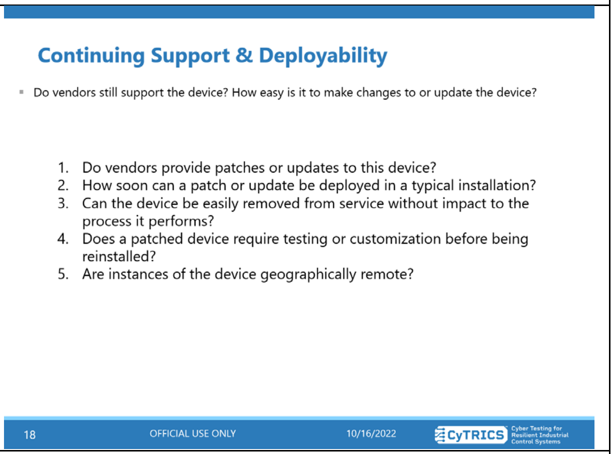
Scope of Control

The Scope of Control (SoC) factor reflects the degree to which the device has the ability to control operational equipment. Control in this context includes actions that directly actuate a physical device (e.g., pump, circuit breakers), as well as actions that provide processed data or communications that directly cause another device to be controlled (e.g., SCADA server, a distributed control system (DCS)).

Range of Values	Description
5	The device uses remote communication to control a wide-area (e.g., distribution feeders, transmission system). Examples may include SCADA/EMS/DMS platforms.
3	The device either directly controls a single actuator (e.g., breaker, switch, transformer tap, valve), or provides telemetry to another device that directly influences a control decision. This also includes devices that use remote communication to control an actuator.
1	The device does not directly control any equipment

17 OFFICIAL USE ONLY CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 17 of the SME Interview Instrument.



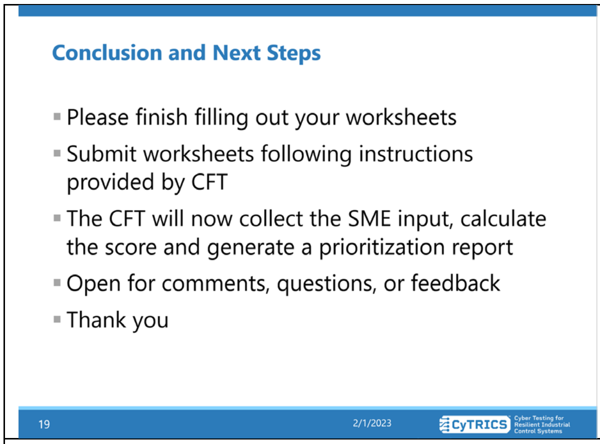
Continuing Support & Deployability

- Do vendors still support the device? How easy is it to make changes to or update the device?

1. Do vendors provide patches or updates to this device?
2. How soon can a patch or update be deployed in a typical installation?
3. Can the device be easily removed from service without impact to the process it performs?
4. Does a patched device require testing or customization before being reinstalled?
5. Are instances of the device geographically remote?

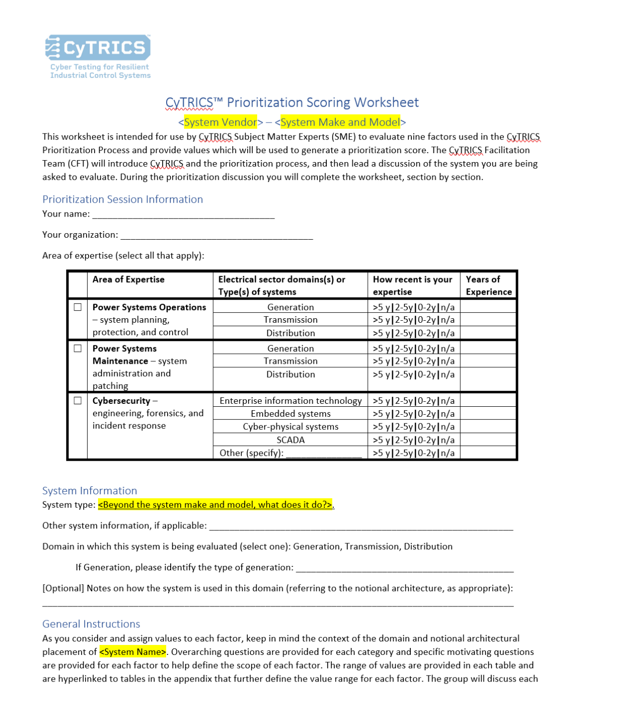
18 OFFICIAL USE ONLY 10/16/2022 CyTRICS Cyber Testing for Resilient Industrial Control Systems

Slide 18 of the SME Interview Instrument.

 **Conclusion and Next Steps** ▪ Please finish filling out your worksheets ▪ Submit worksheets following instructions provided by CFT ▪ The CFT will now collect the SME input, calculate the score and generate a prioritization report ▪ Open for comments, questions, or feedback ▪ Thank you 19 2/1/2023	
Slide 19 of the SME Interview Instrument.	

SME Prioritization Worksheet

This is an example of a SME Prioritization Worksheet used to collect input from SMEs. The CFT emails this to the SMEs prior to the facilitated prioritization session. The SMEs fill it out during the facilitated prioritization session and return it to the CFT when completed.



CyTRICS Cyber Testing for Resilient Industrial Control Systems

CyTRICS™ Prioritization Scoring Worksheet

<System Vendor> – <System Make and Model>

This worksheet is intended for use by CyTRICS Subject Matter Experts (SME) to evaluate nine factors used in the CyTRICS Prioritization Process and provide values which will be used to generate a prioritization score. The CyTRICS Facilitation Team (CFT) will introduce CyTRICS and the prioritization process, and then lead a discussion of the system you are being asked to evaluate. During the prioritization discussion you will complete the worksheet, section by section.

Prioritization Session Information

Your name: ____________________________________

Your organization: ______________________________________

Area of expertise (select all that apply):

	Area of Expertise	Electrical sector domains(s) or Type(s) of systems	How recent is your expertise	Years of Experience
☐	**Power Systems Operations** – system planning, protection, and control	Generation	>5 y|2-5y|0-2y|n/a	
		Transmission	>5 y|2-5y|0-2y|n/a	
		Distribution	>5 y|2-5y|0-2y|n/a	
☐	**Power Systems Maintenance** – system administration and patching	Generation	>5 y|2-5y|0-2y|n/a	
		Transmission	>5 y|2-5y|0-2y|n/a	
		Distribution	>5 y|2-5y|0-2y|n/a	
☐	**Cybersecurity** – engineering, forensics, and incident response	Enterprise information technology	>5 y|2-5y|0-2y|n/a	
		Embedded systems	>5 y|2-5y|0-2y|n/a	
		Cyber-physical systems	>5 y|2-5y|0-2y|n/a	
		SCADA	>5 y|2-5y|0-2y|n/a	
		Other (specify): _______________	>5 y|2-5y|0-2y|n/a	

System Information

System type: <Beyond the system make and model, what does it do?>.

Other system information, if applicable: ____

Domain in which this system is being evaluated (select one): Generation, Transmission, Distribution

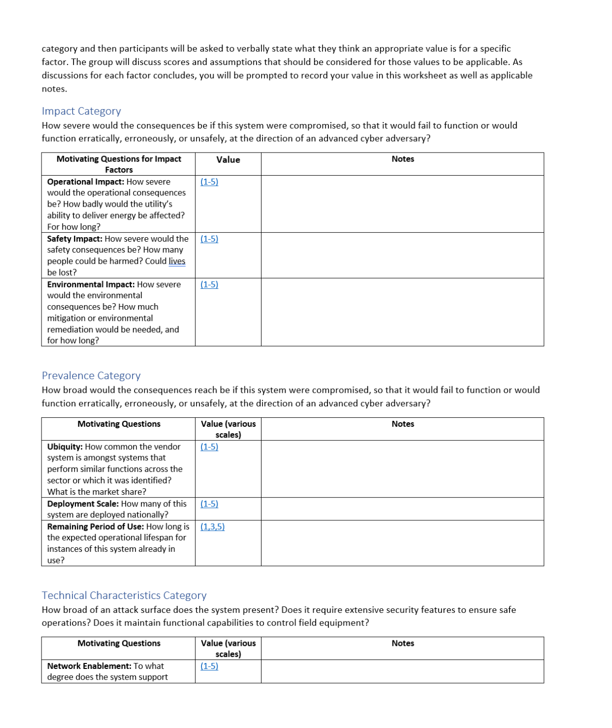
If Generation, please identify the type of generation: ____

[Optional] Notes on how the system is used in this domain (referring to the notional architecture, as appropriate):
____

General Instructions

As you consider and assign values to each factor, keep in mind the context of the domain and notional architectural placement of <System Name>. Overarching questions are provided for each category and specific motivating questions are provided for each factor to help define the scope of each factor. The range of values are provided in each table and are hyperlinked to tables in the appendix that further define the value range for each factor. The group will discuss each

Page 1 of the SME Prioritization Worksheet.



category and then participants will be asked to verbally state what they think an appropriate value is for a specific factor. The group will discuss scores and assumptions that should be considered for those values to be applicable. As discussions for each factor concludes, you will be prompted to record your value in this worksheet as well as applicable notes.

Impact Category

How severe would the consequences be if this system were compromised, so that it would fail to function or would function erratically, erroneously, or unsafely, at the direction of an advanced cyber adversary?

Motivating Questions for Impact Factors	Value	Notes
Operational Impact: How severe would the operational consequences be? How badly would the utility's ability to deliver energy be affected? For how long?	(1-5)	
Safety Impact: How severe would the safety consequences be? How many people could be harmed? Could lives be lost?	(1-5)	
Environmental Impact: How severe would the environmental consequences be? How much mitigation or environmental remediation would be needed, and for how long?	(1-5)	

Prevalence Category

How broad would the consequences reach be if this system were compromised, so that it would fail to function or would function erratically, erroneously, or unsafely, at the direction of an advanced cyber adversary?

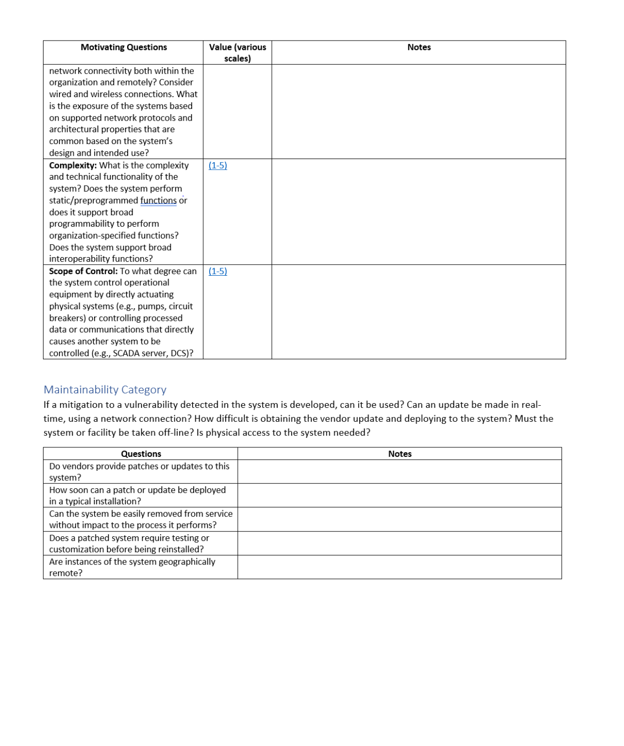
Motivating Questions	Value (various scales)	Notes
Ubiquity: How common the vendor system is amongst systems that perform similar functions across the sector or which it was identified? What is the market share?	(1-5)	
Deployment Scale: How many of this system are deployed nationally?	(1-5)	
Remaining Period of Use: How long is the expected operational lifespan for instances of this system already in use?	(1,3,5)	

Technical Characteristics Category

How broad of an attack surface does the system present? Does it require extensive security features to ensure safe operations? Does it maintain functional capabilities to control field equipment?

Motivating Questions	Value (various scales)	Notes
Network Enablement: To what degree does the system support	(1-5)	

Page 2 of the SME Prioritization Worksheet.

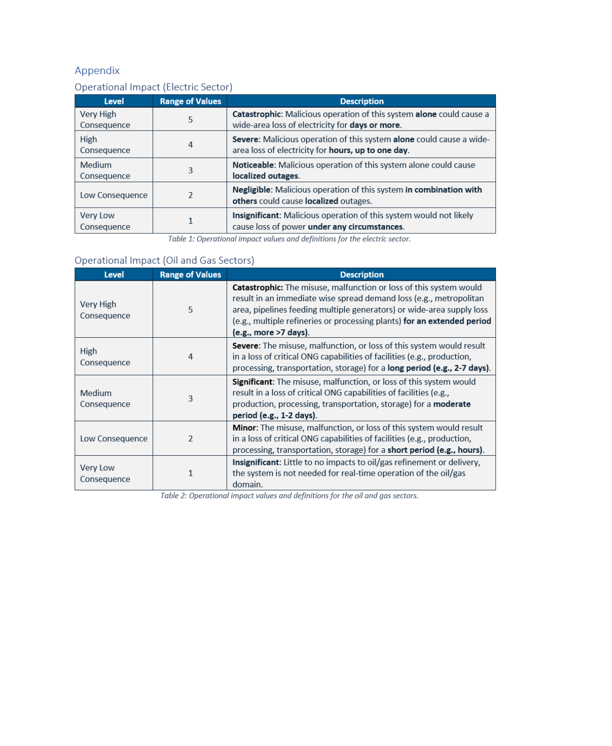


Motivating Questions	Value (various scales)	Notes
network connectivity both within the organization and remotely? Consider wired and wireless connections. What is the exposure of the systems based on supported network protocols and architectural properties that are common based on the system's design and intended use?		
Complexity: What is the complexity and technical functionality of the system? Does the system perform static/preprogrammed functions or does it support broad programmability to perform organization-specified functions? Does the system support broad interoperability functions?	(1-5)	
Scope of Control: To what degree can the system control operational equipment by directly actuating physical systems (e.g., pumps, circuit breakers) or controlling processed data or communications that directly causes another system to be controlled (e.g., SCADA server, DCS)?	(1-5)	

Maintainability Category

If a mitigation to a vulnerability detected in the system is developed, can it be used? Can an update be made in real-time, using a network connection? How difficult is obtaining the vendor update and deploying to the system? Must the system or facility be taken off-line? Is physical access to the system needed?

Questions	Notes
Do vendors provide patches or updates to this system?	
How soon can a patch or update be deployed in a typical installation?	
Can the system be easily removed from service without impact to the process it performs?	
Does a patched system require testing or customization before being reinstalled?	
Are instances of the system geographically remote?	



Appendix

Operational Impact (Electric Sector)

Level	Range of Values	Description
Very High Consequence	5	**Catastrophic**: Malicious operation of this system **alone** could cause a wide-area loss of electricity for **days or more**.
High Consequence	4	**Severe**: Malicious operation of this system **alone** could cause a wide-area loss of electricity for **hours, up to one day**.
Medium Consequence	3	**Noticeable**: Malicious operation of this system alone could cause **localized outages**.
Low Consequence	2	**Negligible**: Malicious operation of this system **in combination with others** could cause **localized** outages.
Very Low Consequence	1	**Insignificant**: Malicious operation of this system would not likely cause loss of power **under any circumstances**.

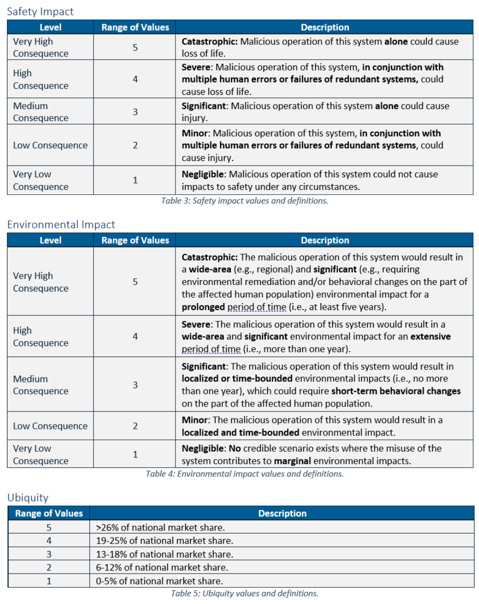
Table 1: Operational impact values and definitions for the electric sector.

Operational Impact (Oil and Gas Sectors)

Level	Range of Values	Description
Very High Consequence	5	**Catastrophic:** The misuse, malfunction or loss of this system would result in an immediate wise spread demand loss (e.g., metropolitan area, pipelines feeding multiple generators) or wide-area supply loss (e.g., multiple refineries or processing plants) **for an extended period (e.g., more >7 days)**.
High Consequence	4	**Severe**: The misuse, malfunction, or loss of this system would result in a loss of critical ONG capabilities of facilities (e.g., production, processing, transportation, storage) for a **long period (e.g., 2-7 days)**.
Medium Consequence	3	**Significant**: The misuse, malfunction, or loss of this system would result in a loss of critical ONG capabilities of facilities (e.g., production, processing, transportation, storage) for a **moderate period (e.g., 1-2 days)**.
Low Consequence	2	**Minor**: The misuse, malfunction, or loss of this system would result in a loss of critical ONG capabilities of facilities (e.g., production, processing, transportation, storage) for a **short period (e.g., hours)**.
Very Low Consequence	1	**Insignificant**: Little to no impacts to oil/gas refinement or delivery, the system is not needed for real-time operation of the oil/gas domain.

Table 2: Operational impact values and definitions for the oil and gas sectors.

Page 3 of the SME Prioritization Worksheet.



Safety Impact

Level	Range of Values	Description
Very High Consequence	5	**Catastrophic:** Malicious operation of this system **alone** could cause loss of life.
High Consequence	4	**Severe**: Malicious operation of this system, **in conjunction with multiple human errors or failures of redundant systems,** could cause loss of life.
Medium Consequence	3	**Significant**: Malicious operation of this system **alone** could cause injury.
Low Consequence	2	**Minor**: Malicious operation of this system, **in conjunction with multiple human errors or failures of redundant systems**, could cause injury.
Very Low Consequence	1	**Negligible:** Malicious operation of this system could not cause impacts to safety under any circumstances.

Table 3: Safety impact values and definitions.

Environmental Impact

Level	Range of Values	Description
Very High Consequence	5	**Catastrophic:** The malicious operation of this system would result in a **wide-area** (e.g., regional) and **significant** (e.g., requiring environmental remediation and/or behavioral changes on the part of the affected human population) environmental impact for a **prolonged** period of time (i.e., at least five years).
High Consequence	4	**Severe**: The malicious operation of this system would result in a **wide-area** and **significant** environmental impact for an **extensive** period of time (i.e., more than one year).
Medium Consequence	3	**Significant**: The malicious operation of this system would result in **localized or time-bounded** environmental impacts (i.e., no more than one year), which could require **short-term behavioral changes** on the part of the affected human population.
Low Consequence	2	**Minor**: The malicious operation of this system would result in a **localized and time-bounded** environmental impact.
Very Low Consequence	1	**Negligible**: **No** credible scenario exists where the misuse of the system contributes to **marginal** environmental impacts.

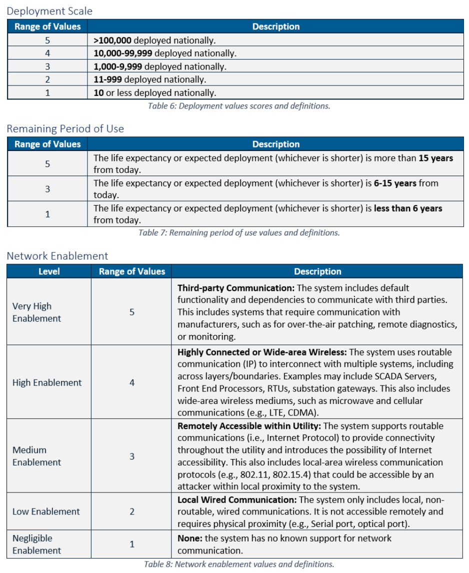
Table 4: Environmental impact values and definitions.

Ubiquity

Range of Values	Description
5	>26% of national market share.
4	19-25% of national market share.
3	13-18% of national market share.
2	6-12% of national market share.
1	0-5% of national market share.

Table 5: Ubiquity values and definitions.

Page 4 of the SME Prioritization Worksheet.



Deployment Scale

Range of Values	Description
5	**>100,000** deployed nationally.
4	**10,000-99,999** deployed nationally.
3	**1,000-9,999** deployed nationally.
2	**11-999** deployed nationally.
1	**10** or less deployed nationally.

Table 6: Deployment values scores and definitions.

Remaining Period of Use

Range of Values	Description
5	The life expectancy or expected deployment (whichever is shorter) is more than **15 years** from today.
3	The life expectancy or expected deployment (whichever is shorter) is **6-15 years** from today.
1	The life expectancy or expected deployment (whichever is shorter) is **less than 6 years** from today.

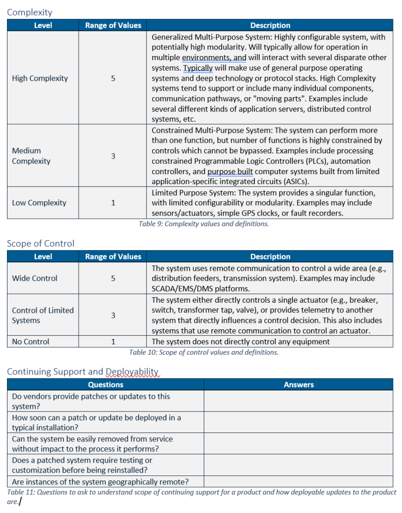
Table 7: Remaining period of use values and definitions.

Network Enablement

Level	Range of Values	Description
Very High Enablement	5	**Third-party Communication:** The system includes default functionality and dependencies to communicate with third parties. This includes systems that require communication with manufacturers, such as for over-the-air patching, remote diagnostics, or monitoring.
High Enablement	4	**Highly Connected or Wide-area Wireless:** The system uses routable communication (IP) to interconnect with multiple systems, including across layers/boundaries. Examples may include SCADA Servers, Front End Processors, RTUs, substation gateways. This also includes wide-area wireless mediums, such as microwave and cellular communications (e.g., LTE, CDMA).
Medium Enablement	3	**Remotely Accessible within Utility:** The system supports routable communications (i.e., Internet Protocol) to provide connectivity throughout the utility and introduces the possibility of Internet accessibility. This also includes local-area wireless communication protocols (e.g., 802.11, 802.15.4) that could be accessible by an attacker within local proximity to the system.
Low Enablement	2	**Local Wired Communication:** The system only includes local, non-routable, wired communications. It is not accessible remotely and requires physical proximity (e.g., Serial port, optical port).
Negligible Enablement	1	**None:** the system has no known support for network communication.

Table 8: Network enablement values and definitions.

Page 5 of the SME Prioritization Worksheet.



Complexity

Level	Range of Values	Description
High Complexity	5	Generalized Multi-Purpose System: Highly configurable system, with potentially high modularity. Will typically allow for operation in multiple environments, and will interact with several disparate other systems. Typically will make use of general purpose operating systems and deep technology or protocol stacks. High Complexity systems tend to support or include many individual components, communication pathways, or "moving parts". Examples include several different kinds of application servers, distributed control systems, etc.
Medium Complexity	3	Constrained Multi-Purpose System: The system can perform more than one function, but number of functions is highly constrained by controls which cannot be bypassed. Examples include processing constrained Programmable Logic Controllers (PLCs), automation controllers, and purpose built computer systems built from limited application-specific integrated circuits (ASICs).
Low Complexity	1	Limited Purpose System: The system provides a singular function, with limited configurability or modularity. Examples may include sensors/actuators, simple GPS clocks, or fault recorders.

Table 9: Complexity values and definitions.

Scope of Control

Level	Range of Values	Description
Wide Control	5	The system uses remote communication to control a wide area (e.g., distribution feeders, transmission system). Examples may include SCADA/EMS/DMS platforms.
Control of Limited Systems	3	The system either directly controls a single actuator (e.g., breaker, switch, transformer tap, valve), or provides telemetry to another system that directly influences a control decision. This also includes systems that use remote communication to control an actuator.
No Control	1	The system does not directly control any equipment

Table 10: Scope of control values and definitions.

Continuing Support and Deployability

Questions	Answers
Do vendors provide patches or updates to this system?	
How soon can a patch or update be deployed in a typical installation?	
Can the system be easily removed from service without impact to the process it performs?	
Does a patched system require testing or customization before being reinstalled?	
Are instances of the system geographically remote?	

Table 11: Questions to ask to understand scope of continuing support for a product and how deployable updates to the product are.

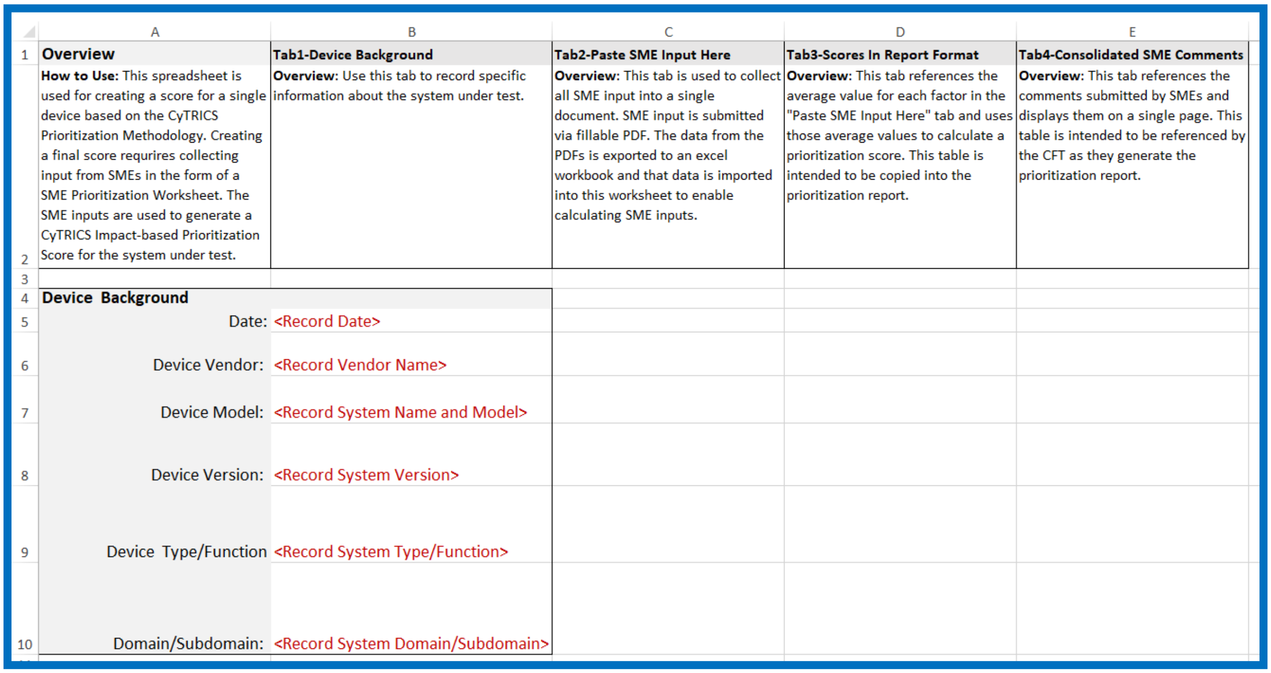
Page 6 of the SME Prioritization Worksheet.

Page 7 of the SME Prioritization Worksheet.

CFT Scoring Instrument

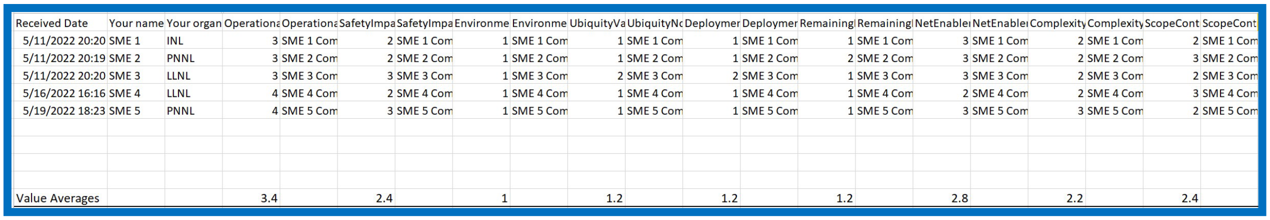
The CFT Scoring Instrument's primary function is to calculate the prioritization score for a system. It has four tabs to assist in gathering, storing, and recalling information as prioritization teams generate a prioritization report.

1. **Tab 1** contains instructions for using the Microsoft Excel workbook and data about the system being scored. The data captured is the date, vendor name, system name and model, system version, system type and function, and system domain and subdomain.
2. **Tab 2** is where SME input from the SME Prioritization Worksheet is imported.
3. **Tab 3** is where the score will be calculated and displayed.
4. **Tab 4** is intended to help the prioritization team as they write the prioritization report. It consolidates the SMEs comments from the individual SME Prioritization Worksheets and groups related comments together.



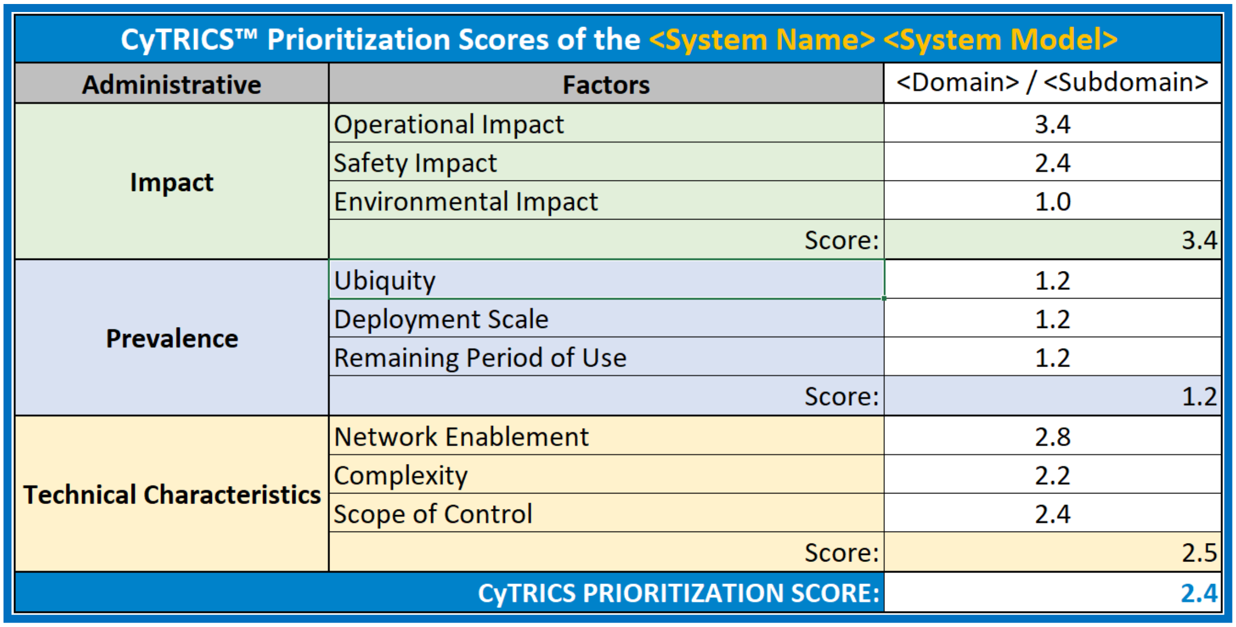
	A	B	C	D	E
1	**Overview**	**Tab1-Device Background**	**Tab2-Paste SME Input Here**	**Tab3-Scores In Report Format**	**Tab4-Consolidated SME Comments**
2	**How to Use:** This spreadsheet is used for creating a score for a single device based on the CyTRICS Prioritization Methodology. Creating a final score requrires collecting input from SMEs in the form of a SME Prioritization Worksheet. The SME inputs are used to generate a CyTRICS Impact-based Prioritization Score for the system under test.	**Overview:** Use this tab to record specific information about the system under test.	**Overview:** This tab is used to collect all SME input into a single document. SME input is submitted via fillable PDF. The data from the PDFs is exported to an excel workbook and that data is imported into this worksheet to enable calculating SME inputs.	**Overview:** This tab references the average value for each factor in the "Paste SME Input Here" tab and uses those average values to calculate a prioritization score. This table is intended to be copied into the prioritization report.	**Overview:** This tab references the comments submitted by SMEs and displays them on a single page. This table is intended to be referenced by the CFT as they generate the prioritization report.
3					
4	**Device Background**				
5	Date:	<Record Date>			
6	Device Vendor:	<Record Vendor Name>			
7	Device Model:	<Record System Name and Model>			
8	Device Version:	<Record System Version>			
9	Device Type/Function	<Record System Type/Function>			
10	Domain/Subdomain:	<Record System Domain/Subdomain>			

Figure 912: Tab 1 of the CFT Scoring Instrument.



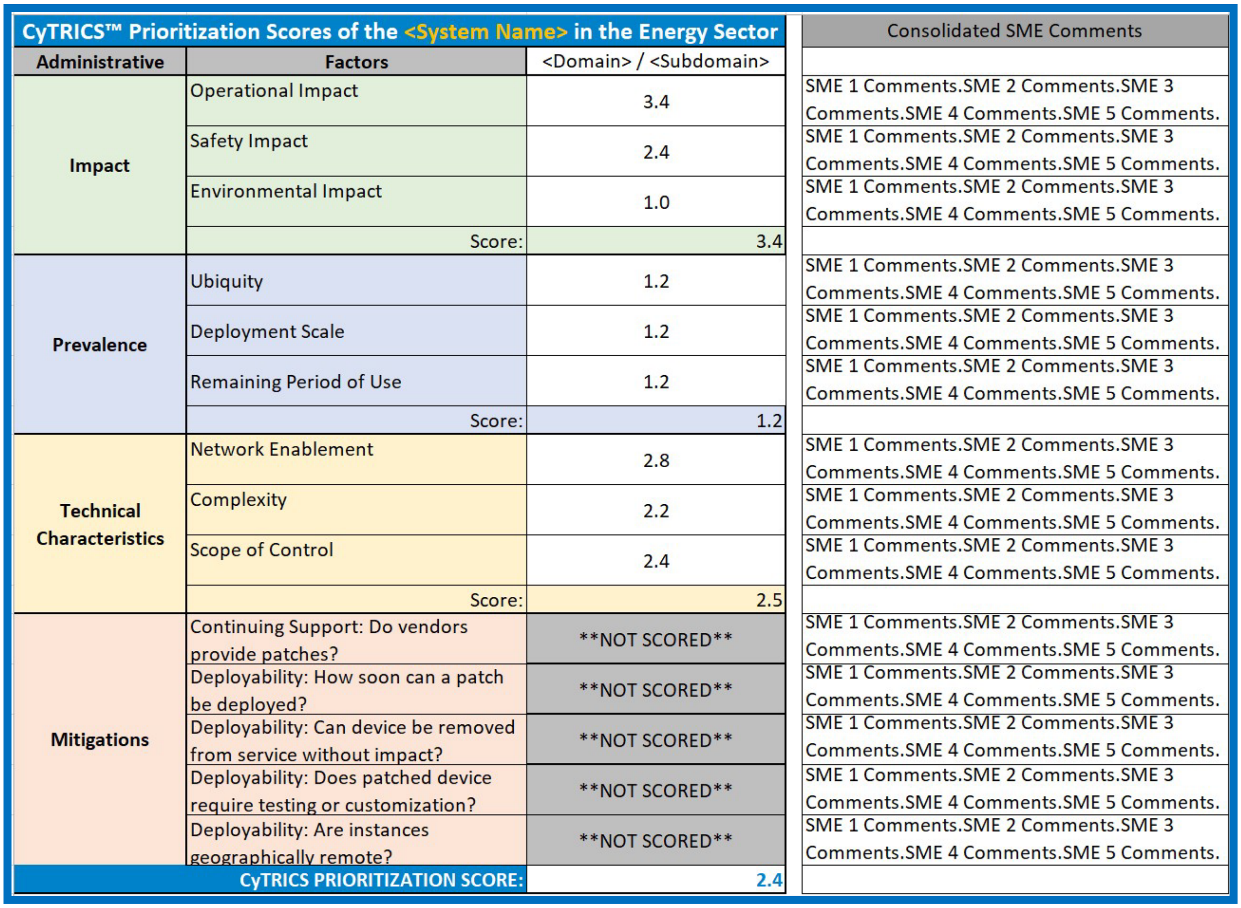
Received Date	Your name	Your organ	Operationa	Operationa	SafetyImpa	SafetyImpa	Environme	Environme	UbiquityVa	UbiquityN	Deploymen	Deploymen	Remaining	Remaining	NetEnable	NetEnable	Complexity	Complexity	ScopeCont	ScopeCont
5/11/2022 20:20	SME 1	INL	3	SME 1 Com	2	SME 1 Com	1	SME 1 Com	1	SME 1 Com	1	SME 1 Com	1	SME 1 Com	3	SME 1 Com	2	SME 1 Com	2	SME 1 Com
5/11/2022 20:19	SME 2	PNNL	3	SME 2 Com	2	SME 2 Com	1	SME 2 Com	1	SME 2 Com	1	SME 2 Com	2	SME 2 Com	3	SME 2 Com	2	SME 2 Com	3	SME 2 Com
5/11/2022 20:20	SME 3	LLNL	3	SME 3 Com	3	SME 3 Com	1	SME 3 Com	2	SME 3 Com	2	SME 3 Com	1	SME 3 Com	3	SME 3 Com	2	SME 3 Com	2	SME 3 Com
5/16/2022 16:16	SME 4	LLNL	4	SME 4 Com	2	SME 4 Com	1	SME 4 Com	1	SME 4 Com	1	SME 4 Com	1	SME 4 Com	2	SME 4 Com	2	SME 4 Com	3	SME 4 Com
5/19/2022 18:23	SME 5	PNNL	4	SME 5 Com	3	SME 5 Com	1	SME 5 Com	1	SME 5 Com	1	SME 5 Com	1	SME 5 Com	3	SME 5 Com	3	SME 5 Com	2	SME 5 Com
Value Averages			3.4		2.4		1		1.2		1.2		1.2		2.8		2.2		2.4	

Figure 1013: Tab 2 of the CFT Scoring Instrument.



CyTRICS™ Prioritization Scores of the <System Name> <System Model>		
Administrative	Factors	<Domain> / <Subdomain>
Impact	Operational Impact	3.4
	Safety Impact	2.4
	Environmental Impact	1.0
	Score:	3.4
Prevalence	Ubiquity	1.2
	Deployment Scale	1.2
	Remaining Period of Use	1.2
	Score:	1.2
Technical Characteristics	Network Enablement	2.8
	Complexity	2.2
	Scope of Control	2.4
	Score:	2.5
	CyTRICS PRIORITIZATION SCORE:	2.4

Figure 1114: Tab 3 of the CFT Scoring Instrument with sample values provided to show a prioritization score.



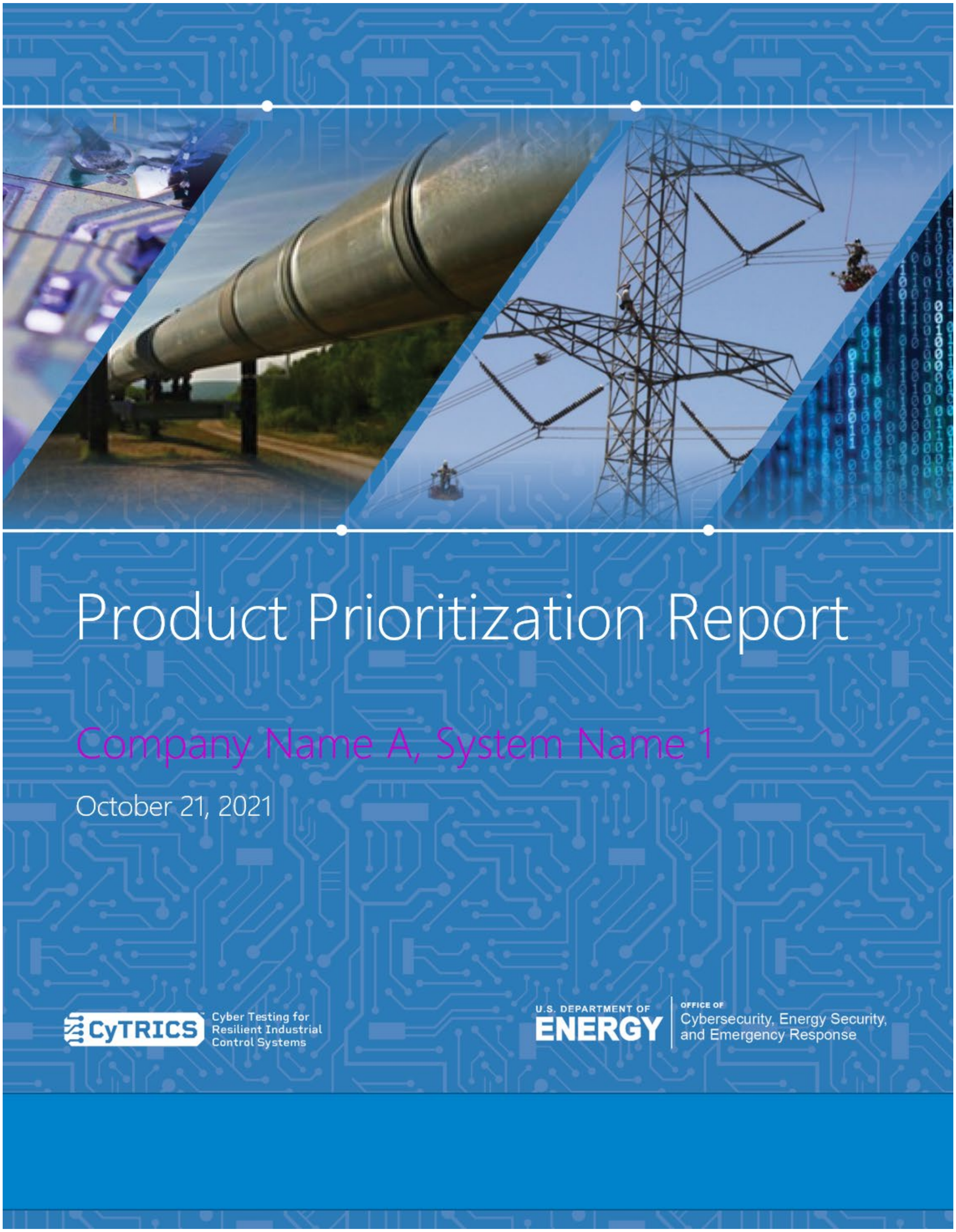
CyTRICS™ Prioritization Scores of the <System Name> in the Energy Sector			Consolidated SME Comments
Administrative	Factors	<Domain> / <Subdomain>	
Impact	Operational Impact	3.4	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Safety Impact	2.4	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Environmental Impact	1.0	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Score:	3.4	
Prevalence	Ubiquity	1.2	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Deployment Scale	1.2	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Remaining Period of Use	1.2	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Score:	1.2	
Technical Characteristics	Network Enablement	2.8	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Complexity	2.2	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Scope of Control	2.4	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Score:	2.5	
Mitigations	Continuing Support: Do vendors provide patches?	**NOT SCORED**	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Deployability: How soon can a patch be deployed?	**NOT SCORED**	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Deployability: Can device be removed from service without impact?	**NOT SCORED**	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Deployability: Does patched device require testing or customization?	**NOT SCORED**	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	Deployability: Are instances geographically remote?	**NOT SCORED**	SME 1 Comments.SME 2 Comments.SME 3 Comments.SME 4 Comments.SME 5 Comments.
	CyTRICS PRIORITIZATION SCORE:	2.4	

Figure 1215: Tab 4 of the CFT Scoring Instrument.

7. Appendix C: Prioritization Report Template

Report Template

[START OF TEMPLATE]



Product Prioritization Report

Company Name A, System Name 1

October 21, 2021

CyTRICS™ Cyber Testing for Resilient Industrial Control Systems

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Company Name A, System Name 1

Executive Summary

The System Name 1 prioritization score was 2.7 out of a maximum score of 5.0.

The Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program is the Department of Energy's (DOE) program for cybersecurity vulnerability testing and subcomponent enumeration. To support program goals, CyTRICS developed a methodology to score the potential risks associated with various deployed systems.[c] The scores generated through this process for systems will help determine which systems CyTRICS will prioritize for testing. This Product Prioritization Report focuses on results for the Company Name A System Name 1 (SN1) system, a software capability for integrating and analyzing data generated by power distribution systems.[7] This system received a prioritization score of 2.7 out of a maximum 5.0, where a 1.0 indicates minimal potential impact to U.S. energy delivery in the case of system malfunction and a 5.0 indicates severe impact.

On the CyTRICS prioritization scale, a system scored as 2.7 is associated with moderate anticipated losses following the exploitation of a system vulnerability. This score is a combination of four category scores, each rated on a 1.0 - 5.0 scale. These scores are shown in Table 1 below and explained further in the following report. Based on the available considerations, potential misuse, malfunction, or loss of the system would result in moderate losses to electricity delivery in the U.S. The most likely impact vector for the misuse of this system is data manipulation resulting in inappropriate and potentially damaging operator action.

Category	Category-Specific Score (Max = 5.0)
Impact	2.3
Prevalence	2.8
Technical Characteristics	3.0
Mitigations	4.6
CyTRICS Prioritization Score	**2.7**

Table 1: CyTRICS prioritization score for the SN1.

[c] CyTRICS uses the term "system" in a generic sense to encompass hardware, software, and/or firmware.

CyTRICS Process Overview

The Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program is the Department of Energy's (DOE) program for cybersecurity vulnerability testing and subcomponent enumeration. Created in 2018, CyTRICS enhances the cyber resilience of highly critical equipment in the energy sector by partnering with stakeholders to identify high priority operational technology (OT) components, perform expert testing, share information about vulnerabilities in the supply chain, and inform improvements in component design and manufacturing. The program leverages best-in-class test facilities and analytic capabilities across multiple DOE National Laboratories, as well as strategic partnerships with technology developers, manufacturers, asset owners and operators, and interagency partners. CyTRICS is led by the DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

CyTRICS was born out of the growing concern that adversaries could exploit weaknesses in digital supply chains, possibly triggering catastrophic effects on energy infrastructure and beyond. To address these concerns, the program identifies common mode vulnerabilities in high-impact hardware, software, and firmware and responsibly discloses them to manufacturers who can develop patches or mitigations before adversaries can exploit them. The CyTRICS program employs several innovative processes: a quantitative methodology for prioritizing OT components; a standardized testing process; a central data repository for cross-component analysis and reporting; and formal partnership agreements with manufacturers and asset owners to foster mutual cooperation.

The mission of CyTRICS is to support DOE's strategy to anticipate, confront, and thwart multiple, ever-changing threats: "In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced."[8]

Because this testing is a time- and resource-intensive process, it is important to prioritize systems with the most potential impact on the energy sector if vulnerable to adversary cyber sabotage. Thus, the purpose of the prioritization process is to identify and prioritize the most impactful systems for CyTRICS testing.

In pursuit of this goal, this CyTRICS prioritization effort included subject matter experts (SMEs) from Idaho National Laboratory (INL), Lawrence Livermore National Laboratory (LLNL), and Pacific Northwest National Laboratory (PNNL). The MITRE Corporation supported the development of the CyTRICS prioritization methodology and Newton-Evans, a market research firm, provided insights into market data illustrating the scope and reach of potential system impacts to individual sections of the energy sector.

The following report summarizes the efforts of the teams listed above. It presents a brief overview of what the SN1 is and does, the assumptions made regarding the SN1's operational context, the results of the SN1 prioritization, and the rationale for each result.

System Name 1 Overview

Company Name A's SN1 processes, stores, analyzes, and displays power distribution data. It operates as a client-server, on-premise software application that collects data from devices connected to the system and stores it using a Microsoft SQL Server owned and operated by the client. Once installed, the SN1 can connect to a wide variety of smart devices across the networked system, such as power and energy meters, protective relays and circuit breakers, RTUs and PLCs, VSDs, UPS, and PQ mitigation equipment. It can integrate with process control systems and Web interfaces for real-time power and equipment monitoring, and it can track data overtime to provide reliable network operation, equipment performance, and reduced network outages. The SN1 is intended to provide both alarm management across the system and analytics for calculating, modeling, forecasting, and tracking key energy indicators and system events[9].

The SN1's primary goal is data ingestion and analytics. To do so, it maintains a connection to many smart devices through a facility's internal communication network. The SN1 itself is not designed for a direct internet connection; its communication abilities are designed for a secured network infrastructure. It is possible for the SN1 to perform some manual control actions through this connected infrastructure, including resetting values on devices, changing device configuration settings, and upgrading device firmware from a file located on the networked system[10].

In terms of its use, the SN1 is primarily designed for energy end-users, not providers, and primarily analyzes power distribution and use. It is estimated to be deployed at 300 to 500 sites, including co-generation sites, and it is most widely used in the data center power management market segment[11].

7.1. Operational Context Assumptions

The CyTRICS prioritization team's primary assumptions regarding the SN1 were related to what it can and cannot control. The webpage for the SN1 has a long list of functions related to data ingestion, analytics, and visualizations; however, it does mention a capacity to "operate breakers remotely to minimize exposure to arc-flash risk." [12] The extent of the SN1's ability to operate breakers, particularly in the context of safety controls, is not detailed within the User Guide or the installation documentation. The documentation states that users can change the settings associated with the *data output* of the objects within the SN1's communication network and makes no mention of the objects' operation. Erring on the side of caution, the scoring team evaluated the SN1 under the assumption that it can send configuration-change commands to the connected devices but not override any associated safety devices.

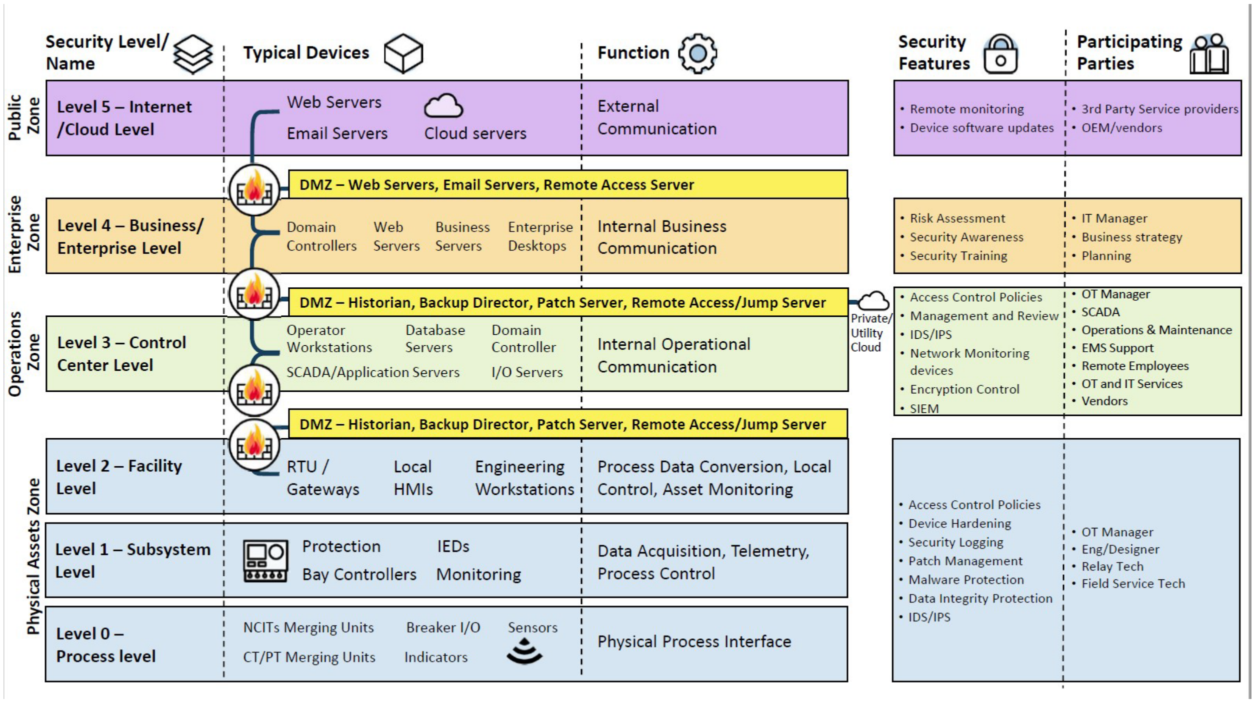


Figure 1: Example representative architecture displaying where the SN1 would sit in a facility's operational network. Source: SN1 Installation Guide.

SN1 Prioritization Scores

The CyTRICS prioritization score is the result of a internally-developed, weighted formula that considers the significance of each of the factors in determining overall energy sector impact, as established in the CyTRICS Scoring Methodology report.[13]

7.2. Overall Prioritization Score: 2.7

Researchers determined a prioritization score of 2.7 for the SN1 used in electric systems due to middling scores in the Impact, Prevalence, and Technical Characteristics factors. The final prioritization score was mainlyt influenced by how the system is primarily for operator and facility data analytics with minimal influence over safety systems; a single device is sufficient for a whole facility, which results in low deployment numbers; and it is only moderately complex in terms of its operational capacity and network connectivity. The factors and associated categories assessed in determining this score are depicted in Figure 2 below.

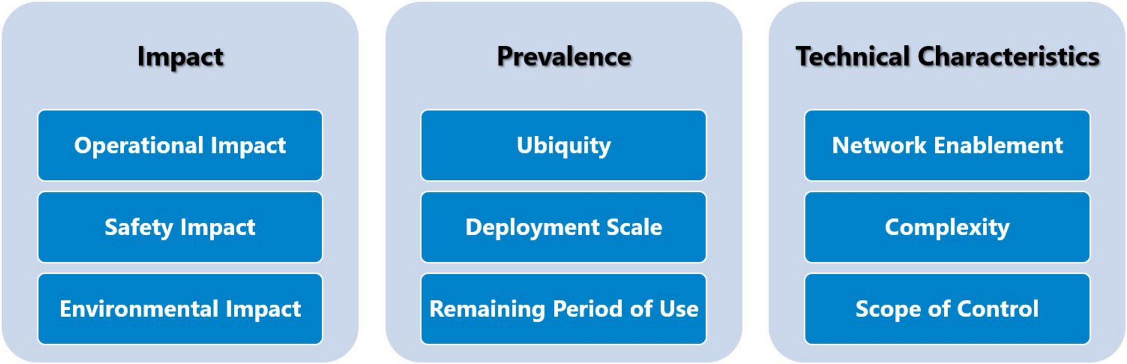


Figure 2: Categories and factors evaluated to determine a CyTRICS prioritization score.

7.3. Factor-Specific Scores

Table 2 presents the scored factor-specific, category-specific, and resulting overall prioritization scores for the SN1. The rationale for each factor-specific score is presented in Table 2.

CyTRICS™ Prioritization Score of the SN1 System in the Energy Sector		
Category	**Factor**	**Electric / End-User Power Monitoring**
Impact	Operational Impact	2.3
	Safety Impact	1.5
	Environmental Impact	1.0
	Score:	2.3
Prevalence	Ubiquity	3.0
	Deployment Scale	1.0
	Operational Lifespan	3.0
	Remaining Period of Use	1.0
	Score:	2.8
Technical Characteristics	Network Enablement	3.0
	Complexity	3.0
	Scope of Control	3.0
	Score:	3.0
Mitigations	Continuing Support	1
	Deployability	4.6
	Score:	4.6
	CyTRICS PRIORITIZATION SCORE:	**2.7**

Table 2: Table of category- and factor-specific scores and the CyTRICS prioritization score for the SN1.

Factor-Specific Score Rationale

This section captures the key points underpinning the CyTRICS factor-specific scores for the SN1.

7.4. Impact

Operational Impact: CyTRICS SMEs determined that a manipulation of the SN1 could create noticeable but localized outages in electricity delivery. Although it can apparently operate breakers remotely, SMEs assumed that the associated safety systems would still be in place, unaffected, and would react in time to prevent lasting or serious damage. The SMEs seemed to generally agree that more information regarding the SN1's operational capabilities would be necessary to indicate Operational Impact conclusively; however, there was general agreement that malicious operations could not directly cause a high impact to the energy system. Operational Impact could result from an operator reading falsified information and making an incorrect operational decision, but this would necessitate multiple errors on the operator's part (including not checking for alarms or errors at the device level). This discussion resulted in an average score of 2.3 across the SMEs, indicating moderate to low impact.

Safety Impact: With respect to the possible impact on human health, the SMEs primarily discussed the number of redundancies related to the operations of the SN1. The prevalent opinion was that a large amount of human error would be necessary in the operation of the SN1 (i.e., not verifying alarms and not verifying erroneous data) to result in harm to personnel. Proper installation of the system would ensure that it could not touch safety systems in place. Because of this, the Safety score was determined to be 1.5, indicating a low impact.

Environmental Impact: The SMEs were not able to identify a specific manipulation pathway through which the SN1 could cause harm to the environment. The potential for the device to create local fires through arcing was considered as an extremely remote possibility, but the prevailing opinion was that even gross mis-operation would not cause significant Environmental Impact without another attack vector. This resulted in a score of 1, indicating very low impact.

7.5. Prevalence

Ubiquity: The market research firm Newton-Evans estimates that the SN1 market share is approximately 20%.[14] The CyTRICS prioritization team assesses Ubiquity as moderate, resulting in a score of 3.

Deployment Scale: Newton-Evans further estimates 300 to 500 sites, including co-generation sites currently use the SN1 in the United States.[15] The CyTRICS prioritization team assesses this Deployment Scale as small, resulting in a score of 1.

Operational Lifespan: Based on information from sources familiar with the product, Newton-Evans determined that the Operational Lifespan is 6-8 years or more as long as upgrades from the supplier are provided and licenses are renewed.[16] The CyTRICS prioritization team assesses this Operational Lifespan scale as moderately long, resulting in a score of 3.

Remaining Period of Use: The Newton-Evans information sources anticipated that newer releases of the SN1 would likely be coming in five to ten years.[17] As new type of power monitoring software from SE is expected within five years, the CyTRICS prioritization team assesses the Remaining Period of Use as short, resulting in a score of 1.

7.6. Technical Characteristics

Network Enablement: The CyTRICS team identified that the SN1 should have a Network Enablement score of 3, which indicates that the device is remotely accessible within the utility. The IT Installation Guide directly asserts that the system supports communication through either an Ethernet (TCP) or serial device network and that it is not intended for internet connections and instead operates through local-area wireless interfaces. These communication protocols could be accessible by an attacker with local proximity to the device. [18]

Complexity: The CyTRICS team identified through the IT Installation Guide, User Guide, and product brochure that the SN1 should have a Complexity score of 3. It requires secure program deployment and an execution environment, accounts, and remote authentication/configuration, and it supports a range of functionality, including ingesting, analyzing, and visualizing data from across a network. It does not, however, do so through broad sets of networking libraries and security features, nor does it provide standard execution environments. [19]

Scope of Control: The CyTRICS team used the User Guide and product brochure to determine that the SN1 should have a Scope of Control score of 3. This is because it does not appear to have broad range of control over many devices and components, but, according to the product brochure, it can control a small number. It also directly provides processed data or communications that directly affect the control of another device, albeit through an operator. [20,21]

7.7. Mitigations

Continuing Support: The vendor currently provides patches and updates. The most recent patch as of the writing of this report was made available on 28 September 2021. Because of this, the CyTRICS team determined that Continuing Support is available and has a score of 1.

Deployability: CyTRICS SMEs discussed the relative ease of updating what is essentially software, especially when it is primarily performing analytics and visualization and is not necessary for ongoing operations. There was some discussion regarding the general difficulty of updating tools within the OT environment as a whole, but the prevalent opinion was that the SN1 would be easy to update in real-time because physical access to the device would not be necessary; the update can be obtained via the vendor's website and placed onto the facility's LAN, and the facility would not need to be taken off-line. Due to the relative ease of deploying an update, the team determined that the Deployability score for the SN1 is a 4.6.

Conclusion

On the CyTRICS prioritization scale, a system scored as 2.7 is associated with moderate anticipated losses following the exploitation of a system vulnerability. This score is a combination of four category scores, each rated on a 1.0–5.0 scale. These scores are shown in Table 3 below and explained further in the above report. Based on the available considerations, potential misuse, malfunction, or loss of the system would result in minimal losses to electricity delivery. The most likely impact vector for the misuse of this system is data manipulation resulting in inappropriate and potentially damaging operator action.

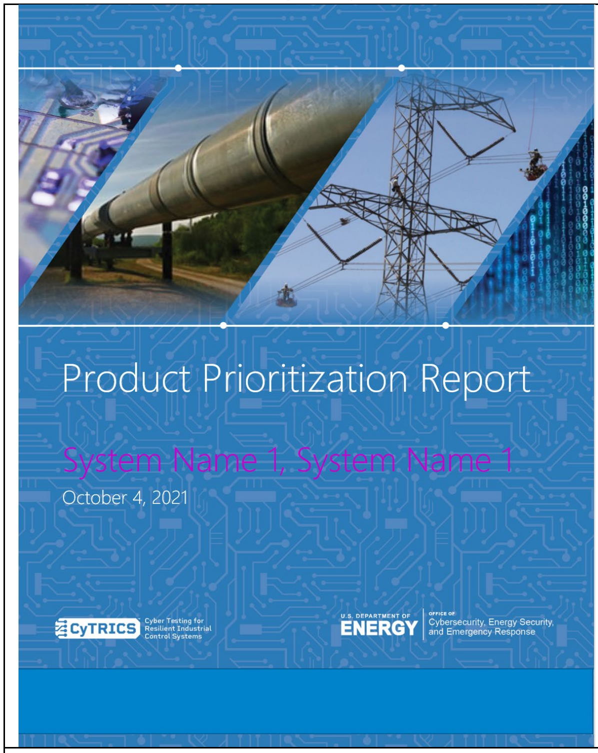
Category	Category-Specific Score (Max = 5.0)
Impact	2.3
Prevalence	2.8
Technical Characteristics	3.0
Mitigations	4.6
CyTRICS Prioritization Score	**2.7**

Table 3: CyTRICS prioritization scores for the SN1.

References

[END OF TEMPLATE]

Example Report: Single System Evaluated in Multiple Subdomains

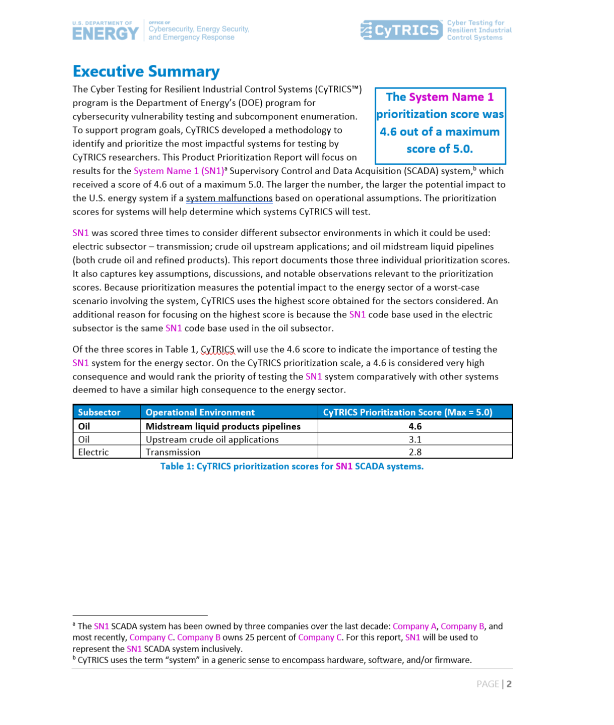


Product Prioritization Report

System Name 1, System Name 1

October 4, 2021

Page 1 of a sample Prioritization Report.



Executive Summary

The System Name 1 prioritization score was 4.6 out of a maximum score of 5.0.

The Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program is the Department of Energy's (DOE) program for cybersecurity vulnerability testing and subcomponent enumeration. To support program goals, CyTRICS developed a methodology to identify and prioritize the most impactful systems for testing by CyTRICS researchers. This Product Prioritization Report will focus on results for the System Name 1 (SN1)[a] Supervisory Control and Data Acquisition (SCADA) system,[b] which received a score of 4.6 out of a maximum 5.0. The larger the number, the larger the potential impact to the U.S. energy system if a system malfunctions based on operational assumptions. The prioritization scores for systems will help determine which systems CyTRICS will test.

SN1 was scored three times to consider different subsector environments in which it could be used: electric subsector – transmission; crude oil upstream applications; and oil midstream liquid pipelines (both crude oil and refined products). This report documents those three individual prioritization scores. It also captures key assumptions, discussions, and notable observations relevant to the prioritization scores. Because prioritization measures the potential impact to the energy sector of a worst-case scenario involving the system, CyTRICS uses the highest score obtained for the sectors considered. An additional reason for focusing on the highest score is because the SN1 code base used in the electric subsector is the same SN1 code base used in the oil subsector.

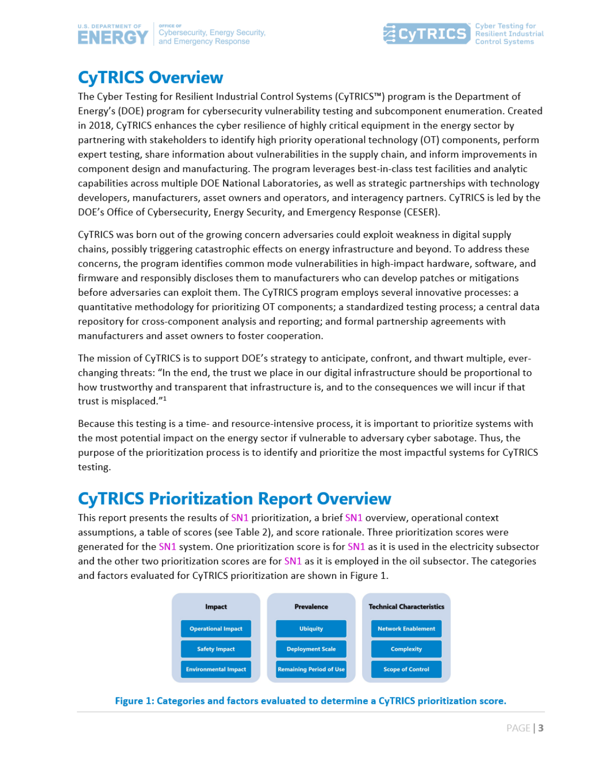
Of the three scores in Table 1, CyTRICS will use the 4.6 score to indicate the importance of testing the SN1 system for the energy sector. On the CyTRICS prioritization scale, a 4.6 is considered very high consequence and would rank the priority of testing the SN1 system comparatively with other systems deemed to have a similar high consequence to the energy sector.

Subsector	Operational Environment	CyTRICS Prioritization Score (Max = 5.0)
Oil	**Midstream liquid products pipelines**	**4.6**
Oil	Upstream crude oil applications	3.1
Electric	Transmission	2.8

Table 1: CyTRICS prioritization scores for SN1 SCADA systems.

[a] The SN1 SCADA system has been owned by three companies over the last decade: Company A, Company B, and most recently, Company C. Company B owns 25 percent of Company C. For this report, SN1 will be used to represent the SN1 SCADA system inclusively.
[b] CyTRICS uses the term "system" in a generic sense to encompass hardware, software, and/or firmware.

Page 2 of a sample Prioritization Report.



CyTRICS Overview

The Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program is the Department of Energy's (DOE) program for cybersecurity vulnerability testing and subcomponent enumeration. Created in 2018, CyTRICS enhances the cyber resilience of highly critical equipment in the energy sector by partnering with stakeholders to identify high priority operational technology (OT) components, perform expert testing, share information about vulnerabilities in the supply chain, and inform improvements in component design and manufacturing. The program leverages best-in-class test facilities and analytic capabilities across multiple DOE National Laboratories, as well as strategic partnerships with technology developers, manufacturers, asset owners and operators, and interagency partners. CyTRICS is led by the DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER).

CyTRICS was born out of the growing concern adversaries could exploit weakness in digital supply chains, possibly triggering catastrophic effects on energy infrastructure and beyond. To address these concerns, the program identifies common mode vulnerabilities in high-impact hardware, software, and firmware and responsibly discloses them to manufacturers who can develop patches or mitigations before adversaries can exploit them. The CyTRICS program employs several innovative processes: a quantitative methodology for prioritizing OT components; a standardized testing process; a central data repository for cross-component analysis and reporting; and formal partnership agreements with manufacturers and asset owners to foster cooperation.

The mission of CyTRICS is to support DOE's strategy to anticipate, confront, and thwart multiple, ever-changing threats: "In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced."[1]

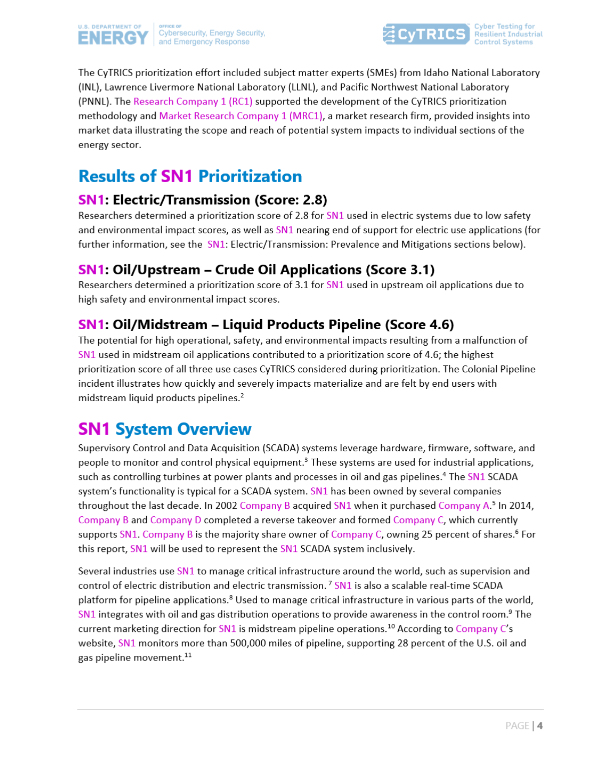
Because this testing is a time- and resource-intensive process, it is important to prioritize systems with the most potential impact on the energy sector if vulnerable to adversary cyber sabotage. Thus, the purpose of the prioritization process is to identify and prioritize the most impactful systems for CyTRICS testing.

CyTRICS Prioritization Report Overview

This report presents the results of SN1 prioritization, a brief SN1 overview, operational context assumptions, a table of scores (see Table 2), and score rationale. Three prioritization scores were generated for the SN1 system. One prioritization score is for SN1 as it is used in the electricity subsector and the other two prioritization scores are for SN1 as it is employed in the oil subsector. The categories and factors evaluated for CyTRICS prioritization are shown in Figure 1.

Figure 1: Categories and factors evaluated to determine a CyTRICS prioritization score.

Page 3 of a sample Prioritization Report.



The CyTRICS prioritization effort included subject matter experts (SMEs) from Idaho National Laboratory (INL), Lawrence Livermore National Laboratory (LLNL), and Pacific Northwest National Laboratory (PNNL). The Research Company 1 (RC1) supported the development of the CyTRICS prioritization methodology and Market Research Company 1 (MRC1), a market research firm, provided insights into market data illustrating the scope and reach of potential system impacts to individual sections of the energy sector.

Results of SN1 Prioritization

SN1: Electric/Transmission (Score: 2.8)

Researchers determined a prioritization score of 2.8 for SN1 used in electric systems due to low safety and environmental impact scores, as well as SN1 nearing end of support for electric use applications (for further information, see the SN1: Electric/Transmission: Prevalence and Mitigations sections below).

SN1: Oil/Upstream – Crude Oil Applications (Score 3.1)

Researchers determined a prioritization score of 3.1 for SN1 used in upstream oil applications due to high safety and environmental impact scores.

SN1: Oil/Midstream – Liquid Products Pipeline (Score 4.6)

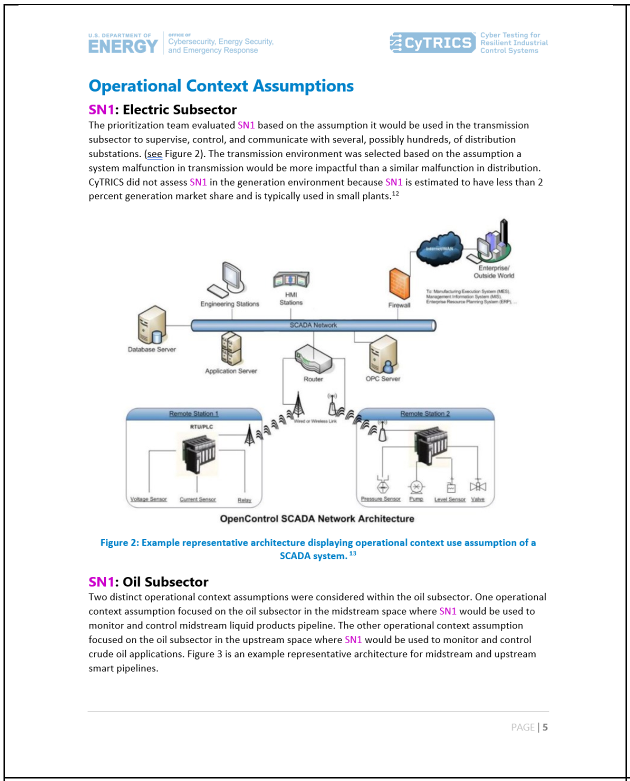
The potential for high operational, safety, and environmental impacts resulting from a malfunction of SN1 used in midstream oil applications contributed to a prioritization score of 4.6; the highest prioritization score of all three use cases CyTRICS considered during prioritization. The Colonial Pipeline incident illustrates how quickly and severely impacts materialize and are felt by end users with midstream liquid products pipelines.[2]

SN1 System Overview

Supervisory Control and Data Acquisition (SCADA) systems leverage hardware, firmware, software, and people to monitor and control physical equipment.[3] These systems are used for industrial applications, such as controlling turbines at power plants and processes in oil and gas pipelines.[4] The SN1 SCADA system's functionality is typical for a SCADA system. SN1 has been owned by several companies throughout the last decade. In 2002 Company B acquired SN1 when it purchased Company A.[5] In 2014, Company B and Company D completed a reverse takeover and formed Company C, which currently supports SN1. Company B is the majority share owner of Company C, owning 25 percent of shares.[6] For this report, SN1 will be used to represent the SN1 SCADA system inclusively.

Several industries use SN1 to manage critical infrastructure around the world, such as supervision and control of electric distribution and electric transmission. [7] SN1 is also a scalable real-time SCADA platform for pipeline applications.[8] Used to manage critical infrastructure in various parts of the world, SN1 integrates with oil and gas distribution operations to provide awareness in the control room.[9] The current marketing direction for SN1 is midstream pipeline operations.[10] According to Company C's website, SN1 monitors more than 500,000 miles of pipeline, supporting 28 percent of the U.S. oil and gas pipeline movement.[11]

Page 4 of a sample Prioritization Report.



Operational Context Assumptions

SN1: Electric Subsector

The prioritization team evaluated SN1 based on the assumption it would be used in the transmission subsector to supervise, control, and communicate with several, possibly hundreds, of distribution substations. (see Figure 2). The transmission environment was selected based on the assumption a system malfunction in transmission would be more impactful than a similar malfunction in distribution. CyTRICS did not assess SN1 in the generation environment because SN1 is estimated to have less than 2 percent generation market share and is typically used in small plants.[12]

Figure 2: Example representative architecture displaying operational context use assumption of a SCADA system. [13]

SN1: Oil Subsector

Two distinct operational context assumptions were considered within the oil subsector. One operational context assumption focused on the oil subsector in the midstream space where SN1 would be used to monitor and control midstream liquid products pipeline. The other operational context assumption focused on the oil subsector in the upstream space where SN1 would be used to monitor and control crude oil applications. Figure 3 is an example representative architecture for midstream and upstream smart pipelines.

PAGE | 5

Page 5 of a sample Prioritization Report.

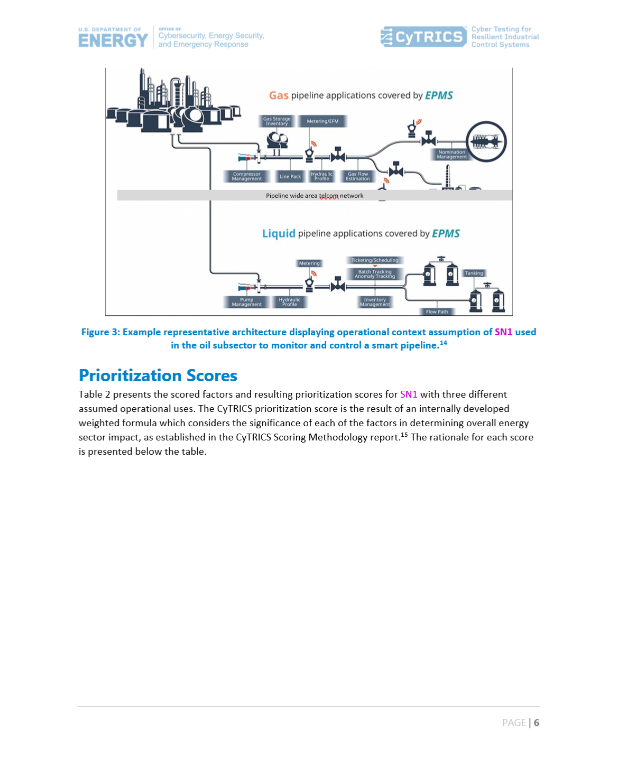


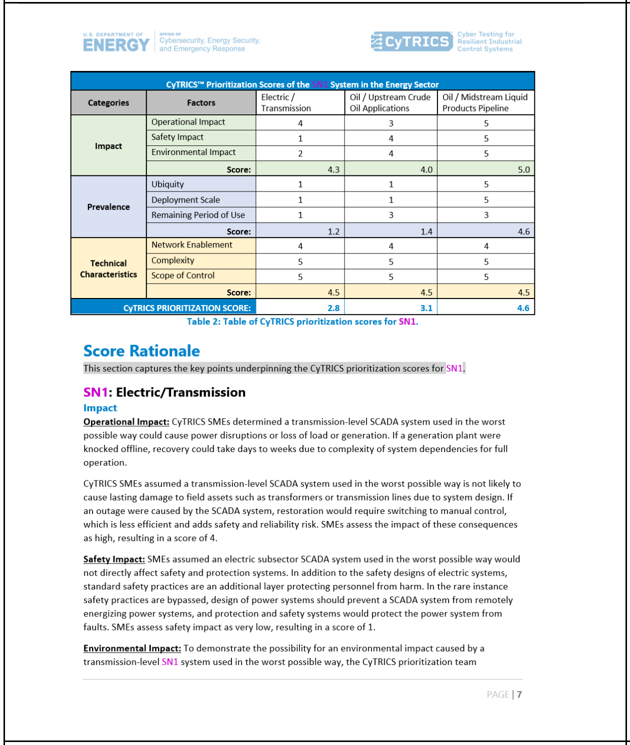
Figure 3: Example representative architecture displaying operational context assumption of SN1 used in the oil subsector to monitor and control a smart pipeline.[14]

Prioritization Scores

Table 2 presents the scored factors and resulting prioritization scores for SN1 with three different assumed operational uses. The CyTRICS prioritization score is the result of an internally developed weighted formula which considers the significance of each of the factors in determining overall energy sector impact, as established in the CyTRICS Scoring Methodology report.[15] The rationale for each score is presented below the table.

PAGE | 6

Page 6 of a sample Prioritization Report.



CyTRICS™ Prioritization Scores of the SN1 System in the Energy Sector				
Categories	Factors	Electric / Transmission	Oil / Upstream Crude Oil Applications	Oil / Midstream Liquid Products Pipeline
Impact	Operational Impact	4	3	5
	Safety Impact	1	4	5
	Environmental Impact	2	4	5
	Score:	4.3	4.0	5.0
Prevalence	Ubiquity	1	1	5
	Deployment Scale	1	1	5
	Remaining Period of Use	1	3	3
	Score:	1.2	1.4	4.6
Technical Characteristics	Network Enablement	4	4	4
	Complexity	5	5	5
	Scope of Control	5	5	5
	Score:	4.5	4.5	4.5
CyTRICS PRIORITIZATION SCORE:		2.8	3.1	4.6

Table 2: Table of CyTRICS prioritization scores for SN1.

Score Rationale

This section captures the key points underpinning the CyTRICS prioritization scores for SN1.

SN1: Electric/Transmission

Impact

Operational Impact: CyTRICS SMEs determined a transmission-level SCADA system used in the worst possible way could cause power disruptions or loss of load or generation. If a generation plant were knocked offline, recovery could take days to weeks due to complexity of system dependencies for full operation.

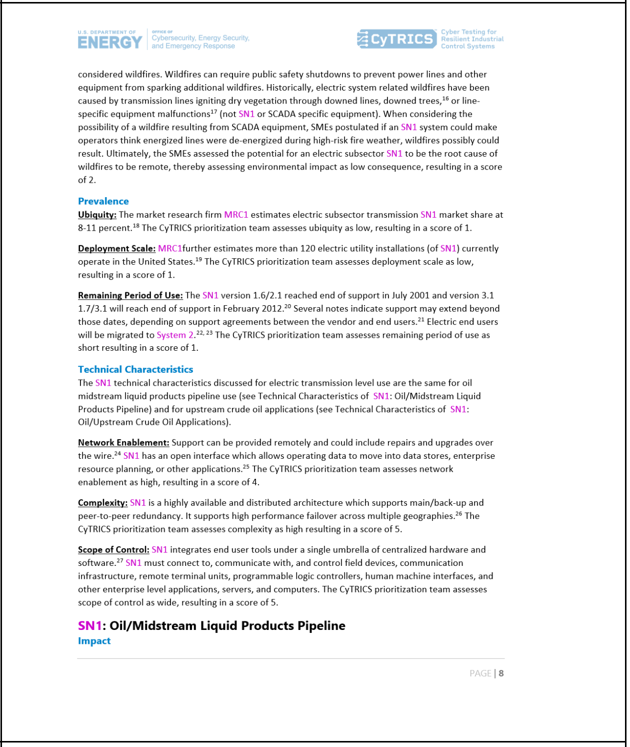
CyTRICS SMEs assumed a transmission-level SCADA system used in the worst possible way is not likely to cause lasting damage to field assets such as transformers or transmission lines due to system design. If an outage were caused by the SCADA system, restoration would require switching to manual control, which is less efficient and adds safety and reliability risk. SMEs assess the impact of these consequences as high, resulting in a score of 4.

Safety Impact: SMEs assumed an electric subsector SCADA system used in the worst possible way would not directly affect safety and protection systems. In addition to the safety designs of electric systems, standard safety practices are an additional layer protecting personnel from harm. In the rare instance safety practices are bypassed, design of power systems should prevent a SCADA system from remotely energizing power systems, and protection and safety systems would protect the power system from faults. SMEs assess safety impact as very low, resulting in a score of 1.

Environmental Impact: To demonstrate the possibility for an environmental impact caused by a transmission-level SN1 system used in the worst possible way, the CyTRICS prioritization team

PAGE | 7

Page 7 of a sample Prioritization Report.



considered wildfires. Wildfires can require public safety shutdowns to prevent power lines and other equipment from sparking additional wildfires. Historically, electric system related wildfires have been caused by transmission lines igniting dry vegetation through downed lines, downed trees,[16] or line-specific equipment malfunctions[17] (not SN1 or SCADA specific equipment). When considering the possibility of a wildfire resulting from SCADA equipment, SMEs postulated if an SN1 system could make operators think energized lines were de-energized during high-risk fire weather, wildfires possibly could result. Ultimately, the SMEs assessed the potential for an electric subsector SN1 to be the root cause of wildfires to be remote, thereby assessing environmental impact as low consequence, resulting in a score of 2.

Prevalence

Ubiquity: The market research firm MRC1 estimates electric subsector transmission SN1 market share at 8-11 percent.[18] The CyTRICS prioritization team assesses ubiquity as low, resulting in a score of 1.

Deployment Scale: MRC1further estimates more than 120 electric utility installations (of SN1) currently operate in the United States.[19] The CyTRICS prioritization team assesses deployment scale as low, resulting in a score of 1.

Remaining Period of Use: The SN1 version 1.6/2.1 reached end of support in July 2001 and version 3.1 1.7/3.1 will reach end of support in February 2012.[20] Several notes indicate support may extend beyond those dates, depending on support agreements between the vendor and end users.[21] Electric end users will be migrated to System 2.[22, 23] The CyTRICS prioritization team assesses remaining period of use as short resulting in a score of 1.

Technical Characteristics

The SN1 technical characteristics discussed for electric transmission level use are the same for oil midstream liquid products pipeline use (see Technical Characteristics of SN1: Oil/Midstream Liquid Products Pipeline) and for upstream crude oil applications (see Technical Characteristics of SN1: Oil/Upstream Crude Oil Applications).

Network Enablement: Support can be provided remotely and could include repairs and upgrades over the wire.[24] SN1 has an open interface which allows operating data to move into data stores, enterprise resource planning, or other applications.[25] The CyTRICS prioritization team assesses network enablement as high, resulting in a score of 4.

Complexity: SN1 is a highly available and distributed architecture which supports main/back-up and peer-to-peer redundancy. It supports high performance failover across multiple geographies.[26] The CyTRICS prioritization team assesses complexity as high resulting in a score of 5.

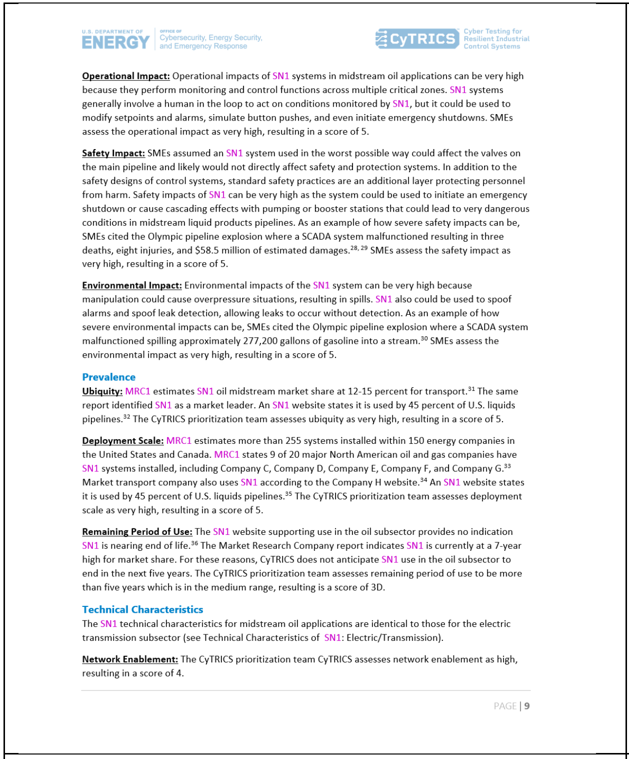
Scope of Control: SN1 integrates end user tools under a single umbrella of centralized hardware and software.[27] SN1 must connect to, communicate with, and control field devices, communication infrastructure, remote terminal units, programmable logic controllers, human machine interfaces, and other enterprise level applications, servers, and computers. The CyTRICS prioritization team assesses scope of control as wide, resulting in a score of 5.

SN1: Oil/Midstream Liquid Products Pipeline

Impact

PAGE | 8

Page 8 of a sample Prioritization Report.



Operational Impact: Operational impacts of SN1 systems in midstream oil applications can be very high because they perform monitoring and control functions across multiple critical zones. SN1 systems generally involve a human in the loop to act on conditions monitored by SN1, but it could be used to modify setpoints and alarms, simulate button pushes, and even initiate emergency shutdowns. SMEs assess the operational impact as very high, resulting in a score of 5.

Safety Impact: SMEs assumed an SN1 system used in the worst possible way could affect the valves on the main pipeline and likely would not directly affect safety and protection systems. In addition to the safety designs of control systems, standard safety practices are an additional layer protecting personnel from harm. Safety impacts of SN1 can be very high as the system could be used to initiate an emergency shutdown or cause cascading effects with pumping or booster stations that could lead to very dangerous conditions in midstream liquid products pipelines. As an example of how severe safety impacts can be, SMEs cited the Olympic pipeline explosion where a SCADA system malfunctioned resulting in three deaths, eight injuries, and $58.5 million of estimated damages.[28, 29] SMEs assess the safety impact as very high, resulting in a score of 5.

Environmental Impact: Environmental impacts of the SN1 system can be very high because manipulation could cause overpressure situations, resulting in spills. SN1 also could be used to spoof alarms and spoof leak detection, allowing leaks to occur without detection. As an example of how severe environmental impacts can be, SMEs cited the Olympic pipeline explosion where a SCADA system malfunctioned spilling approximately 277,200 gallons of gasoline into a stream.[30] SMEs assess the environmental impact as very high, resulting in a score of 5.

Prevalence

Ubiquity: MRC1 estimates SN1 oil midstream market share at 12-15 percent for transport.[31] The same report identified SN1 as a market leader. An SN1 website states it is used by 45 percent of U.S. liquids pipelines.[32] The CyTRICS prioritization team assesses ubiquity as very high, resulting in a score of 5.

Deployment Scale: MRC1 estimates more than 255 systems installed within 150 energy companies in the United States and Canada. MRC1 states 9 of 20 major North American oil and gas companies have SN1 systems installed, including Company C, Company D, Company E, Company F, and Company G.[33] Market transport company also uses SN1 according to the Company H website.[34] An SN1 website states it is used by 45 percent of U.S. liquids pipelines.[35] The CyTRICS prioritization team assesses deployment scale as very high, resulting in a score of 5.

Remaining Period of Use: The SN1 website supporting use in the oil subsector provides no indication SN1 is nearing end of life.[36] The Market Research Company report indicates SN1 is currently at a 7-year high for market share. For these reasons, CyTRICS does not anticipate SN1 use in the oil subsector to end in the next five years. The CyTRICS prioritization team assesses remaining period of use to be more than five years which is in the medium range, resulting is a score of 3D.

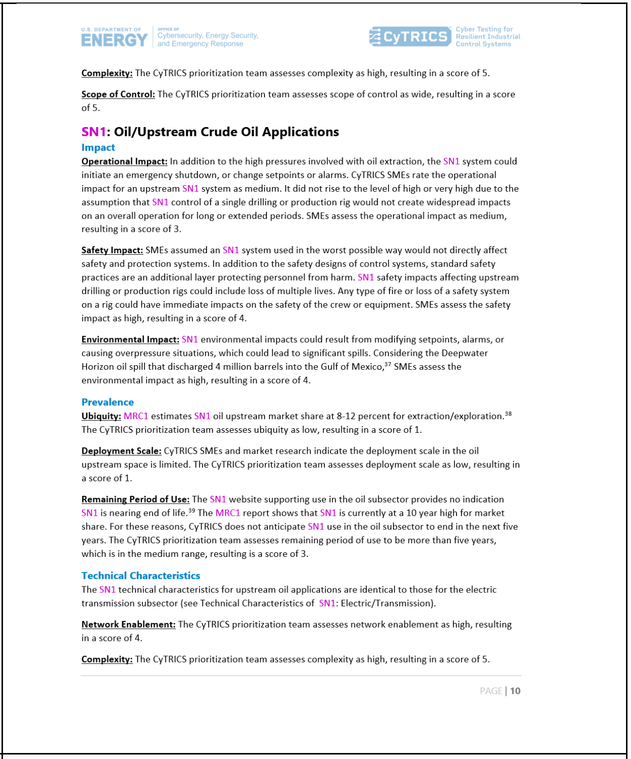
Technical Characteristics

The SN1 technical characteristics for midstream oil applications are identical to those for the electric transmission subsector (see Technical Characteristics of SN1: Electric/Transmission).

Network Enablement: The CyTRICS prioritization team CyTRICS assesses network enablement as high, resulting in a score of 4.

PAGE | 9

Page 9 of a sample Prioritization Report.



Complexity: The CyTRICS prioritization team assesses complexity as high, resulting in a score of 5.

Scope of Control: The CyTRICS prioritization team assesses scope of control as wide, resulting in a score of 5.

SN1: Oil/Upstream Crude Oil Applications

Impact

Operational Impact: In addition to the high pressures involved with oil extraction, the SN1 system could initiate an emergency shutdown, or change setpoints or alarms. CyTRICS SMEs rate the operational impact for an upstream SN1 system as medium. It did not rise to the level of high or very high due to the assumption that SN1 control of a single drilling or production rig would not create widespread impacts on an overall operation for long or extended periods. SMEs assess the operational impact as medium, resulting in a score of 3.

Safety Impact: SMEs assumed an SN1 system used in the worst possible way would not directly affect safety and protection systems. In addition to the safety designs of control systems, standard safety practices are an additional layer protecting personnel from harm. SN1 safety impacts affecting upstream drilling or production rigs could include loss of multiple lives. Any type of fire or loss of a safety system on a rig could have immediate impacts on the safety of the crew or equipment. SMEs assess the safety impact as high, resulting in a score of 4.

Environmental Impact: SN1 environmental impacts could result from modifying setpoints, alarms, or causing overpressure situations, which could lead to significant spills. Considering the Deepwater Horizon oil spill that discharged 4 million barrels into the Gulf of Mexico,[37] SMEs assess the environmental impact as high, resulting in a score of 4.

Prevalence

Ubiquity: MRC1 estimates SN1 oil upstream market share at 8-12 percent for extraction/exploration.[38] The CyTRICS prioritization team assesses ubiquity as low, resulting in a score of 1.

Deployment Scale: CyTRICS SMEs and market research indicate the deployment scale in the oil upstream space is limited. The CyTRICS prioritization team assesses deployment scale as low, resulting in a score of 1.

Remaining Period of Use: The SN1 website supporting use in the oil subsector provides no indication SN1 is nearing end of life.[39] The MRC1 report shows that SN1 is currently at a 10 year high for market share. For these reasons, CyTRICS does not anticipate SN1 use in the oil subsector to end in the next five years. The CyTRICS prioritization team assesses remaining period of use to be more than five years, which is in the medium range, resulting is a score of 3.

Technical Characteristics

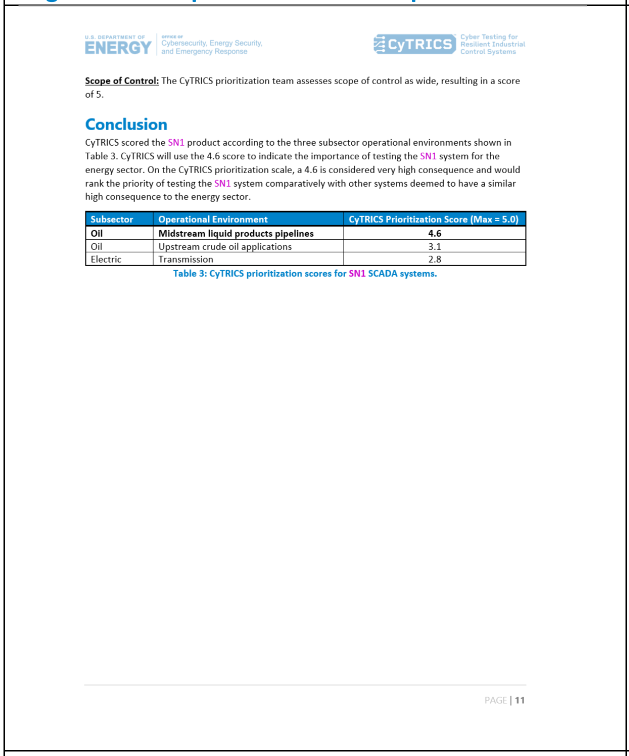
The SN1 technical characteristics for upstream oil applications are identical to those for the electric transmission subsector (see Technical Characteristics of SN1: Electric/Transmission).

Network Enablement: The CyTRICS prioritization team assesses network enablement as high, resulting in a score of 4.

Complexity: The CyTRICS prioritization team assesses complexity as high, resulting in a score of 5.

PAGE | 10

Page 10 of a sample Prioritization Report.



Scope of Control: The CyTRICS prioritization team assesses scope of control as wide, resulting in a score of 5.

Conclusion

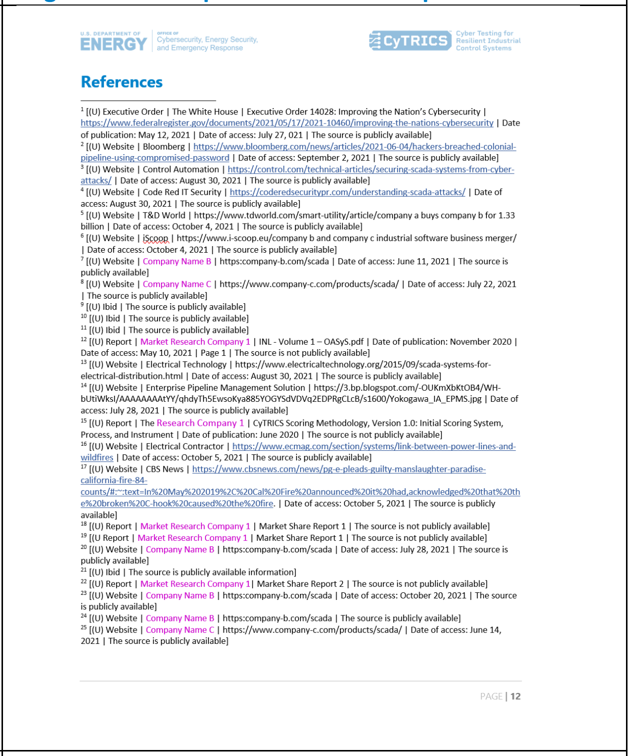
CyTRICS scored the SN1 product according to the three subsector operational environments shown in Table 3. CyTRICS will use the 4.6 score to indicate the importance of testing the SN1 system for the energy sector. On the CyTRICS prioritization scale, a 4.6 is considered very high consequence and would rank the priority of testing the SN1 system comparatively with other systems deemed to have a similar high consequence to the energy sector.

Subsector	Operational Environment	CyTRICS Prioritization Score (Max = 5.0)
Oil	**Midstream liquid products pipelines**	**4.6**
Oil	Upstream crude oil applications	3.1
Electric	Transmission	2.8

Table 3: CyTRICS prioritization scores for SN1 SCADA systems.

PAGE | 11

Page 11 of a sample Prioritization Report.

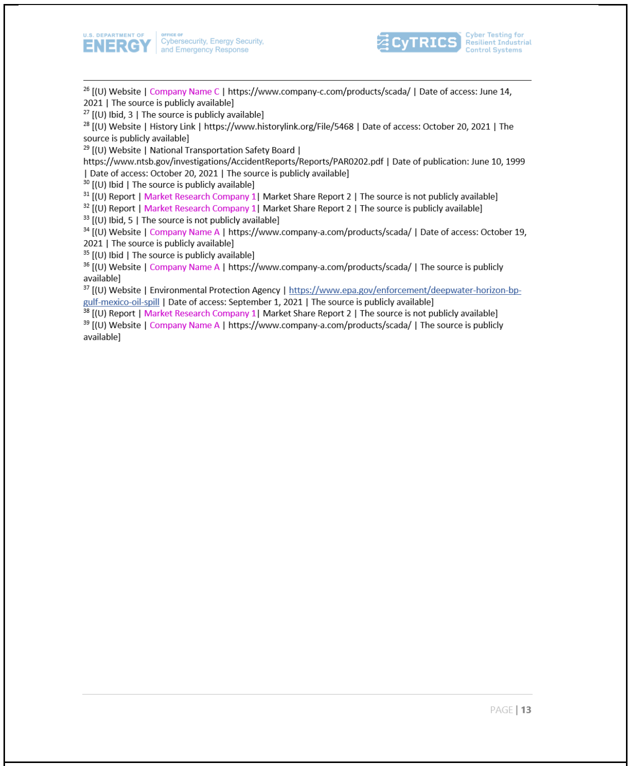


References

[1] [(U) Executive Order | The White House | Executive Order 14028: Improving the Nation's Cybersecurity | https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity | Date of publication: May 12, 2021 | Date of access: July 27, 021 | The source is publicly available]
[2] [(U) Website | Bloomberg | https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password | Date of access: September 2, 2021 | The source is publicly available]
[3] [(U) Website | Control Automation | https://control.com/technical-articles/securing-scada-systems-from-cyber-attacks/ | Date of access: August 30, 2021 | The source is publicly available]
[4] [(U) Website | Code Red IT Security | https://coderedsecuritypr.com/understanding-scada-attacks/ | Date of access: August 30, 2021 | The source is publicly available]
[5] [(U) Website | T&D World | https://www.tdworld.com/smart-utility/article/company a buys company b for 1.33 billion | Date of access: October 4, 2021 | The source is publicly available]
[6] [(U) Website | iScoop | https://www.i-scoop.eu/company b and company c industrial software business merger/ | Date of access: October 4, 2021 | The source is publicly available]
[7] [(U) Website | Company Name B | https:company-b.com/scada | Date of access: June 11, 2021 | The source is publicly available]
[8] [(U) Website | Company Name C | https://www.company-c.com/products/scada/ | Date of access: July 22, 2021 | The source is publicly available]
[9] [(U) Ibid | The source is publicly available]
[10] [(U) Ibid | The source is publicly available]
[11] [(U) Ibid | The source is publicly available]
[12] [(U) Report | Market Research Company 1 | INL - Volume 1 – OASyS.pdf | Date of publication: November 2020 | Date of access: May 10, 2021 | Page 1 | The source is not publicly available]
[13] [(U) Website | Electrical Technology | https://www.electricaltechnology.org/2015/09/scada-systems-for-electrical-distribution.html | Date of access: August 30, 2021 | The source is publicly available]
[14] [(U) Website | Enterprise Pipeline Management Solution | https://3.bp.blogspot.com/-OUKmXbKtOB4/WH-bUtiWksI/AAAAAAAAtYY/qhdyTh5EwsoKya885YOGYSdVDVq2EDPRgCLcB/s1600/Yokogawa_IA_EPMS.jpg | Date of access: July 28, 2021 | The source is publicly available]
[15] [(U) Report | The Research Company 1 | CyTRICS Scoring Methodology, Version 1.0: Initial Scoring System, Process, and Instrument | Date of publication: June 2020 | The source is not publicly available]
[16] [(U) Website | Electrical Contractor | https://www.ecmag.com/section/systems/link-between-power-lines-and-wildfires | Date of access: October 5, 2021 | The source is publicly available]
[17] [(U) Website | CBS News | https://www.cbsnews.com/news/pg-e-pleads-guilty-manslaughter-paradise-california-fire-84-counts/#:~:text=In%20May%202019%2C%20Cal%20Fire%20announced%20it%20had,acknowledged%20that%20the%20broken%20C-hook%20caused%20the%20fire. | Date of access: October 5, 2021 | The source is publicly available]
[18] [(U) Report | Market Research Company 1 | Market Share Report 1 | The source is not publicly available]
[19] [(U Report | Market Research Company 1 | Market Share Report 1 | The source is not publicly available]
[20] [(U) Website | Company Name B | https:company-b.com/scada | Date of access: July 28, 2021 | The source is publicly available]
[21] [(U) Ibid | The source is publicly available information]
[22] [(U) Report | Market Research Company 1| Market Share Report 2 | The source is not publicly available]
[23] [(U) Website | Company Name B | https:company-b.com/scada | Date of access: October 20, 2021 | The source is publicly available]
[24] [(U) Website | Company Name B | https:company-b.com/scada | The source is publicly available]
[25] [(U) Website | Company Name C | https://www.company-c.com/products/scada/ | Date of access: June 14, 2021 | The source is publicly available]

PAGE | 12

Page 12 of a sample Prioritization Report.



U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response
CyTRICS Cyber Testing for Resilient Industrial Control Systems

[26] [(U) Website | Company Name C | https://www.company-c.com/products/scada/ | Date of access: June 14, 2021 | The source is publicly available]
[27] [(U) Ibid, 3 | The source is publicly available]
[28] [(U) Website | History Link | https://www.historylink.org/File/5468 | Date of access: October 20, 2021 | The source is publicly available]
[29] [(U) Website | National Transportation Safety Board | https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf | Date of publication: June 10, 1999 | Date of access: October 20, 2021 | The source is publicly available]
[30] [(U) Ibid | The source is publicly available]
[31] [(U) Report | Market Research Company 1| Market Share Report 2 | The source is not publicly available]
[32] [(U) Report | Market Research Company 1| Market Share Report 2 | The source is publicly available]
[33] [(U) Ibid, 5 | The source is not publicly available]
[34] [(U) Website | Company Name A | https://www.company-a.com/products/scada/ | Date of access: October 19, 2021 | The source is publicly available]
[35] [(U) Ibid | The source is publicly available]
[36] [(U) Website | Company Name A | https://www.company-a.com/products/scada/ | The source is publicly available]
[37] [(U) Website | Environmental Protection Agency | https://www.epa.gov/enforcement/deepwater-horizon-bp-gulf-mexico-oil-spill | Date of access: September 1, 2021 | The source is publicly available]
[38] [(U) Report | Market Research Company 1| Market Share Report 2 | The source is not publicly available]
[39] [(U) Website | Company Name A | https://www.company-a.com/products/scada/ | The source is publicly available]

PAGE | 13

Page 13 of a sample Prioritization Report.

Citations

[i] Office of Cybersecurity, Energy Security, and Emergency Response. “Reference Architecture for Electric Energy OT.” Accessed 14 October 2022. https://secure-energy.inl.gov/.

[ii] Office of Cybersecurity, Energy Security, and Emergency Response. “Reference Architecture for Electric Energy OT.” Accessed 14 October 2022. https://secure-energy.inl.gov/.

[iii] Office of Cybersecurity, Energy Security, and Emergency Response. “Reference Architecture for Electric Energy OT.” Accessed 14 October 2022. https://secure-energy.inl.gov/.

[iv] Office of Cybersecurity, Energy Security, and Emergency Response. “Reference Architecture for Electric Energy OT.” Accessed 14 October 2022. https://secure-energy.inl.gov/.

[v] Office of Cybersecurity, Energy Security, and Emergency Response. “Reference Architecture for Electric Energy OT.” Accessed 14 October 2022. https://secure-energy.inl.gov/.

[vi] TATA Consultancy Services. “Reference3 Architecture Guided Digital Initiative Assessment in Oil & Gas Sector.” Accessed 14 October 2022. https://www.tcs.com/content/dam/tcs/pdf/corporatetcs/digital-transformation-oil-gas-value-chain1.pdf

[7] [(U) Website | Company Name A | https://www.cna.com/products/overview| Date of access: August 16, 2021 | The source is publicly available]

[8] [(U) Executive Order | The White House | Executive Order 14028: Improving the Nation’s Cybersecurity | https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity | Date of publication: May 12, 2021 | Date of access: July 27, 021 | The source is publicly available]

[9] [(U) Website | Company Name A | https://www.cna.com/products/overview| Date of access: August 16, 2021 | The source is publicly available]

[10] [(U) IT Guide | Company Name A | https://download.cna.com/user_guide.html | Date of access: August 16, 2021 | The source is publicly available]

[11] [(U) Vendor A Market Share Report, 1| The source is not publicly available]

[12] [(U) Website | Company Name A | https://www.cna.com/products/overview | Date of access: August 16, 2021 | The source is publicly available]

[13] [(U) Report | The MITRE Corporation | CyTRICS Scoring Methodology, Version 1.0: Initial Scoring System, Process, and Instrument | Date of publication: June 2020 | The source is not publicly available]

[14] [(U) Vendor A Market Share Report, 1| The source is not publicly available]

[15] [(U) Vendor A Market Share Report, 1| The source is not publicly available]

[16] [(U) Vendor A Market Share Report, 1| The source is not publicly available]

[17] [(U) Vendor A Market Share Report, 1| The source is not publicly available]

[18] [(U) IT Guide | Company Name A | https://download.cna.com/IT_guide.html | Date of access: August 16, 2021 | The source is publicly available]

[19] [(U) IT Guide | Company Name A | https://download.cna.com/IT_guide.html | Date of access: August 16, 2021 | The source is publicly available]

[20] [(U) User Guide | Company Name A | https://download.cna.com/user_guide.html | Date of access: August 16, 2021 | The source is publicly available]

[21] [(U) Product Brochure | Company Name A | https://download.cna.com/product_brochure.html | Date of access: August 16, 2021 | The source is publicly available]