Trade-off Analysis of Operational Technologies to Advance Cyber Resilience through Automated and Autonomous Response to Threats

September 2022

Craig G Rieger, Robert Christopher Ivans, Shannon Leigh Eggers, Costas Kolias

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-22-67746-Revision-0

Trade-off Analysis of Operational Technologies to Advance Cyber Resilience through Automated and Autonomous Response to Threats

Craig G Rieger, Robert Christopher Ivans, Shannon Leigh Eggers, Costas Kolias

September 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517, DE-AC07-05ID14517

Trade-off Analysis of Operational Technologies to Advance Cyber Resilience through Automated and Autonomous Response to Threats

Craig Rieger
National and Homeland Security
Idaho National Laboratory
Idaho Falls, ID
craig.rieger@inl.gov

Constantinos Kolias
Department of Computer Science
University of Idaho
Idaho Falls, ID
kolias@uidaho.edu

Robert C. Ivans
National and Homeland Security
Idaho National Laboratory
Idaho Falls, ID
robert.ivans@inl.gov

Shannon Eggers
National and Homeland Security
Idaho National Laboratory
Idaho Falls, ID
shannon.eggers@inl.gov

***Abstract*—The advancement of cyber resilience requires a preliminary stage of characterizing the trade-off space of mitigation options and how these might affect the stability and determinism of an operational technology (OT). This first step will set the stage for the proper cyber-secure and cyber-resilient design and confirm the affects that can be considered and approved by the OT and the security groups. To provide a baseline for this discussion, this paper provides a consideration of the cyber-physical interactions, possible mitigation steps against certain attacks and their corresponding affects that lend to the security design planning and evaluation process. As an integral part of the proposed scheme this work introduces the concept of system-wide fuzzer, i.e., a tool that manipulates the system state in an effort to determine mitigation response sequences that minimize detriments and maximize benefit in accordance with specified operational requirements.**

***Index Terms*—automated, autonomous, cyber, response, mitigation**

I. Introduction

The ability to advance response strategies against cyber-attacks and reduce the reaction time from seconds down to milliseconds requires a pathway to automated and autonomous response. To allow such considerations to be implemented in Operational Technology (OT) environments, it is imperative to have a clear understanding of the physical process system effects that are spawned from modifying the network behavior. One way to achieve this, at least to some extent, is by adopting design philosophies that fully characterize the dynamic interaction of setpoints and data that are necessary for the operation of the OT system. This is especially critical where the dependencies are associated with the dynamics of feedback control.

The purpose of this paper is to advance the schema for evaluating OT cyber-resilience architectures to enable the application of automated and autonomous mitigation to cyber-attack. This results in a trade-off situation. On the one hand, remediating actions may mitigate the impact of cyber-attacks. On the other hand, such measures may threaten system stability and can compromise the deterministic nature of OT. This trade-off space analysis provides a process to consider cyber and physical mitigations to an attack and then confirm whether the desired level of resilience of the system is maintained. Towards achieving this, the time dynamics will be considered, as well as the data dependencies. The resulting trade-off construct provides a framework for enumerating the types of mitigations that are acceptable in achieving a desired level of cyber-resilience.

Prior efforts in the field of response methods and systems are largely centralized for proper operation [1]. In our case, the proposed methods are distributed, building upon prior considerations for cyber resilience through multiagent architectures [2]. In this context, while practical metrics have been defined in the past [3], the ability to adapt [4] to what may be unexpected failures such as cyber-attack are at the heart of the definition to resilience [5]. Therefore, in this work, as a means to evaluate the resilience to the proposed cyber and physical mitigations, the concept of an OT, systemic fuzzer is introduced. The reader should notice that within the scope of the proposed scheme, this type of technology is not used as a means to merely discover exploitable cyber-vulnerabilities. This is how software and protocol fuzzing tools are commonly used in cybersecurity analysis [6]–[11] . Rather, the purpose of a systemic fuzzer is to test the proposed combinations of responses and variations of such to confirm system response and ultimately determine the optimum resilience [12]. Other work has considered a systemic approach to network based vulnerabilities to correlate weaknesses, but generally extends the traditional goal of a fuzzer [13].

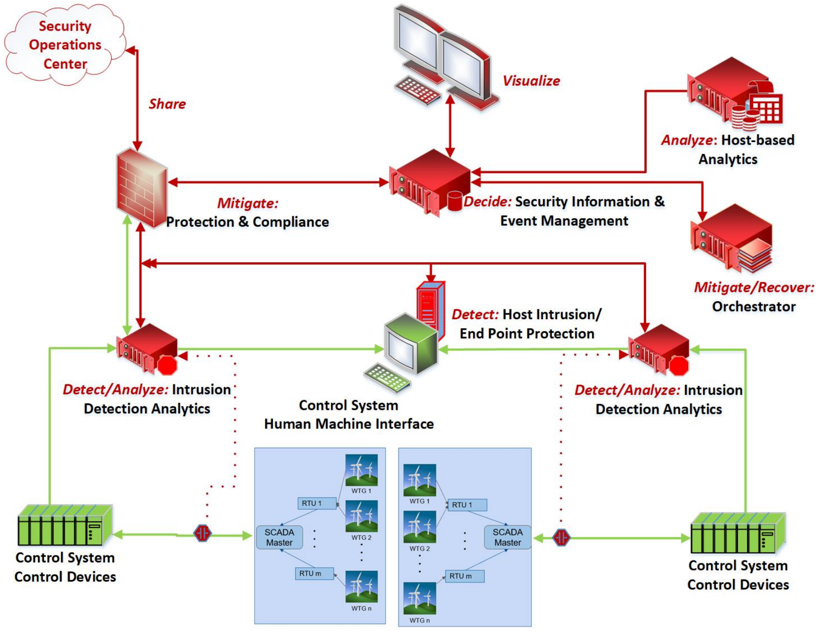

Security Operations Center
Share
Visualize
Analyze: Host-based Analytics
Mitigate: Protection & Compliance
Decide: Security Information & Event Management
Mitigate/Recover: Orchestrator
Detect: Host Intrusion/ End Point Protection
Detect/Analyze: Intrusion Detection Analytics
Control System Human Machine Interface
Detect/Analyze: Intrusion Detection Analytics
RTU 1
WTG 1
SCADA Master
WTG 2
RTU m
WTG n
Control System Control Devices
Control System Control Devices

Fig. 1: Reference Architecture

II. OT Architectural Interactions

A simplified view of a reference architecture for an OT system is provided in Fig. 1. A reference architecture includes several elements:

- Detect: Includes methods and systems for the monitoring and analysis of network traffic to recognize anomalies and undesirable traffic.
- Analyze: Comprises of methods, including machine learning, for acquiring details regarding the nature and gaining insight in the execution methodology of the attack.
- Decide/Visualize: Encompasses methods for the presentation of information to cyber-defenders for quick recognition and response.
- Mitigate/Recover: Incorporates a set of methods to stop a cyber-attack and reverse any negative affects.
- Share: Refers to a set of tools that describe details of a seen cyber-attack. This information can be securely shared to benefit the defenses of other organizations in the future.

The reference architecture provides a foundation on which cyber-physical responses are built to provide an increased level of security. However, recognizing the traffic patterns and resulting metrics requires an understanding of two critical factors namely, timing and data [5].

Precisely, when it comes to evaluating the considerations for cyber-physical response that can impact the stable operation of the OT, one must factor in both timing and data issues [5]. Considering time and data in the form of Fig. 2, the resilience impact on the system can be illustrated [4]. The resilience of a system can be understood by its ability to initially reduce the impact of a disturbance (resist stage) and recover from it in both the short- (respond) and long term (restore). In further detail, in Fig. 2 the red curve indicates the trajectory of a system that is not particularly resilient and falls below some predefined normalcy criterion while the green curves are systems that maintain a minimum level of acceptable operation during this crisis, indicating resilient (as opposed to fragile/brittle) systems (the upper, more so than the lower).

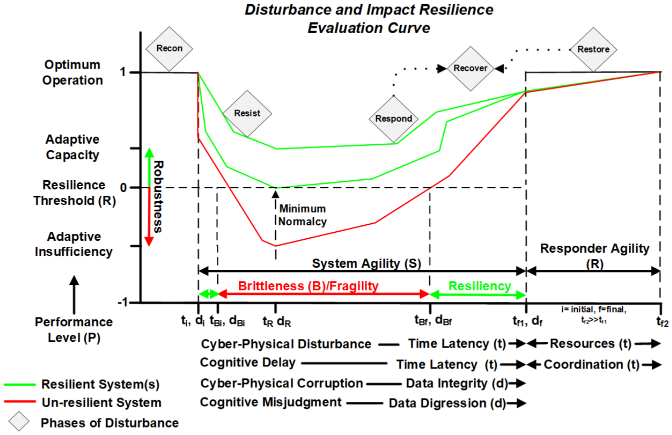


Fig. 2: Disturbance and Impact Resilience Curve. [4]

To provide context that will be relevant for evaluating the trade-off space, a decomposition of the timing and data considerations must be defined in terms of OT functionality. Timing issues include considerations that revolve around latency. Data issues involve the types of physical parameters for monitoring and control that are shared on a OT network. While many roles could be considered for human monitoring and response, such as instrument technician and operator, this paper focuses

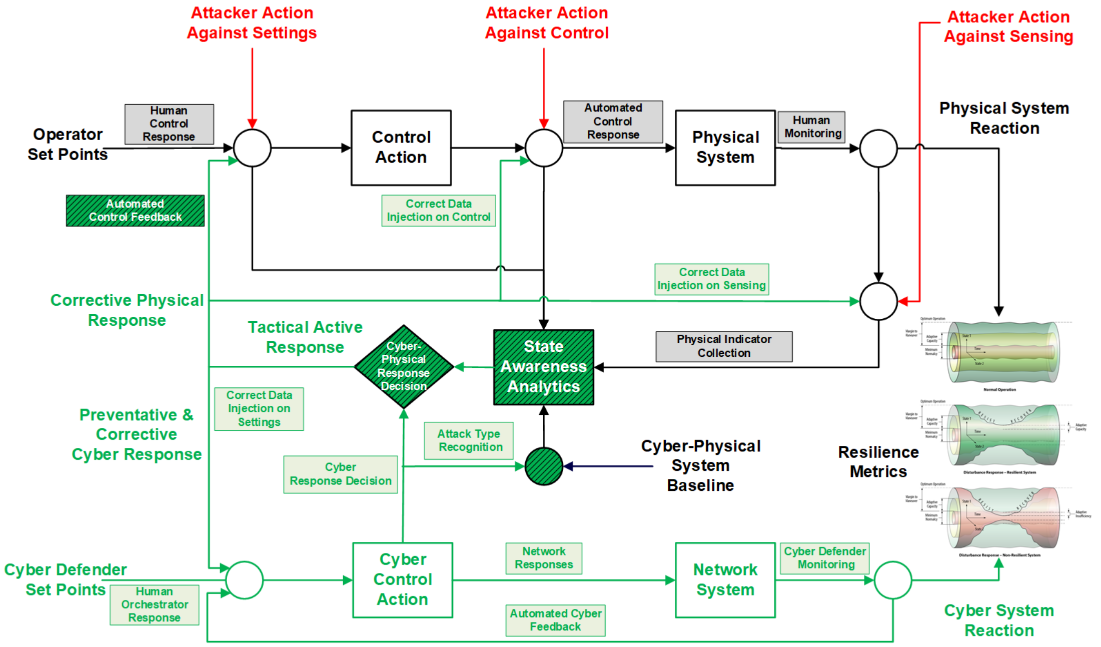

Attacker Action Against Settings
Attacker Action Against Control
Attacker Action Against Sensing
Operator Set Points
Human Control Response
Control Action
Automated Control Response
Physical System
Human Monitoring
Physical System Reaction
Automated Control Feedback
Correct Data Injection on Control
Correct Data Injection on Sensing
Corrective Physical Response
Tactical Active Response
Cyber-Physical Response Decision
State Awareness Analytics
Physical Indicator Collection
Correct Data Injection on Settings
Attack Type Recognition
Preventative & Corrective Cyber Response
Cyber Response Decision
Cyber-Physical System Baseline
Resilience Metrics
Optimum Operation
Margin to Maneuver
Adaptive Capacity
Minimum Normalcy
State 1
Time
State 2
Normal Operation
RESIST
RECOVER
Disturbance Response – Resilient System
Adaptive Insufficiency
Disturbance Response – Non-Resilient System
Cyber Defender Set Points
Human Orchestrator Response
Cyber Control Action
Network Responses
Automated Cyber Feedback
Network System
Cyber Defender Monitoring
Cyber System Reaction

Fig. 3: Cyber-Physical Response for Trade-off

only on humans operating the OT. A simple taxonomy of the data and time considerations is included below, where plant is associated with the physical process (i.e., power, chemical, etc.):

- Plant Physical Data
  - Human Monitoring
    - Raw Analog Plant Information
    - Raw Digital Plant Information
    - System State
    - Raw Data Analytics
  - Human Plant Response
    - Plant Controller Set Points
    - Plant Hand Switch Positions
    - Plant Tuning Parameters
  - System State
    - OT Device Health Status
    - OT Network Health Status
- Time
  - Loss of Determinism
  - Packet Not Delivered

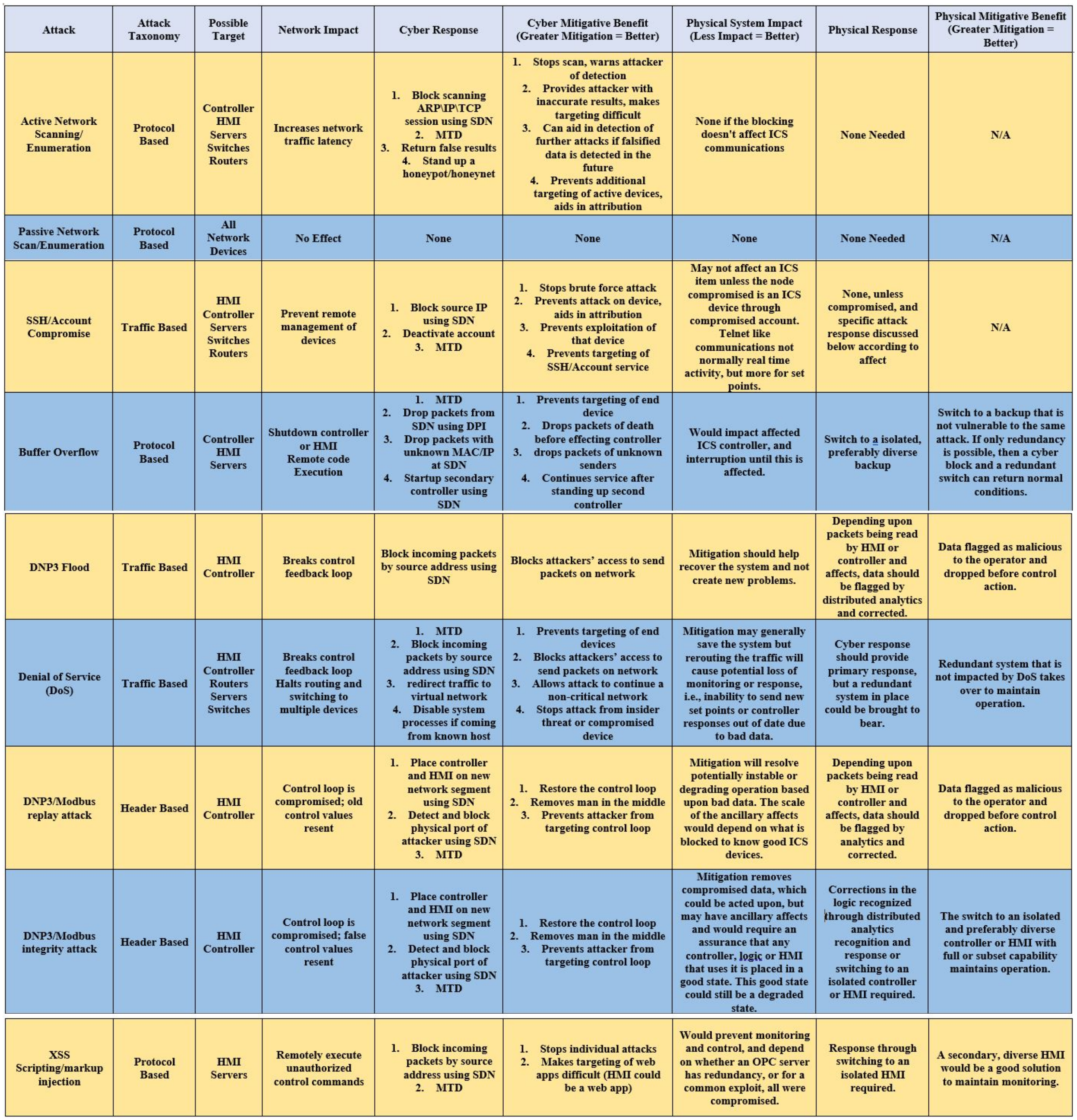
The specific focus of these categories are the pertinent information used in OT operation, and not in the communications semantics. The application of a cyber-physical feedback loop to mitigate attacks in real time is provided in Fig. 3. To complement analytics of recognition that are informed by intrusion detection system(s) (IDS), both commercial and those advanced from research, resulting cyber corrections can include software defined network (SDN) and firewall changes that isolate/redirect expected malicious communications. Physical corrections can include filtering/offsetting malicious changes to return to normal. The cyber and physical system reaction provides the basis for interpreting the benefit of the mitigation, as well as the cost of the mitigation, all of which can be confirmed by metrics on resilience.

From the standpoint of the physical corrections, it must be noted that the communications pathways must be maintained to ensure that corrections can be implemented on the OT devices, such as the process controller. For the cyber corrections, the communications would generally be on a separate security management network but the design of the communications is still as important. That is, the distribution of the recognition and response to ensure both a continued cyber resilience in contested space [4]. Summarizing, the resilience of the communications design is dependent upon the ability to maintain both monitoring/control for process operation and security alert recognition/response.

The taxonomy of the data and time for the cyber system can be considered in similar fashion to that of the physical (provided below). While the cyber system communications might be on a separate network from the physical, this taxonomy provides insights into the trade-off design considerations that must be considered to ensure the operations of the communications pathways. The human roles would be different from the physical, and include cyber defenders and analysts.

- Cyber Data
  - Human (Cyber Defender) Monitoring
    - Raw Log Information
    - Raw IDS Information
    - System State
    - Raw Data Analytics
  - Human (Cyber Defender) Control Response
    - SDN Controller Set Points

Fig. 4: Cyber-Physical Trade-offs.
(See below for acronyms)



Attack	Attack Taxonomy	Possible Target	Network Impact	Cyber Response	Cyber Mitigative Benefit (Greater Mitigation = Better)	Physical System Impact (Less Impact = Better)	Physical Response	Physical Mitigative Benefit (Greater Mitigation = Better)
Active Network Scanning/ Enumeration	Protocol Based	Controller HMI Servers Switches Routers	Increases network traffic latency	1. Block scanning ARP\IP\TCP session using SDN 2. MTD 3. Return false results 4. Stand up a honeypot/honeynet	1. Stops scan, warns attacker of detection 2. Provides attacker with inaccurate results, makes targeting difficult 3. Can aid in detection of further attacks if falsified data is detected in the future 4. Prevents additional targeting of active devices, aids in attribution	None if the blocking doesn't affect ICS communications	None Needed	N/A
Passive Network Scan/Enumeration	Protocol Based	All Network Devices	No Effect	None	None	None	None Needed	N/A
SSH/Account Compromise	Traffic Based	HMI Controller Servers Switches Routers	Prevent remote management of devices	1. Block source IP using SDN 2. Deactivate account 3. MTD	1. Stops brute force attack 2. Prevents attack on device, aids in attribution 3. Prevents exploitation of that device 4. Prevents targeting of SSH/Account service	May not affect an ICS item unless the node compromised is an ICS device through compromised account. Telnet like communications not normally real time activity, but more for set points.	None, unless compromised, and specific attack response discussed below according to affect	N/A
Buffer Overflow	Protocol Based	Controller HMI Servers	Shutdown controller or HMI Remote code Execution	1. MTD 2. Drop packets from SDN using DPI 3. Drop packets with unknown MAC/IP at SDN 4. Startup secondary controller using SDN	1. Prevents targeting of end device 2. Drops packets of death before effecting controller 3. drops packets of unknown senders 4. Continues service after standing up second controller	Would impact affected ICS controller, and interruption until this is affected.	Switch to a isolated, preferably diverse backup	Switch to a backup that is not vulnerable to the same attack. If only redundancy is possible, then a cyber block and a redundant switch can return normal conditions.
DNP3 Flood	Traffic Based	HMI Controller	Breaks control feedback loop	Block incoming packets by source address using SDN	Blocks attackers' access to send packets on network	Mitigation should help recover the system and not create new problems.	Depending upon packets being read by HMI or controller and affects, data should be flagged by distributed analytics and corrected.	Data flagged as malicious to the operator and dropped before control action.
Denial of Service (DoS)	Traffic Based	HMI Controller Routers Servers Switches	Breaks control feedback loop Halts routing and switching to multiple devices	1. MTD 2. Block incoming packets by source address using SDN 3. redirect traffic to virtual network 4. Disable system processes if coming from known host	1. Prevents targeting of end devices 2. Blocks attackers' access to send packets on network 3. Allows attack to continue a non-critical network 4. Stops attack from insider threat or compromised device	Mitigation may generally save the system but rerouting the traffic will cause potential loss of monitoring or response, i.e., inability to send new set points or controller responses out of date due to bad data.	Cyber response should provide primary response, but a redundant system in place could be brought to bear.	Redundant system that is not impacted by DoS takes over to maintain operation.
DNP3/Modbus replay attack	Header Based	HMI Controller	Control loop is compromised; old control values resent	1. Place controller and HMI on new network segment using SDN 2. Detect and block physical port of attacker using SDN 3. MTD	1. Restore the control loop 2. Removes man in the middle 3. Prevents attacker from targeting control loop	Mitigation will resolve potentially instable or degrading operation based upon bad data. The scale of the ancillary affects would depend on what is blocked to know good ICS devices.	Depending upon packets being read by HMI or controller and affects, data should be flagged by analytics and corrected.	Data flagged as malicious to the operator and dropped before control action.
DNP3/Modbus integrity attack	Header Based	HMI Controller	Control loop is compromised; false control values resent	1. Place controller and HMI on new network segment using SDN 2. Detect and block physical port of attacker using SDN 3. MTD	1. Restore the control loop 2. Removes man in the middle 3. Prevents attacker from targeting control loop	Mitigation removes compromised data, which could be acted upon, but may have ancillary affects and would require an assurance that any controller, logic or HMI that uses it is placed in a good state. This good state could still be a degraded state.	Corrections in the logic recognized through distributed analytics recognition and response or switching to an isolated controller or HMI required.	The switch to an isolated and preferably diverse controller or HMI with full or subset capability maintains operation.
XSS Scripting/markup injection	Protocol Based	HMI Servers	Remotely execute unauthorized control commands	1. Block incoming packets by source address using SDN 2. MTD	1. Stops individual attacks 2. Makes targeting of web apps difficult (HMI could be a web app)	Would prevent monitoring and control, and depend on whether an OPC server has redundancy, or for a common exploit, all were compromised.	Response through switching to an isolated HMI required.	A secondary, diverse HMI would be a good solution to maintain monitoring.

(a) ARP = Address Resolution Protocol, ICS = Industrial Control System, IP = Internet Protocol, MTD = Moving Target Defense, TCP = Transport Control Protocol, XSS = Cross-Site Scripting

        - Security Appliance Parameters
    - Security System Health State
        - Security System Device Status
        - Security System Network Status
- Time
    - Latency of Packet Delivery
    - Packet Not Delivered

Considering these cyber and physical taxonomies, the elements of the reference architecture illustrated in 1 can be recognized. That is, detection, analysis and response are part of all cyber and physical feedback loops. As we shall see in the next section, the trade-off design can be further considered in terms of cyber-attack scenario types and potential cyber-physical responses.

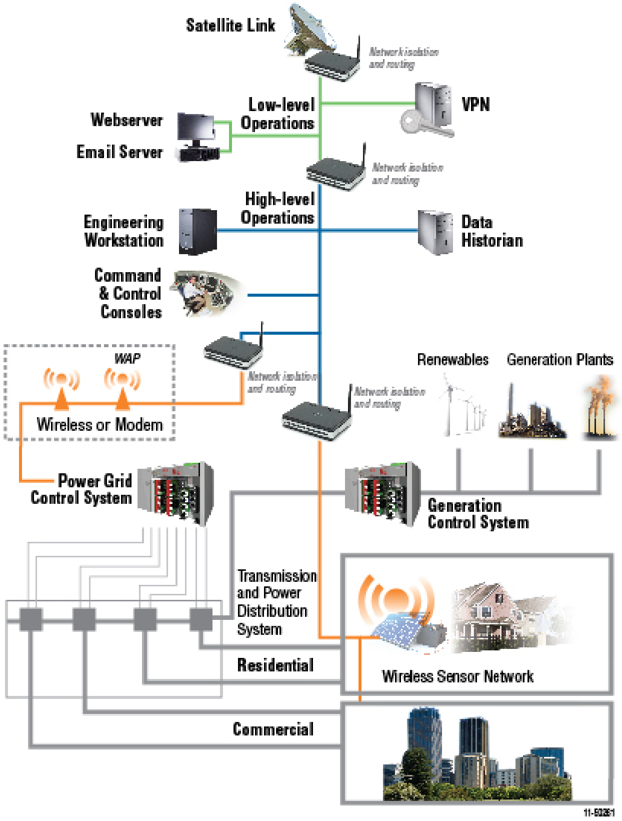

Satellite Link
Network isolation and routing
Webserver
Email Server
Low-level Operations
VPN
Network isolation and routing
Engineering Workstation
High-level Operations
Data Historian
Command & Control Consoles
WAP
Wireless or Modem
Network isolation and routing
Network isolation and routing
Renewables
Generation Plants
Power Grid Control System
Generation Control System
Transmission and Power Distribution System
Residential
Wireless Sensor Network
Commercial
11-50261

Fig. 5: OT Network

III. Taxonomy of Interaction and the Cyber-Physical Interface

Figure 4 provides a framework for considering the use of cyber and physical responses to several types of cyber-attack scenarios. These scenarios are reflective of Fig. 3, and provide the potential benefits from individual response approaches and the potential physical affects and resilience metrics [3]. The result of this breakdown provides a more generic approach to the considerations necessary for a trade-off analysis, which would preface the implementation of such an automated and autonomous response. Different response approaches could be applied for an individual network and considered as part of the design process.

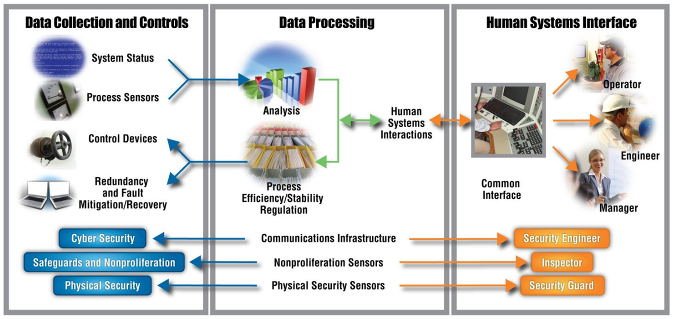


Fig. 6: Traditional OT Interfaces

The trade-off analysis provides a basis for evaluating the risk versus benefits, but this analysis must also consider the communications design and the benefits as well as limitations. The taxonomies provided in the prior section provide a consideration of the normal cyber and physical related parameter exchanges occurring over the communications system, which require consideration in developing a secure foundation for a communications system. The expectations go beyond what is required for reliable communications between OT devices, such as shown in Fig. 5. That is, in addition to a reference architecture for security, as is given in Fig. 1, other foundational security considerations are often considered and implemented. These include segmentation of traffic and isolation of the most critical aspects. The trade-off options provide the basis for application of active network adaptations for cyber, such as with SDN, and active physical adaptations, such as switching to a backup, known good device or known-secure device corrections to mitigate undesirable cyber-attacks, such as parameter offsets from data injection.

The resulting implementation of an automated and autonomous response will build upon the secure foundation designed in the communications system. However, the confirmation of the appropriateness of these cyber-physical responses would need to be further validated. In addition, validations to consider the breadth of potential responses would further provide an understanding of the sensitivity of the system to certain changes. In the next section, we will provide a basis to consider the validations.

IV. Trade-off Space Validations

While transport/network layer communications based upon transport control protocol, internet protocol (IP) communications networks are now prevalent, many OT vendors include their own protocol application to ensure determinism and proprietary device interface functionality. The common types of traditional OT functions and data interfaces are illustrated in Fig. 6. The network integration is often based upon maintaining this functionality and interfaces, but does not consider designs to accommodate the benefits of new cybersecurity

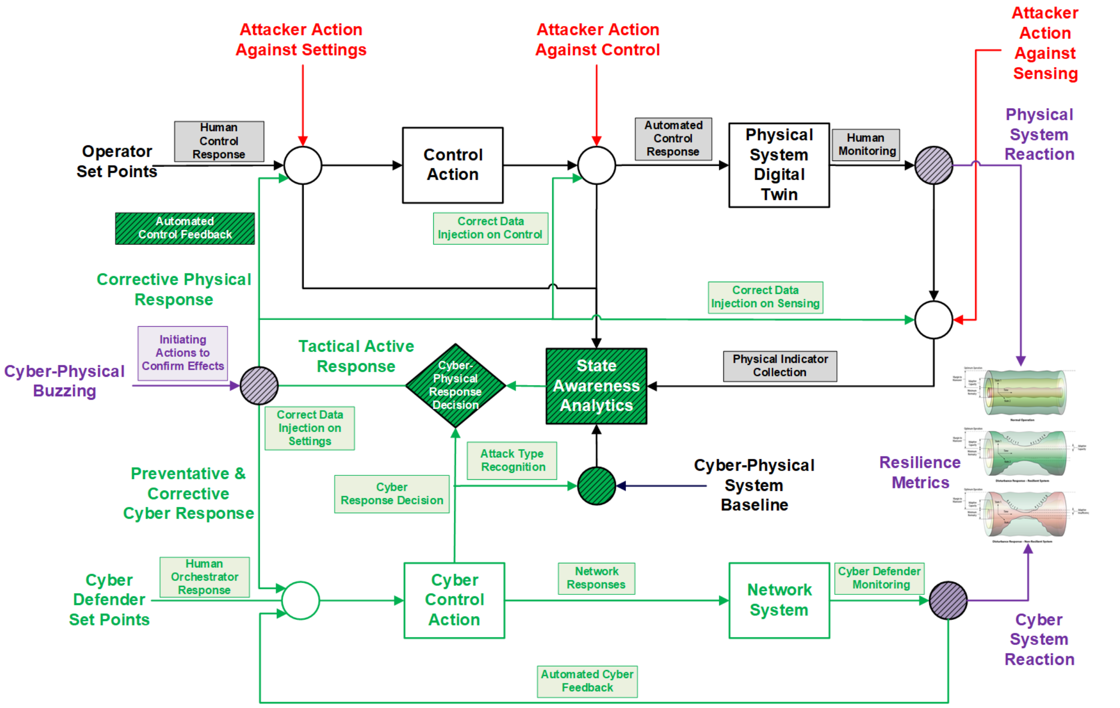

Attacker Action Against Settings
Attacker Action Against Control
Attacker Action Against Sensing
Operator Set Points
Human Control Response
Control Action
Automated Control Response
Physical System Digital Twin
Human Monitoring
Physical System Reaction
Automated Control Feedback
Correct Data Injection on Control
Corrective Physical Response
Correct Data Injection on Sensing
Initiating Actions to Confirm Effects
Cyber-Physical Buzzing
Tactical Active Response
Cyber-Physical Response Decision
State Awareness Analytics
Physical Indicator Collection
Correct Data Injection on Settings
Attack Type Recognition
Cyber Response Decision
Preventative & Corrective Cyber Response
Cyber-Physical System Baseline
Resilience Metrics
Human Orchestrator Response
Cyber Defender Set Points
Cyber Control Action
Network Responses
Network System
Cyber Defender Monitoring
Cyber System Reaction
Automated Cyber Feedback

Fig. 7: Cyber-Physical Feedback for Evaluating Trade-off with Digital Twins

technology and potential cyber-physical responses that could isolate or reroute communications in a mitigative response to a cyber-attack.

To design for such considerations in the future, a taxonomy of data exchange and time considerations will provide the foundation for application of response technologies. This includes technologies such as an SDN, which can be introduced when the trade-off space is informed by the OT design. The resulting guarantees will ensure that impact to the OT process is understood and minimized. However, leveraging current OT design tools that provide an understanding of this data exchange and time can start with the engineering workstations (EWS). For decades such design tools provided a means to develop the plant control configuration, operator HMI and other inter-node interactions. Enhancing these tools to consider and compile the communications-related dependencies would inform the taxonomy, and as a result, inform any potential affects that may occur as the results of cyber response.

Enhancing these tools to provide the ability to confirm the disturbance or delay of traffic could, in fact, provide a basis to plan for the interface that considers the mitigative action for a cyber-attack. The result would include a cyber-informed tool that would consider the communications boundaries that codify those parameters of greatest importance. Hardware-in-the-loop (HIL) testing with high fidelity emulations would confirm the effectiveness of the responses without unexpected impact. The important point is the communications dependence would now be instantiated and validated to confirm the benefit of the trade-off analysis in the OT design.

To provide the basis for HIL validation, the development of digital twins provides an opportunity to perform such trade-off analysis through systemic testing without concerns for physical impact. This would generally involve the integration of the emulation to the automation, logic or process controller. Such emulations can come from different vendors and specific to the domain, but ultimately should interface to the user-created control logic running on the same hardware as it would exist in the operating plant, i.e., power system, chemical plant, etc. In this way, the injection of mitigation responses will better reflect the hardware specific characteristics as would be seen in the plant.

In addition, considering the concept of a fuzzer can add formality to a test procedure for stressing the system to confirm response calls. As compared to the traditional use of a fuzzer that is used for the identification of vulnerabilities with a security implication, the new application would be for evaluating the impacts to the physical operation from implementation of cyber response methods. Such a design is simply illustrated with a modification of the prior trade-off diagram and shown in Fig. 7.

To distinguish this OT-specific application while paralleling the concept of a fuzzer, we are coining the new name ”buzzer.” The rationale for the buzzer would be to evaluate all potential cyber-physical responses and confirm the acceptability of the OT and coupled plant response (using a digital twin). For the physical responses, the consideration of where the physical data correction is performed and the timing of this correction will be critical to its effectiveness.

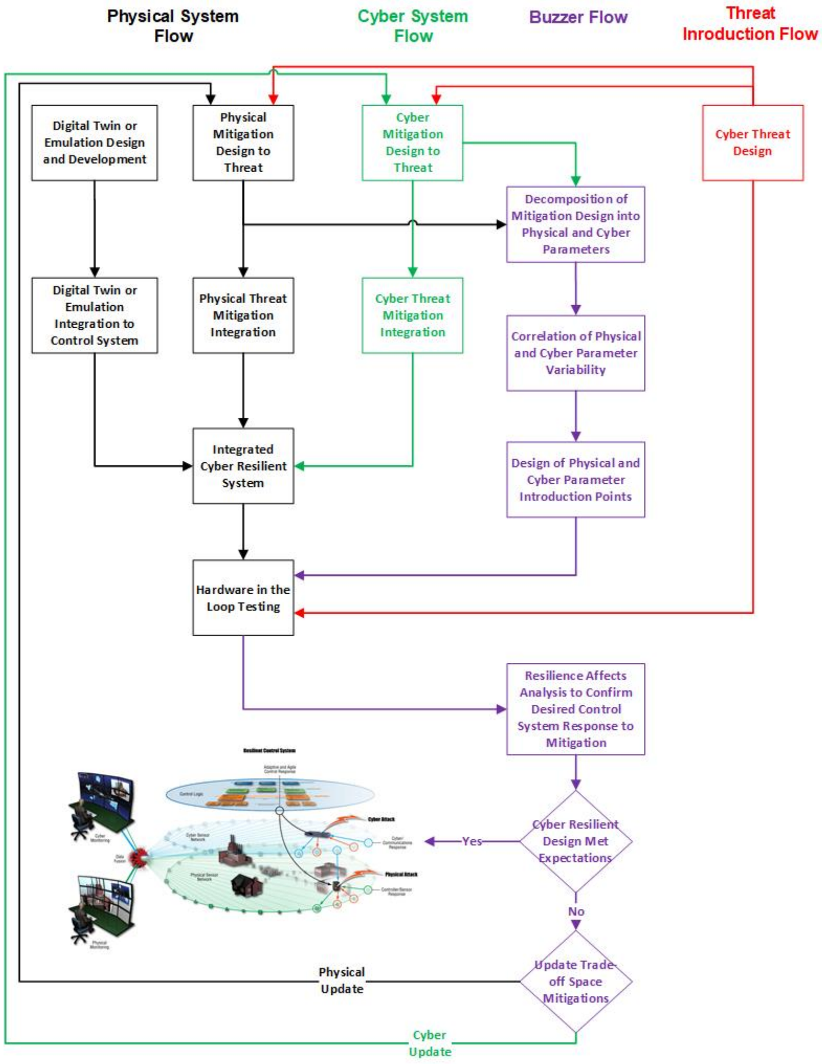

Physical System Flow
Cyber System Flow
Buzzer Flow
Threat Inroduction Flow
Digital Twin or Emulation Design and Development
Physical Mitigation Design to Threat
Cyber Mitigation Design to Threat
Cyber Threat Design
Decomposition of Mitigation Design into Physical and Cyber Parameters
Digital Twin or Emulation Integration to Control System
Physical Threat Mitigation Integration
Cyber Threat Mitigation Integration
Correlation of Physical and Cyber Parameter Variability
Integrated Cyber Resilient System
Design of Physical and Cyber Parameter Introduction Points
Hardware in the Loop Testing
Resilience Affects Analysis to Confirm Desired Control System Response to Mitigation
Cyber Resilient Design Met Expectations
Yes
No
Update Trade-off Space Mitigations
Physical Update
Cyber Update

Fig. 8: Tradeoff Analysis Process Flow for a OT Network

V. Trade-off Process Example

To illustrate the process for a trade-off analysis, consider Fig. 8, which provides a generalized flow diagram. Within this figure, consideration of the physical OT and emulated plant, both cyber and physical mitigations to the cyber threat, the buzzer analysis and potential threats are all represented. The challenges of providing a relevant trade-off analysis are based upon emulation or digital twin fidelity, the relevant representation of the hardware implementations of the OT, the scalability of the threat set identified and other factors. Metrics of resilience should consider the physical system resilience first, such as the referenced for power systems [14], and then evaluate how the type of cyber-attack would lead to this result [3]. For example, a denial of service attack can lead to a delay in communications that can cause control algorithms to base decisions on old data and yield instabilities in physical process responses.

The trade-off process starts with a design that considers the threats and responses, such as documented in Fig. 4. This design requires input from a team that includes the OT engineer, cybersecurity engineer/scientist and domain engineer (as a minimum). Based upon the trade-off design, the individual decomposition of the responses is considered in the design of the buzzer, that will inject these responses for a variety of cyber-attack sequences and then perform a comparative analysis to confirm the desired resilience is maximized and system impact is minimized.

VI. Summary

This paper has outlined a foundation for performing trade-off analysis between mitigation, benefit, and impact within OT environments. This necessary process will provide the stepping stone to informed acceptance of technologies to achieve cyber resilience.

Recognizing the taxonomy of the cyber and physical parameter interfaces can enable an understanding of the expected and relevant communications traffic for an OT system.

Through enhancement of current OT design tools to include communications consideration can inform the OT designer of the trade-off risk that are based upon these taxonomies. This understanding is necessary for OT asset owners before accepting cyber feedback responses, but even cybersecurity methods such as network segmentation.

Leveraging digital twins for plant emulation to measure impact and existing tools for response like SDN would allow for reducing the time to mitigate and reduce the impact from cyber-attack. Through a defined process for trade-off evaluation, the use of a buzzer would confirm the plant behavior for each cyber and physical response and provide the final confirmation of the design to the desired resilience and threat-resilient control system.

Acknowledgment

Effort performed through Department of Energy under U.S. DOE Idaho Operations Office Contract DE-AC07-05ID14517, as part of Laboratory Directed Research and Development, Resilient Control and Instrumentation Systems (ReCIS) program of Idaho National Laboratory.

References

[1] H. A. Kholidy, "Autonomous mitigation of cyber risks in the cyber–physical systems," Future Generation Computer Systems, vol. 115, pp. 171–187, 2021.

[2] C. Rieger, C. Kolias, J. Ulrich, and T. R. McJunkin, "A cyber resilient design for control systems," in 2020 Resilience Week (RWS), 2020, pp. 18–25.

[3] C. G. Rieger, "Resilient control systems practical metrics basis for defining mission impact," in 2014 7th International Symposium on Resilient Control Systems (ISRCS), 2014, pp. 1–10.

[4] C. Rieger, K. Schultz, T. Carroll, and T. McJunkin, "Resilient control systems—basis, benchmarking and benefit," IEEE Access, vol. 9, pp. 57 565–57 577, 2021.

[5] C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: Next generation design research," in 2009 2nd Conference on Human System Interactions, 2009, pp. 632–636.

[6] J. Somorovsky, "Systematic Fuzzing and Testing of TLS Libraries." Vienna Austria: ACM, Oct. 2016, pp. 1492–1504. [Online]. Available: https://dl.acm.org/doi/10.1145/2976749.2978411

[7] Y. Cai and W. K. Chan, "MagicFuzzer: Scalable deadlock detection for large-scale applications," 2012, pp. 606–616.

[8] S. Gan, C. Zhang, X. Qin, X. Tu, K. Li, Z. Pei, and Z. Chen, "CollAFL: Path Sensitive Fuzzing," in 2018 IEEE Symposium on Security and Privacy (SP), May 2018, pp. 679–696.

[9] C. Lemieux and K. Sen, "FairFuzz: a targeted mutation strategy for increasing greybox fuzz testing coverage." Montpellier France: ACM, Sep. 2018, pp. 475–485. [Online]. Available: https://dl.acm.org/doi/10.1145/3238147.3238176

[10] C. Aschermann, T. Frassetto, T. Holz, P. Jauernig, A.-R. Sadeghi, and D. Teuchert, "Nautilus: Fishing for Deep Bugs with Grammars," San Diego, CA, 2019.

[11] C. Aschermann, S. Schumilo, T. Blazytko, R. Gawlik, and T. Holz, "Redqueen: Fuzzing with Input-to-State Correspondence," San Diego, CA, 2019.

[12] C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: Next generation design research," in 2009 2nd Conference on Human System Interactions, 2009, pp. 632–636.

[13] Y. Chen, B. Xuan, C. M. Poskitt, J. Sun, and F. Zhang, "Active fuzzing for testing and securing cyber-physical systems," in Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis. ACM, jul 2020. [Online]. Available: https://doi.org/10.11452F3395363.3397376

[14] T. Phillips, T. McJunkin, C. Rieger, J. Gardner, and H. Mehrpouyan, "An operational resilience metric for modern power distribution systems," in 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2020, pp. 334–342.