MTR180048
MITRE TECHNICAL REPORT

MITRE

Assessment of Operational Energy System Cybersecurity Vulnerabilities

Performed at the request of the Assistant Secretary for Research and Engineering's Reliance 21 Energy & Power Community of Interest

Alexander D. Schlichting, Ph.D.

January 2018

Sponsor: OSD
Dept. No.: T821
Contract No.: W56KGU-16-C-0010
Project No.: 0717D190-EP

McLean, VA

Approved By

2/2/2018

Kurt Eisenbeiser, Ph.D.,
Power and Energy Systems Group Lead
T821, Emerging Technologies Department

Date

Abstract

The development of intelligent operational energy systems introduces significant cyber security and resiliency concerns to the science and technology community within the energy and power sector of the U.S. Department of Defense. Operational energy systems are comprised of cyber-physical systems and must be able to safely function and respond in challenging tactical environments. This report summarizes the findings of a study examining the common cyber vulnerabilities for intelligent operational energy systems, their potential impacts, and potential mitigation strategies. The result is a set of recommended next steps for the operational energy science and technology community.

This page intentionally left blank.

Executive Summary

The proliferation of intelligent, sometimes referred to as smart, digital control systems for complex physical processes has created an entirely new class of systems where cyber security is a concern: cyber-physical systems (CPS). CPS are engineered systems that integrate computational algorithms and physical components. For reference, a cyber event, in the context of CPS, includes any time a control signal is transmitted or a controller setting is modified. Advanced industrial controls, one type of CPS, face many challenges associated with ensuring cyber security and resiliency: long deployments with limited software patching, minimal local computing resource overhead for complex processes, use in systems with strict size, weight, and power restrictions, and significant interactions with the physical world and human users. The Department of Defense (DoD) Reliance 21 Energy & Power Community of Interest is concerned with the cyber security and resiliency of their next generation of intelligent operational energy systems, which leverages advances in tactical computing and processing capabilities to dynamically improve their performance based on the platform, its mission, and the operating environment. The purpose of this report is to provide an overview of the common cyber vulnerabilities for CPS relevant to intelligent operational energy systems, describe common methods used to mitigate these vulnerabilities, and provide recommendations for the way ahead.

Cyber security and resiliency of intelligent operational energy systems are a means to an end, specifically a way to provide mission assurance. The primary objective of mission assurance is for the mission to still be successful even if the system has been degraded. While the first component of mission assurance is to prevent malicious actors from exploiting a vulnerability to gain access to the system, the second component is to prevent them from causing an actual impact to the system, and the third component is to prevent those impacts from causing the mission to fail. These three components help explain the wide range of steps that individual power and energy systems researchers can take to improve mission assurance when developing intelligent control algorithms and device communications interfaces. The vulnerabilities of energy and power CPS, including intelligent operational energy systems, stem from features of the controls architecture, specification requirements for the system design, and, very frequently, implementation errors or oversights. Malicious actors can leverage these vulnerabilities to disrupt, deny, degrade, destroy, or deceive the system (or user), with a range of potential consequences for the overall mission.

During this study, multiple CPS cyber security and resiliency experts implored power and energy system researchers to consider all three mission assurance objectives, not just preventing malicious actors from causing harm once inside of the system. This is because an unsecure intelligent operational energy system could serve as a pathway to the rest of the platform through shared communications pathways. Bearing that in mind, the most common cyber vulnerabilities seen by the Department of Homeland Security for critical infrastructure CPS are: improper input validation by CPS, poor access controls to CPS or controls networks, and weak user and device authentication to execute access controls. All of these cyber vulnerabilities impact intelligent operational energy systems.

There are three types of cyber vulnerability mitigation strategies, or countermeasures, that could be used to address vulnerabilities in DoD intelligent operational energy systems. From the least to most costly these are: changing tactics, techniques, and procedures during design and development; leveraging materiel solutions to address architecture and specification requirement vulnerabilities; and developing new science and technology when no current solution is sufficient. A defense-in-depth cyber security approach for CPS grabs from a toolbox of existing

tactics, techniques, procedures, and materiel to greatly improve the cyber security and resiliency of the system by leveraging people, technology, operations, and intelligence. This approach requires the development of an overall risk management plan for how to implement the other steps, including leveraging secure network architectures, applying perimeter controls on devices and networks, and implementing active security monitoring. High-assurance CPS development is a design and development technique whose major components are especially relevant to intelligent operational energy systems: constrain the programming language to limit unintended behaviors, simplify the device and software interfaces to minimize potential back doors, automate the development of as much code as possible to minimize potential mistakes, perform complete system verification testing on high-risk high-reward components and functions, and institute a high-assurance culture throughout the organization. Implementing redundancy with diversity in the controls system architecture is a materiel solution that can also be implemented for intelligent operational energy systems to increase the difficulty for an adversary to affect the system. Although it is typically done with redundant physical components using differing algorithms to achieve the same function, there are efforts to implement them solely using software to minimize the size, weight, and power requirements.

As part of a defense-in-depth program, vulnerability identification and assessment processes are critical to prioritize the development and implementation of cyber vulnerability mitigation strategies and countermeasures. Red- and Blue-Teaming processes are one tool to help conduct a vulnerability assessment. A robust Blue-Teaming process would develop a comprehensive "knowledge-of-self" for the system-under-test and its mission essential functions, and a Red Team emulates a malicious actor attempting to impact mission essential functions. There are a number of technologies and systems engineering processes under development to facilitate vulnerability identification and assessment activities. Of particular note are the model-based systems security engineering approaches that would make use of cyber-physical models of intelligent operational energy systems. Using models instead of physical systems or system specifications would allow initial vulnerability assessments to keep pace with the dynamic nature of a science and technology effort. They would also enable a more rigorous approach to conducting the assessment and evaluating proposed solutions, something not easily achieved by table top exercises.

It is recommended that the Energy & Power Community of Interest and its individual researchers implement a number of steps to address potential cyber vulnerabilities in future DoD intelligent operational energy systems. Individual energy and power researchers should be involved in improving the cyber security and resiliency of their proposed intelligent operational energy systems to help protect their necessary performance as vulnerability mitigation strategies and countermeasures are incorporated. The first step is to leverage the field of high-assurance cyber-physical system development to address the most common vulnerability, improper input validation, and "design-in" a large degree of resiliency by constraining the possible behavior of the system instead of only planning for its expected behavior. The second is to implement secure controls network architectures by implementing concepts such as least privileges, network segmentation, and demilitarized zones. Third, researchers should implement as robust of activity logging capabilities as the controls system can withstand. Not only does this aid in forensics activities that improve available intelligence, but it lays the groundwork for when intrusion detection and prevention systems are capable of operating in the tactical environment. Last, individual research projects should develop, or require vendors to provide, comprehensive cyber-physical models of their operational energy systems. The models should be leveraged by maturing model-based systems security engineering capabilities to conduct rigorous cyber

vulnerability assessments and evaluate potential mitigation strategies earlier in the design process. The earlier an effort is implemented during the design process, the more cost-effective it will be.

Acknowledgments

During the research for and writing of this report, multiple cyber-physical systems and cyber security subject matter experts shared their knowledge and guidance. The author would like to thank Daniel Koller of the Office of Naval Research and Robert Timpany of the Department of Homeland Security's National Cybersecurity & Communications Integration Center for their time and insight.

Given MITRE's broad expertise in cyber security and cyber-physical systems, the author would like to thank a very wide range of people who shared their time and insight given their various expertise. In no particular order: Marie Collins, Matthew Mickelson, Joseph Ferraro, Jenny Poisson, Frank DiBonaventuro, and Frank Lynam.

Last, the author would like to than the individual MITRE technical reviewers for this report, again in no particular order: Matthew Mickelson, Nathan Edwards, John Hoyt, and Frank DiBonaventuro.

Table of Contents

List of Figures

List of Tables

This page intentionally left blank.

1 Motivation

The concepts of cyber vulnerabilities and cyber security have traditionally applied to the information technology (IT) domain. The entire class of operational technology (OT), the hardware and software that interacts with physical systems and processes, was not a concern because it was rarely, if ever, connected to the Internet and only performed basic functions. This included commonly used industrial control systems (ICS) such as programmable logic controllers (PLCs), as well as supervisory control and data acquisition (SCADA) systems [1]. However, the proliferation of intelligent digital control systems for complex physical processes has developed an entirely new class of OT where cyber security is a concern: cyber-physical systems (CPS). The NSF defines CPS as: "engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components" [2]. They are generally viewed as the combination of IT and OT systems, and Table 1-1 outlines some of the typical differences between CPS and IT. It is these differences that preclude simply adopting the cyber security technologies and methodologies developed for IT systems.

The 2015 & 2016 cyber-attacks on the Ukraine power grid illustrated that malicious cyber actors linked to foreign governments are developing sophisticated malware for compromising ICS [3, 4, 5, 6]. The 2016 incident also showed that these attacks can be automated to occur after the malware has been installed, as opposed to requiring a human-in-the-loop. This not only means that the attacks can be very widespread, but that they can be carried out on CPS not continuously connected to the Internet. In addition, researchers are finding vulnerabilities in commercial components such as solar panel power electronics [7]. This is concerning as utility companies in the United States (U.S.) that operate critical ICS infrastructure, such as the Wolf Creek Nuclear Operating Corporation, are being actively targeted by malicious cyber actors [8]. Combined, these incidents highlight that malicious foreign cyber actors have a motivation to disrupt U.S. energy and power systems and the capability to compromise the Department of Defense (DoD) operational energy systems.

In the 2016 National Defense Authorization Act (NDAA), section 1647 directed the Secretary of Defense to complete an evaluation of the cyber vulnerabilities of every major weapon system within the DoD and develop proposed mitigation strategies by the end of calendar year 2019 [9]. This has led to multiple Service-led efforts to perform cyber vulnerability assessments of legacy platforms and current missions, such as the efforts lead by the U.S. Air Force (USAF) Cyber Resiliency Office for Weapon Systems (CROWS) office (see section 9.14). While these efforts are focused on legacy DoD systems and may or may not include the operational energy sub-system as part of their scope, they illustrate the importance that the DoD has placed on the cyber security and resiliency of their capabilities and the importance the Energy & Power Community of Interest (E&P CoI) should place on them, as well. The E&P CoI is a DoD-wide coordinating body organized by the Assistant Secretary of Defense for Research & Engineering (ASD(R&E)) under the Reliance 21 program. The E&P COI helps coordinate science and technology (S&T) investments and researchers in DoD energy and power to meet Joint challenges. Fielded operational energy systems already contain significant OT with limited or no connectivity with complex data networks. However, the next generation will be intelligent operational energy systems more closely aligned with CPS, leveraging advances in available tactical computing and processing capabilities to dynamically improve their performance based on the platform, its mission, and the operational environment.

It could be argued that the cyber security of operational energy system CPS should not be considered while the underlying system science is still being developed. However, Figure 1-1 illustrates the lesson learned that considerations for cyber security (and resiliency) earlier in the lifecycle are more cost-effective [10]. It also behooves the E&P CoI to think about cyber security to help ensure that any mitigations or counter measures implemented later in the development cycle do not significantly negatively impact the performance and safety of their technologies.

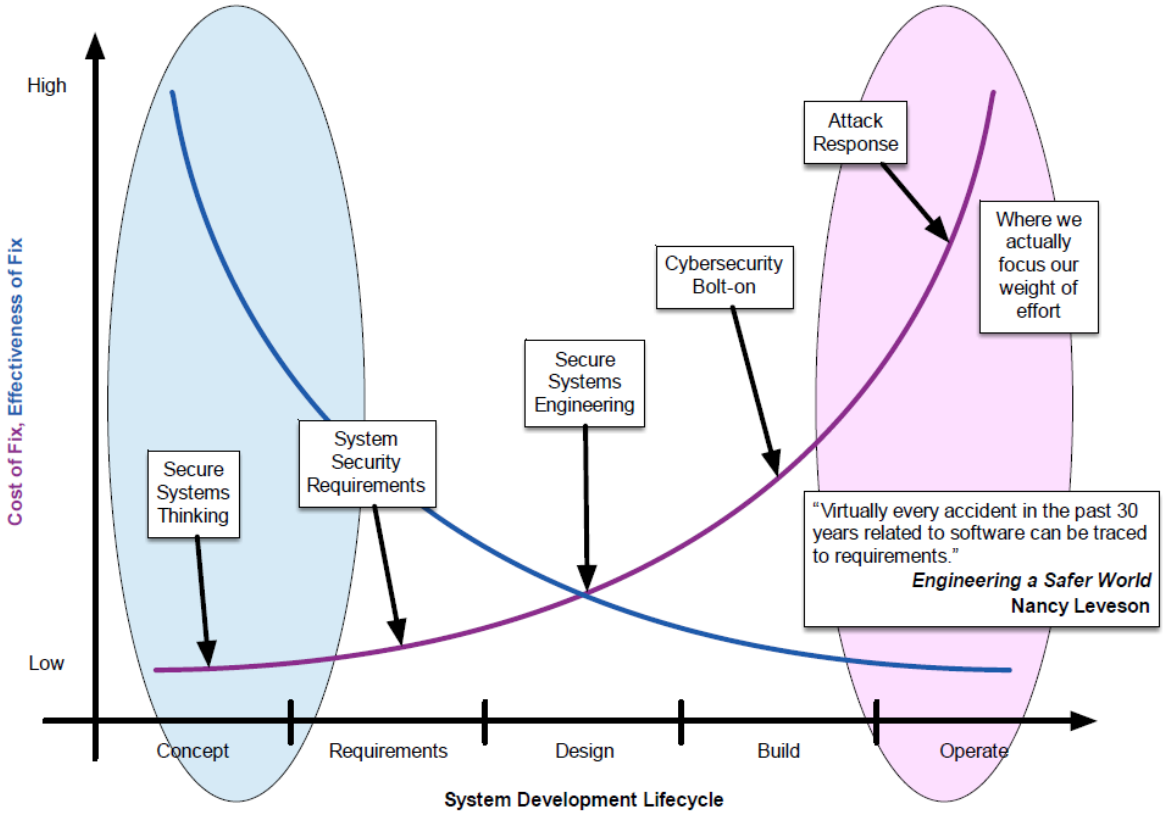

Figure 1-1 The generalized cost and effectiveness of cyber security measures when applied throughout the system development lifecycle [10].

Table 1-1 An overview of the differences between IT and CPS [11].

	IT	CPS (IT & OT)
Life Time & Refresh	3 – 5 years	10 – 30 years
Patching & Updating	Regularly Scheduled, Automated Deployments, Some Integration Testing, Reboots often required	Slow development of patches. Difficult to update, original equipment manufacturers (OEMs) often not incentivized to update, users often not qualified to make updates.
Detection / Monitoring	Enterprise systems are typically under continuous monitoring and have endpoint solution to log and alert on suspicious behavior.	Typically minimal ability to log or alert. Difficult to apply endpoint monitoring solutions.
Availability	Outages/delays are mostly acceptable	Outages/delays are less acceptable, functions are time sensitive, availability affects the health and safety of humans.
Health & Safety	The system itself (as opposed to the mission it supports) typically has no impact to the health and safety of users.	Devices and systems of devices actuate physical processes directly affecting human health and safety.
User Interfaces	Varied	Very minimal, if present.
Size, Weight, and Power (SWAP) Considerations	Systems are typically only bound by SWAP requirements of the associated datacenter.	Systems are limited to the SWAP requirements of the associated platform (e.g., elevators, vehicles, weapons, environmental controllers) in which the device resides.
Autonomy	Autonomous behavior can adapt to software function; affecting other applications/code.	Autonomous behavior can adapt to the physical world; potentially impacting health/safety of humans and requiring additional ethics considerations.
Security Controls	Implemented by technical staff. Physical security; Policy controls; often incorporating multi-factor	Typically implemented by non-professionals staff. Typically reliant on physical security.
Operational Controls	Operational controls are typically centralized.	Typically several interdependent control systems. Multiple security domains and security assumptions.

It is important to understand that every CPS, including DoD operational energy systems, will always have the highest risk vulnerability: the operators themselves [12]. Through "social engineering," malicious actors can install malware on computers or mobile devices that are then connected for control, diagnostic, or maintenance purposes to the otherwise isolated operational energy system control network. In addition, there is also the persistent insider threat and supply chain vulnerability. As a result, CPS security researchers, and this report on operational energy systems, assume that malicious actors will be able to gain access at some point. It is up to the E&P CoI and CPS security communities to ensure that mission essential functions (MEF) are both secure and resilient. Given access, it should be extremely difficult to cause significant negative impact and that the system can complete its mission successfully and quickly return to its full capability after a successful attack.

The rest of this report is organized as follows: sections 2 & 3 provide the target audience (the E&P CoI) with the necessary background on both the goals of cyber security and the most common and relevant known vulnerabilities relevant to operational energy systems. Sections 5, 6, and 7 examine the current practice in cyber security and resiliency for CPS that are relevant to generic operational energy systems described in section 4. Section 8 summarizes the recommendations for the E&P CoI's path forward to improve the cyber security and resiliency of its operational energy systems based on the research done for this report. Last, section 9 is included as a resource for the E&P CoI members and includes short summaries of the many relevant efforts and offices identified during the course of the study.

2 Introduction to Mission Assurance of Cyber-Physical Systems

The primary goal for intelligent operational energy systems is that they are able to complete their MEF. The DoD Directive 3020.40 defines Mission Assurance (MA) as "a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan" [13]. There are four possible mission states, which progress as a malicious actor achieves greater success [14]:

1. Pristine Mission: vulnerabilities are mitigated and malicious actors have not gained access to the system.
2. Exploited Mission: an adversary is able to exploit a vulnerability to gain access to the system, but has not caused any impacts on the system.
3. Attacked Mission: the system is unable to expel an attacker, who is then able to cause an impact on the system, but the mission has not failed.
4. Failed Mission: the malicious actor successfully ended the mission, and the system now attempts to recover.

The object of MA is to first prevent malicious actors from exploiting vulnerabilities by having none. Failing that, to prevent them from being able to have an actual impact on the system performance, and finally limit the consequences of any impacts they are able to have. The concepts of cyber (and cyber-physical) security are necessary tools to achieve the MA of intelligent operational energy systems as they help prevent malicious cyber actors from being able to step through the mission states and cause a failed mission. In fact, the general process for achieving MA, listed below, is very similar to that which will be described for achieving the cyber security of CPS, but with a larger scope [15]:

1. Prioritization of MEF based on the larger mission
2. Mapping of selected MEF into smaller components
3. Vulnerability assessment of selected MEF
4. Development of mitigations
5. Red-teaming to evaluate effectiveness of mitigations

Sections 3 and 5 will make clear that the goals of MA and cyber security are related: a high assurance CPS is typically cyber secure. A cyber event occurs every time an external signal modifies the flow of control data or information in an intelligent system [15]. Cyber events are not limited to databases in server stacks and internet traffic passing through your home or office router. Data passing through a standard data bus, such as the MIL-STD-1553 Avionics Bus [16], is a cyber event. Changing the settings stored in the memory of a processor for a local controller is a cyber event. In the field of IT cyber security, three primary tenets of Information Assurance (IA) are often cited: confidentiality, integrity, and availability [17]. However, system failure can result in significant safety concerns in operational energy systems. As such, the confidentiality of the data is often not a priority, coming in well behind both integrity and availability. Whether confidentiality is considered at all will be very system and mission specific.

A cyber vulnerability in a CPS arises when a flaw or weakness in the system, procedures, access controls, or implementation of cyber operations can be exploited by a malicious actor, often called a threat source, to cause impacts to physical systems and processes [18]. This may seem extremely broad, but consider the case of when detailed system specifications fall into the hands

of a malicious actor, who now has the knowledge to skirt around or defeat the designed security measures. Broader cyber security efforts, such as the one overseen by the CROWS office (see section 9.14), consider the access controls to this type of documentation for operational systems. However, document control policy is generally outside of the scope of the E&P CoI and, therefore, this report.

Across all of the aforementioned sources of CPS vulnerabilities there are three different types: ones arising from the features of the architecture, those that come from specification requirements for the system, and quite frequently many that come as a result of the actual implementation by the engineers [17]. An example vulnerability arising from a feature of the architecture would be if all of the control parameters were centralized and not stored locally due to a lack of memory at the distributed CPS. This would leave the system vulnerable to unstable operation if communication is lost between the central controller and local systems. An example vulnerability coming from a system specification requirement could be the necessity to plug unsecured personal mobile computing devices, which are more likely to be infected with malware, into tactical generators to interface with the control system. An example of a vulnerability resulting from the implementation would be if a controls developer accidentally forgot a line of code, or left in a debugging mechanism used during development, and a malicious actor was able to successfully send an above-range speed control signal to a motor.

When malicious actors successfully exploit a vulnerability they then seek to generate at least one of what are referred to as the D5 effects: disrupt, deny, degrade, destroy, and deceive (Figure 2-1). The effects are varied in terms of both the severity (degree) and the duration for the system, which combined determine the severity of the consequences to the MEF and overall mission. The "deceive" effect covers the entire range because deceptions can be designed to achieve any of the other four effects and itself can cover the entire range.

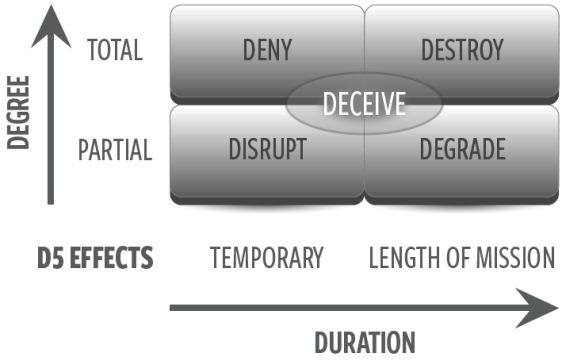

Figure 2-1 The D5 of adverse cyber effects [17].

3 Cyber Vulnerabilities of Cyber-Physical Systems

Referring back to the possible mission states discussed in section 2, different system vulnerabilities allow malicious actors to gain access (from pristine to exploited mission), have an impact (from exploited to attacked mission), and end the system's mission (from attack to failed mission). It is a challenge to answer the question of which community is responsible for mitigating which vulnerabilities throughout the development lifecycle of a complex CPS. The common assumption is that, for example, the E&P CoI should only be concerned with preventing those with inappropriate cyber access from having an impact on the operational energy system operation and causing the mission to fail. This stems from the assumption that operational energy systems are not connected to the Internet or other accessible networks, and therefore are not vulnerable to capabilities such as the Shodan search engine [19]. However, the introduction of operational energy system controls to the information networks and data buses used by the rest of the platform mission capabilities means that assumption is no longer always valid. The E&P CoI needs to concern itself with all types of vulnerabilities, from those present in a pristine mission all the way to those in a failed mission from which the system needs to recover.

During the course of this study, multiple subject matter experts (SMEs) charged with improving the cyber security of a platform or weapon system warned that an intelligent and interconnected operational energy system can be used by a malicious actor as a gateway to other mission critical and sensitive platform systems, such as secure communications or weapons systems. Imagine that an unsecure mobile device with embedded malware is used during platform maintenance to run operational energy system diagnostics. That mobile device would not normally be allowed on the same network as classified communications equipment, but the embedded malware now has access through the platform data bus. The same access could also be afforded from weaker supply chain controls on operational energy systems relative to those for the rest of the platform sub-systems. The SMEs implored the E&P CoI to consider both how to prevent those with access from impacting the mission and how to prevent malicious actors from getting access so the operational energy system cannot be used as a gateway to the rest of the systems. This is especially important as the E&P CoI needs to ensure that the technologies and methodologies used to both ensure a successful mission and prevent malicious transit through an operational energy system do not hinder performance.

The U.S. Department of Homeland Security (DHS) Control Systems Security Program (CSSP) tracks and evaluates common and relatively simple vulnerabilities for ICS as part of its mission to improve the overall cyber security of critical infrastructure [20]. These are provided as an example with the acknowledgement that they are not applicable to every intelligent operational energy system. Also, a proactive organization does not account for only known vulnerabilities, but systematically applies security and resiliency practices throughout to decrease the risk from unknown vulnerabilities, as well. In a 2010 assessment across multiple CSSP efforts, three vulnerabilities were the most common:

1. Improper ICS input validation
2. Poor ICS access controls
3. Weak user and device authentication

The first one, the improper validation of data and commands being sent to and processed by ICS, was the most common and represented over 40% of the vulnerabilities found in vendor products. The most common example is called a "buffer overflow" vulnerability, which is when data is

written to memory that exceeds its allocation and overwrites nearby data[1]. At one end the results can be simple abnormal operation, at the other are cases where an attacker embeds an entirely new program piece-by-piece. The way to best understand the potential impacts of one controller exhibiting abnormal behavior is to view the operational energy system control architecture as a hierarchy of components where each layer monitors and controls the behavior of the layer below it, relying upon models of expected behavior to do so [21]. Even simple abnormal operation can have drastic impacts on system operation as the other connected controllers and sub-systems do not recognize the behavior and can respond through abnormal behavior of their own or capability fail-safe shutdowns. Two other common forms of improper input validation are the lack of bounds checking on an input (e.g., accessing an array beyond its size and receiving a nonsensical value, or accepting a negative value integer command which has no physical meaning for the controlled sub-system), and providing remote users the ability to inject unintended commands [20]. The Aurora test conducted by DHS at Idaho National Laboratory (INL) is a very common example of the potential impacts of improper input validation: a grid-connected generator can be destroyed by altering its settings outside of the bounds for grid-connected operation [22].

The second most frequent vulnerability, improper access controls, can be summarized by a single coding concept: least privileges [20]. The least privileges concept is the premise that users and control systems should only be able to do what they need to do, view what they need to see, and nothing else. This helps prevent a malicious actor or code that has access to a single control system from extending its reach much further. For an operational energy system on a platform, the analog would be ensuring that a local device controller not have unnecessary access to other mission critical systems (e.g., secure communications) or data not related to its mission. The operational energy system controller should be provided with the minimum access necessary to ensure its own operation and nothing more. Privilege escalation is what happens if a malicious actor or program gains access to a controller or process with higher privileges than it currently has, gaining the use of those higher privileges. Often ICS services are started with root user permissions, the highest possible, even when not necessary; it is often done because of the extra effort required to set up the appropriate hierarchy of privilege levels. This type of oversight should be prevented for intelligent operational energy system controls networks.

The third most frequent vulnerability, weak user and device authentication, can completely nullify any efforts to limit access through the least privileges concept [20]. Essentially, it is up to the developer to ensure that each device, process, or service with any sort of access control is set up to properly validate those requesting access. A common practice is to have the "client," whether that is a user interface or an overarching controller, perform its own authentication and the device controller assumes that any commands or queries coming from that controller are valid. However, this can be easily manipulated by intercepting the communications stream. Each individual device controller needs to be able to perform its own, concurrent, authentication. Authentication on both ends of a communication channel can help prevent man-in-the-middle attacks, where data and messages are inappropriately re-routed for monitoring and manipulation.

It is worth mentioning briefly here the potential risk that an intelligent and integrated operational energy system can pose to secure communication and processing systems. Adversaries could leverage power line modulation caused by electromagnetic radiation emitted by connected

[1] Common Weakness Enumeration (CWE) numbers are assigned by DHS NCCIC to validated vulnerabilities. The stack-based buffer overflow is CWE-121 and the the heap-based buffer overflow is CWE-122. Improper input validation is CWE-20. CWE and other similar catalogs are used during system vulnerability identification and assessment efforts, which are discussed in more detail in section 7.

electronic systems, a phenomenon sometimes referred to as TEMPEST [23]. An adversary could theoretically hijack cryptographic keys by monitoring the modulations in an insufficiently shielded interconnected electric power system to then monitor sensitive communications, among other activities. The U.S. National Security Agency (NSA) maintains a TEMPEST Certification Program that can be leveraged, when necessary, to ensure operational energy systems do not introduce this vulnerability to connected mission systems [24].

4 Generic Operational Energy Systems

Three generalized system schematics of the next generation of intelligent operational energy systems were developed to illustrate the cyber vulnerabilities of their CPS: energy optimized platforms (EOP), tactical microgrids (TMG), and dismounted Soldiers (SDR). The following sections describe each of the generalized systems and should be kept in mind when reading the rest of this report.

4.1 Energy Optimized Platforms (EOP)

The EOP generalized system shown in Figure 4-1 is meant to be applicable to intelligent air, ground, and sea platforms with integrated power, energy, and thermal systems that have an over-arching energy management system (EMS). The propulsion and/or prime mover, along with its electronic control unit (ECU), can be integrated with the EMS. While shown in the high level schematic, the propulsion and prime power systems are not considered in the present report as they are not within the scope of the E&P CoI and instead are binned with the Air Platforms or Ground & Sea Platforms CoIs. The EOP schematic is the recognition that across many of these platforms there is an electric generator to provide an electric power bus, a thermal management system (TMS) that runs throughout the platform, and a supplemental energy storage system with a separate battery management system (BMS). Due to the large variety of potential loads connected to the electrical, thermal, and data circuits for the EOP they are not considered in detail in this analysis. The EOP schematic would need to be heavily modified, by design, to be used to assess the cyber vulnerabilities of a specific platform.

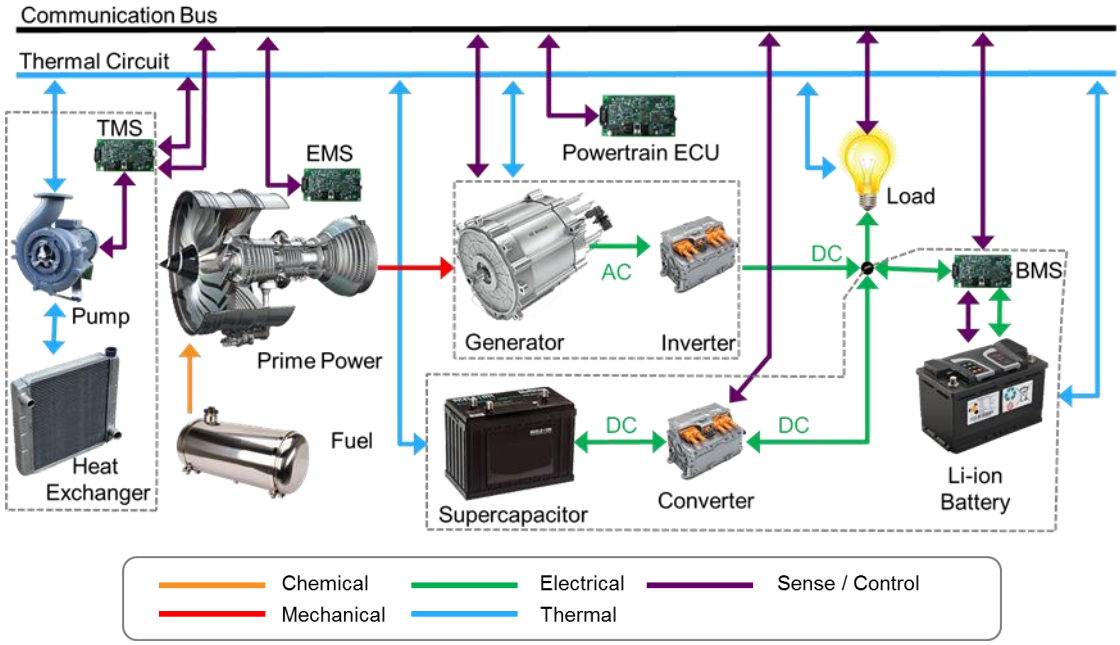

Figure 4-1 Schematic of the cyber-physical relationships of a generalized energy optimized platform.

4.2 Tactical Microgrids (TMG)

The generalized TMG shown in Figure 4-2 illustrates typical possible components, however with the acknowledgement that TMGs are highly variable in practice based on the unique characteristics of the situation at hand (or mission, enemy, terrain, troops available, time, and civilian considerations, METT-TC). Large TMG designs can consist of multiple connected intelligent power distribution (IPD) units that allow for the sharing of power from non-local sources for local loads throughout the network. The power sources attached to the IPDs can be standard combustion engine and electric generator combinations (GenSets), distributed energy resources such as battery energy storage or photovoltaic panels, or even hybrid-electric or electric vehicles in a vehicle-to-grid configuration. Vehicle-to-grid systems are already partially covered by the combination of the diagram in section 4.1**Error! Reference source not found.** a nd by the GenSets presented here. Also, loads were simplified into two categories due to the large variety that can be attached to a TMG, with "Smart Loads" denoting those that have digital control mechanisms that can communicate with the TMG's IPDs.

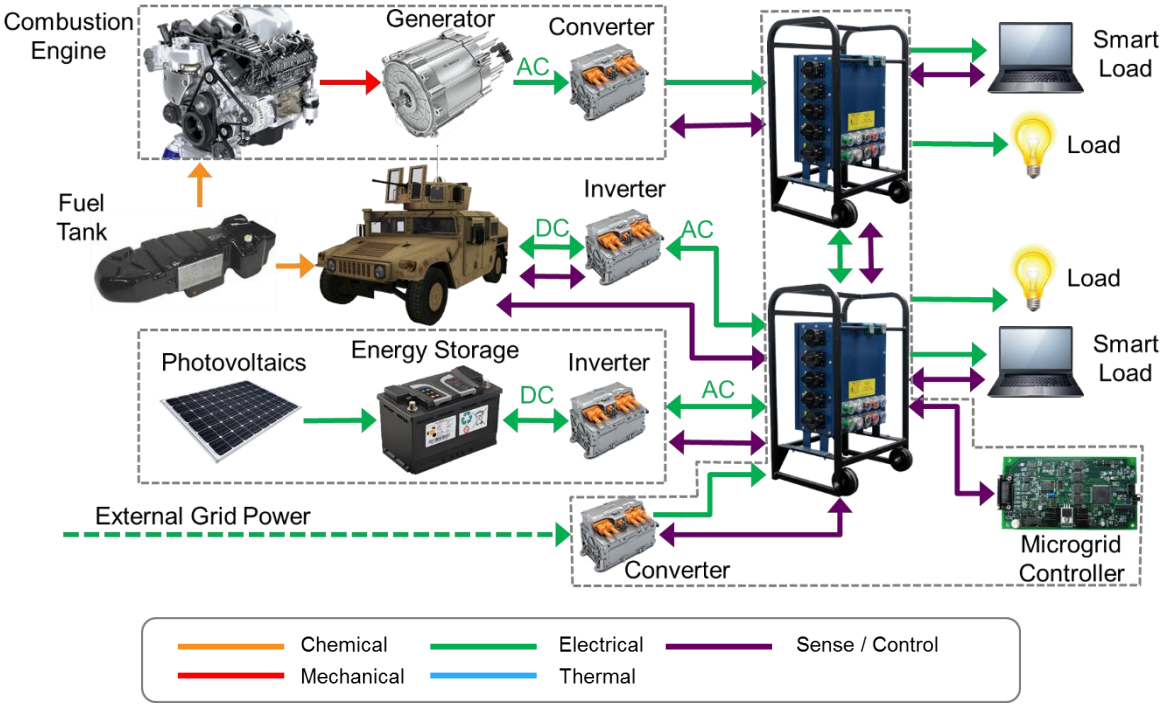

Figure 4-2 Schematic of the cyber-physical relationships of a generalized tactical microgrid.

4.3 Dismounted Soldiers (SDR)

The generalized Dismounted Soldier (SDR) cyber-physical schematic shown in Figure 4-3 is based on a Soldier power and data manager designed to allow distributed Soldier equipment to draw power from centralized conformal wearable batteries (CWB), decreasing the number of disparate spare batteries a Soldier needs to carry with the goal of reducing the overall load due to batteries. The primary power consumption is from the Soldier radios. Other common components are loads such as hand-held GPS receivers used for positioning, navigation, and timing (PNT), the mobile device that serves as a user interface and command and control (C2) device, and any alternative energy sources such as packable photovoltaic power systems.

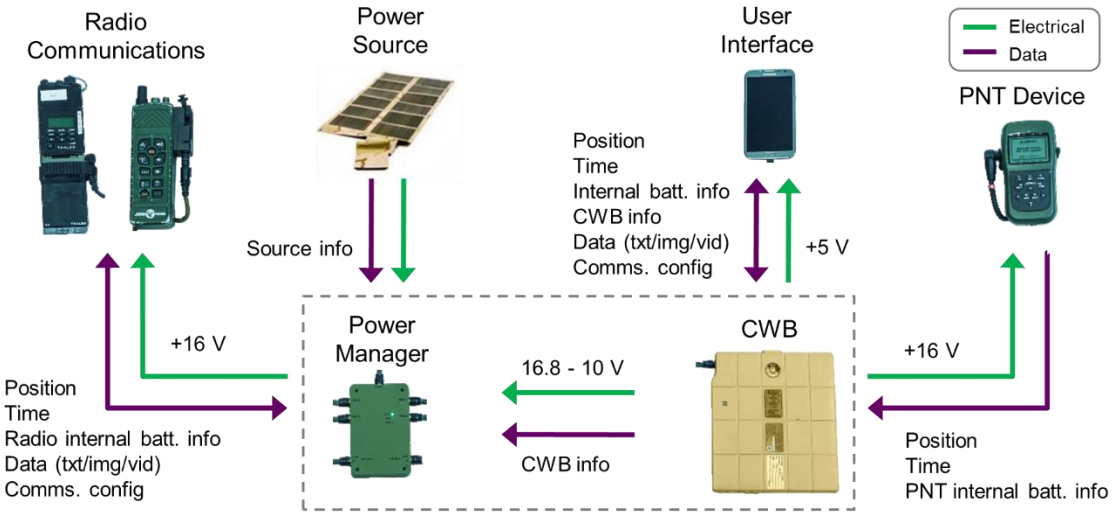

Figure 4-3 Schematic of the cyber-physical relationships of a generalized dismounted Soldier equipment set.

5 Common Approaches for Cyber Security

This section is not intended to be a comprehensive accounting of all cyber security approaches, but a selection of those considered most applicable to intelligent operational energy systems and the cyber vulnerabilities of their CPS. There are three types of vulnerability mitigations or countermeasures discussed in the rest of this section. Tactics, techniques, and procedures (TTP) are generally the least costly and can be used to address many implementation vulnerabilities; materiel solutions are, however, frequently the only option for addressing architecture and specification vulnerabilities; the last resort is the development of new S&T when TTP and materiel solutions are insufficient [17].

5.1 Defense-in-Depth

The Defense-in-Depth Cyber Security approach is one that focuses around the acknowledgement that there is no single "silver bullet" in any of the techniques discussed in this report that will stop all adversaries from exploiting all vulnerabilities in a CPS [25]. It is referenced by a number of related, completed or ongoing efforts, such as the Sandia Microgrid Cyber Security Architecture stemming from the Smart Power Infrastructure Demonstration for Energy Reliability and Security Joint Capability Technology Demonstration (SPIDERS JCTD) (see section 9.1) and the OSD-funded Tactical Microgrid Standards Consortium (TMSC) (see section 9.2). It is also mentioned by the U.S. Army Tank Automotive Research, Development, and Engineering Center (TARDEC) as a near-term goal for its open system vehicle architectures [26]. The end goal can be summarized as leveraging a combination of people, technology, operations, and intelligence to increase the cost to an adversary of exploiting a vulnerability while simultaneously improving the ability to detect an intrusion and actively defend the system from it [25]. The over-arching principles can be summarized as layered defenses in multiple places, with strength appropriate to the asset risk, robust access management and encryption, and intrusion detection, analysis, and response [27]. The main elements of the strategy are:

1. Having an overall risk management program for the mission or capability,
2. Developing a specific resilient cybersecurity architecture,
3. Taking measures to ensure the physical security of the components,
4. Leveraging secure network architecture techniques,
5. Applying proper network perimeter security controls and access privileges,
6. Managing the security of individual controllers and device operating systems,
7. Performing active security monitoring,
8. Properly managing outside vendor relationships,
9. And implementing the policies, procedures, and training to manage the human element [25].

Given the breadth of the activities, it is clear that no one organization would be charged with executing all individual components, particularly when considering the DoD's operational energy systems. The USAF CROWS office (see section 9.14) is an example of an organization highly focused on implementing #1, an overall risk management strategy for weapon system missions, and using that role to help other organizations executing the other functions. The

TMSC effort (see section 9.2) is an example of using collaboratively developed standards to define a secure controls network architecture and perimeter with Industry partners and vendors.

The following sections give more detailed descriptions of some of the Defense-in-Depth elements that are of key importance for the E&P CoI.

5.1.1 Risk Management Program

The first step that any organization needs to take toward improving the cyber security of their systems is to develop an end-to-end risk management program, such as the effort coordinated out of the USAF CROWS office. The purpose of the risk management program is to understand the specific risks posed by their potentially vulnerable systems toward completing their specific missions and then setting up the programs and processes to address the other elements of the Defense-in-Depth strategy [25].

The E&P CoI is concerned with what cyber-physical security measures they should be implementing on their next generation of intelligent, integrated power and thermal networks, such as the ones discussed in section 4. The focus of the E&P CoI for this element of the overall Defense-in-Depth strategy should be on performing the asset characterization and risk assessments for the systems under development. Ideally, the risk assessment steps would occur in collaboration with the future asset owner and operator communities to bring their perspectives on how the fielded system would need to operate in both normal and abnormal situations. The risk assessment step would also commonly be performed using intelligence on adversary motives and capabilities. However, these assessments would likely need to occur in a manner that assumes adversary intent and the resources to exploit a vulnerability given that the E&P CoI is developing unique capabilities that have few-to-no currently fielded analogs to reference threat data.

The cyber-attack risk assessment process is a very challenging, but important process that is also an active systems engineering research field. A more thorough discussion of what steps the E&P CoI can take are in section 7.

5.1.2 Network Architecture & Perimeter Security

The second most common type of CPS vulnerability is the lack of strong and proper access controls to its settings and controlled processes (see section 3). When configuring large-scale ICS, the DHS National Cybersecurity and Communications Integration Center (NCCIC) (see section 9.18) has a recommended secure network architecture that divides the IT and OT into six different levels [25]. The goal of their architecture is to prevent a malicious cyber actor from being able to travel within the system after successfully exploiting one component of it. Leveraging an architecture design that prevents malicious actors from easily spreading throughout and between networked systems can help to mitigate individual CPS that do not have strong and proper access controls. DoD intelligent operational energy systems do not possess the same wide area connectivity and may have varying configurations of the middle levels based on the specific application (e.g., an EOP, TMB, or SDR architecture from section 4). Figure 5-1 is a notional and generalized adaptation of the recommended NCCIC architecture for an intelligent operational energy system. The instrument level, level 0, is where the baseline CPS components are, specifically the sensors that monitor the physical processes plus the actuators that are used to control them. The device level, level 1, houses the electric generator, TMS, or BMS, etc. The system level, level 2, represents the overarching operational energy system controller for the EOP or entire TMG, or the EMS. In an ICS network architecture, the site operations and control

level is level 3 and houses applications, databases, activity logging (a.k.a., historian), etc. In an intelligent operational energy system, those functions would likely be placed in level 2. Also, although not shown here due to space considerations, more than one device is controlled by the system controller, and the blocks shown in Figure 5-1 for levels 0 and 1 could be repeated any number of times.

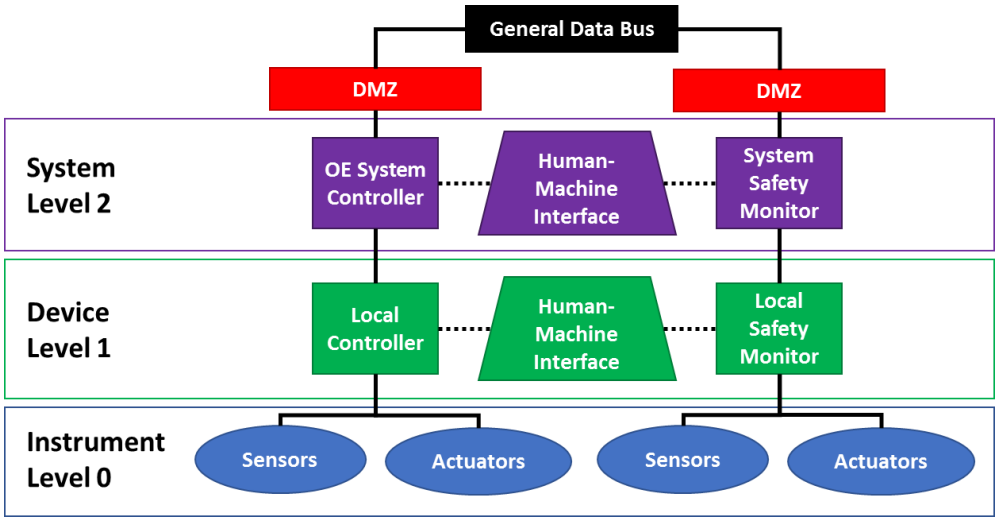

Figure 5-1 A notional and generalized adaptation of the DHS NCCIC recommended ICS Secure Network Architecture for DoD operational energy systems.

The controls network architecture shown in Figure 5-1 is intended to leverage a diverse set of secure design recommendations. The first is network communications and software segmentation. The software development best practices put forward by RTCA, Inc. as part of its guidelines for commercial aerospace software flight safety certification (see section 9.17) describe how the different software functions, when partitioned, should not be able to contaminate another function's code or data and, when they fail, have no adverse impacts on another software function (i.e., no common-mode vulnerabilities). The Sandia Microgrid Cyber Security Architecture (see section 9.1) applies the concept of controls network segmentation by enclaves and functional domains. The enclaves refer to a grouping of systems where all the devices across the systems in an enclave are trusted and communication is generally unrestricted. The functional domains allow for controlled communications between the enclaves for specific purposes. The two concepts can be applied to DoD intelligent operational energy systems by ensuring that the various controllers cannot make fundamental changes to each other's coded operation, that the system controllers can only change specified local controller parameters within pre-determined bounds, and that the communications and control messages of different system functions (e.g., thermal management vs. electrical energy storage) are isolated to operate independently outside of the overall system controller's internal decisions relating the two.

There are a couple of pathways toward enforcing the network segmentation and software partitioning design. Prescriptive whitelisting is when the network or software has a communications traffic monitoring capability and a database of which devices or software functions are allowed to communicate, and how [25, 27]. Prescriptive application whitelisting is a version that is similar to the functional domains concept mentioned previously, where all commands and data traffic for a specific system function are monitored and those that do not fit the definitions database are prevented from moving on to their destination. However, this approach presents significant safety concerns as the monitor might block a necessary command

missed during the development of the database [28]. This concern has depressed demand for this type of capability from ICS vendors, who generally are not providing prescriptive application whitelisting capabilities [29]. The risk can be minimized if it is possible to build up the definitions database over a very long period of time across a very wide array of representative platform actions, and the devices within the operational energy system are relatively set (i.e., not a TMG as they are inherently variable).

Prescriptive network whitelisting is another method of segmentation or partitioning that NCCIC recommends be implemented, specifically by utilizing what they term demilitarized zones (DMZ) between segments of the network [25]. Their work leads them to recommend using multiple DMZs to isolate specific network functions and capabilities, as it has thus far proven effective at increasing the cyber security of large architectures. A DMZ typically separates the enterprise IT from the OT on a traditional ICS architecture. The DMZ can be summarized as both a physical and cyber sub-network where shared resources can be placed so both the IT and OT networks can access them, but without having to direct access each other. Firewalls are used to set up and maintain the DMZ, specifying the allowed traffic between the IT and OT zones.

Multiple DMZs can be used by an intelligent operational energy system to isolate it from the rest of the mission capabilities on a platform or at a mobile operating base, etc. All of the operational energy system controls would be contained within a network area protected by DMZs. This addresses the risk that a necessary safety command might be inadvertently blocked because communication traffic within the DMZ is not actively hindered. This also addresses a common concern held by those tasked with the overall platform cyber security: the ability of an adversary to exploit the operational energy system and gain access to other platform subsystems. Setting up DMZs to contain any databases or services that are needed by the operational energy system and another platform sub-system will allow system designers to restrict the commands and data that are able to pass back-and-forth between them, hampering a malicious cyber actor's ability to travel within the platform. One challenge with applying DMZs to an operational energy system is that the platform's general data bus might be the only physical method for communication between different components, especially in legacy platforms with strict SWaP constraints. This makes network segmentation especially challenging. Virtual local area networks (VLAN) are one option for setting up software-only DMZs if the data bus can support them, or be retrofitted to support one. Multiple government agencies have been funding efforts for more than five years to develop software-defined networking (SDN) capabilities for use with CPS, enabling the dynamic rerouting of traffic around breaks plus network whitelisting without a separate physical network [30]. However, new systems and platforms should look very closely at what networking hardware would be necessary to install both physical and cyber DMZs between its integrated power, propulsion, and thermal systems and the rest of the platform sub-systems. This is because VLANs and likely other software-based networking methods have multiple known vulnerabilities a malicious actor could exploit [25].

One last aspect that bears mentioning in Figure 5-1 is the presence of an isolated set of safety monitoring and controls devices operating in parallel to the energy monitoring and controls devices. Setting up separate, and isolated safety monitoring and protection systems, either software, hardware, or both, is another best practice advised by RTCA for commercial aerospace software-systems [31] and is expected to become another recommended best practice for ICS by DHS NCCIC [29]. This makes it very difficult for a malicious cyber actor who has access to the operational energy controls network to cause catastrophic damage to the system or platform as the separate safety systems will effectively limit them to significantly lower consequence attack effects. A separate and isolated safety monitoring system could mean the difference between a

generator failing completely or just running at an inefficient level and burning more fuel than necessary.

The network architecture cyber security concepts discussed in this section, such as controls network segmentation and DMZs, need to be considered whenever the DoD S&T Community develops open architecture standards for its mobile systems. The TMSC effort (see section 9.2) has a cyber security effort that leverages segmentation and DMZs for its controls network architecture. However, the other major open architecture definition efforts reviewed did not have as much of an emphasis on cyber security. The VICTORY effort (see section 9.13) is reportedly closely following the LOSA effort (see section 9.7), however the LOSA effort did not appear to have a significant emphasis on cyber security, itself. The robot operating system (ROS) effort (see section 9.8), an open systems architecture for unmanned systems, is in the process of developing cyber security tools that can be incorporated as desired and, when released, should be evaluated for potential adoption to operational energy systems.

5.1.3 Continuous, or Security Monitoring

Security monitoring, also referred to as continuous monitoring, is a critical component of a full defense-in-depth strategy, and the capabilities within CPS are very immature [25], with a lot of ongoing research activity and academically-affiliated spin-off companies leading its commercial application. Intrusion prevention systems (IPS) actively prevent activity that is deemed to be malicious or potentially harmful. There is a significant risk that autonomous decision-making capabilities will inappropriately stop a control function (referred to as a false positive), that is necessary for the safe and successful operation of the system. This is similar to the risk posed by prescriptive application whitelisting discussed in section 5.1.2): any false positives could lead to unintended catastrophic consequences. Intrusion detection systems (IDS), however, are passive: a user or system administrator is notified when malicious or potentially harmful activity is detected, but IDS do not actively work to prevent the activity.

DoD operational energy systems are deployed and used in chaotic and unpredictable tactical environments with significant human control and interaction. This increases the challenge of implementing robust anomaly detection and therefore the risk of false positives discussed above. The DoD operational energy community should not consider anomaly-based IDS a potential cyber security technology at least until the specific technology has been successfully applied to utility electric power microgrids, which are stationary and involve significantly fewer human decisions and interactions. Any IPS capability should not be considered until an IDS relying on the same detection capabilities has been successfully fielded and demonstrated an acceptably low false positive rate. With that in mind, the rest of this section describes some of the ongoing work in both IDS and IPS.

The Defense Advanced Research Projects Agency (DARPA) Rapid Attack Detection Isolation & Characterization Systems (RADICS) program (see section 9.6) aims to develop the technology needed to realize the full potential of IPS. The envisioned capabilities would allow the software-based monitoring systems to detect anomalous cyber activity, including in CPS, identify whether it is malicious or not, and even reconfigure the network to isolate the intrusion while maintaining as much system operational capability as possible. The National Rural Electric Cooperative Association (NRECA) is one of the performers on the DARPA RADICS program. Previously, NRECA had developed its *Essence* prototype to demonstrate the potential benefits of its "reactive" approach to cyber security for microgrids: discovering malicious activity and then automatically isolating the affected systems while modifying the agile microgrid architecture to

accommodate for their temporary loss (see section 9.3). Their technology relies upon the development of what they term the common grid state database (CGSD), allowing artificial intelligence and machine learning algorithms to compare potential anomalous activity against the CGSD baseline. Also, Argonne National Laboratory is leading efforts as part of the Department of Energy (DOE) Cybersecurity for Energy Delivery Systems (CEDS) research and development program to develop what is being called an attack-resilient, wide-area monitoring, protection, and control (WAMPAC) framework [32]. It leverages models of CPS properties for anomaly detection algorithms as part of a framework that also features a self-healing CPS controls network with moving target defense protection.

As noted from the utility grid examples above, there are two general approaches that can be leveraged, even concurrently, to develop the energy network behavior baseline: using historical data or developing models. However, developing a historical baseline of control network activity would require the operational energy system to have already been fielded for a significant period of time and have a defined and limited set of possible behaviors. The Anomaly Detection for Cyber-Physical Systems (ADCPS) effort (see section 9.19) seeks to address that limitation: the first couple of technical tasks are to develop open-systems models and data for power and energy devices to enable model-based anomaly detection for CPS. There is also the Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA) effort led by Georgia Institute of Technology, which aims to develop faster than real-time power grid modeling to allow for anomaly detection using dynamic state estimation [33]. Theoretically, this would allow a CPS monitoring capability to identify instances where the power and energy device behavior does not match with its control parameters or environmental conditions. This would not require prior field data for the specific operating conditions or environment, simply a validated model that applies to the situation. This approach would also help identify spoofing attacks where the controller or user is made to see incorrect data on system performance, leading to incorrect and potentially disastrous decisions.

Signature-based detection is another method of security monitoring that follows a different fundamental principle from the anomaly detection based method discussed above and would be better able to perform in chaotic and unpredictable tactical environments [25]. However, it relies upon frequently updated signature definition files and so might not be effective for operational energy systems, which are highly mobile. It can be used with both IPS and IDS but focuses on detecting known patterns of malicious activity. The signature database can be informed using known attacks on traditional ICS systems plus any data available from the logging activities of fielded intelligent operational energy systems that track “who made what changes and when.” The signatures database of fielded devices using signature-based IPS or IDS would need to be frequently updated to maintain its ability to detect the latest attack strategies, which may preclude the use of signature-based detection on systems that would not be able to easily receive these updates (i.e., most DoD operational energy systems).

Another challenge with implementing security monitoring on operational energy systems is the level of logging and data capture infrastructure necessary to develop a sufficient technical baseline similar to a CGSD. Although there is typically some form of logging capability built into the system, SWaP constraints might preclude expanding those to what is necessary for security monitoring. A related challenge is that the monitoring point may not have introspection into the other segments of an operational energy system (i.e., it lacks visibility upward, downward, or laterally). As the operational energy community is waiting for the maturation of IDS in the fixed electric grid environment, a simple first step would be expanding any existing operational energy device performance logging to include tracking of “who made what changes

and when" for all system, network, and device cyber and cyber-physical systems to assist with post-incident forensics. The type of tracked changes would include firmware updates, parameter and settings modifications, command signals, and data requests.

5.2 High-Assurance Design Practices

The most commonly reported or discovered vulnerabilities in CPS relate to input and command validation by the individual device (see section 3). These vulnerabilities typically arise when the controls are developed in a less-than-rigorous manner and can be avoided if the programmer makes a point to avoid them. The concept of high assurance CPS system design for cyber security aims to provide MA by minimizing the number of ways that any actor (malicious or otherwise) can cause the system to behave in ways other than as designed by targeting these easily avoidable vulnerabilities. It stems from high assurance design practices for software used in critical applications, such as in aviation, nuclear reactors, and space systems [31, 34]. In those applications, the primary concern is for the controls software to be incapable of existing in states that present significant safety concerns for the operators or the system. Wherever possible, applying the concept of high assurance design to operational energy systems would significantly increase their overall safety while having the added benefit of making it extremely difficult for a malicious actor with access to cause catastrophic damage to the system or mission.

The DARPA High-Assurance Cyber Military Systems (HACMS) project (see section 9.4) aimed to build the software development technologies that would make it significantly easier to deploy high assurance military system software, such as for unmanned systems and platform control systems. Although the operating system and controls synthesis and verification tools are still immature, there are a number of secure code compilers already available that should be explored. A researcher with one of the performers for the HACMS project recently published an adaptation of high-assurance design practices to CPS [35]. The author provided five general "hints," with the acknowledgement that there are exceptions:

1. Constrain the programming language,
2. Simple interfaces are secure interfaces,
3. Automate the glue code and architecture development,
4. System verification is a probabilistic game, and
5. High-assurance systems require a high-assurance culture.

A constrained programming language is often referred to as Turing-incomplete or even "weak," in that Turing-complete languages allow for functions to exhibit seemingly arbitrary behavior with unlimited memory resources if the developer is not careful to properly limit the function. Implementing the final controls in a Turing-incomplete language increases the assurance that the software will only behave as originally intended. It is also mathematically feasible to automate the verification of the software function when using a Turing-incomplete language, something that is very complex for Turing-complete languages. This helps lessen the burden of accuracy and completeness (i.e., addressing every possible coding contingency) on the developer. One example is the Ada programming language and the accompanying GNAT Compiler [36, 37]. There are also a number of secure code compilers available that allow initial development in a more powerful language but final implementation in a Turing-incomplete language.

The HACMS performer [35] also noted that the interfaces between different software components could present significant vulnerabilities due to added complexities in the ways that

two components could interact. These complexities could take the form of ill-defined or "catch-all" messages commonly used during debugging, artificial and assumed limits placed on data and messages sizes, or even the ability to remotely reset the system by overwriting its memory (i.e., a manual factory reset button or sequence). These features could easily be exploited by malicious actors, if discovered, to circumvent installed security mechanisms and cause unexpected system behaviors. Taking care to limit the interfaces between different components to only the bare minimum necessary for full and safe functionality will help prevent the unintentional insertion of interface vulnerabilities. Automating the development of as much of the architecture as possible is another method to help keep the interfaces simple: setting up scripts to generate new instances of interfaces and other components will help ensure they are not only operating in the intended manner but that they do not have any simple errors that could lead to significant vulnerabilities. Another example is to automate the memory allocation functions, which would also potentially reduce the risk posed by the simple, yet common, buffer stack overflow vulnerability mentioned in section 3 [38].

Once the control software is developed, it needs to be verified for its operation and safety. However, it can be very costly and time consuming to verify every individual line of code throughout the entire system, even when using automated software assurance tools such as Coverity, and HP Fortify [39, 40]. The result is a trade-off between focusing on protecting critical components and functions or spreading out the verification effort across the entire system. A common framework used by software developers to categorize the level of verification effort applied to individual components and functions is called the Common Criterial Evaluation Assurance levels [41]. The different levels are:

1. Functionally tested
2. Structurally tested
3. Methodically tested and checked
4. Methodically designed, tested, and reviewed
5. Semi-formally designed and tested
6. Semi-formally verified design and tested
7. Formally verified design and tested

For example, a very critical component can be assigned to be formally verified and tested, but non-critical components just functionally tested. The Carnegie Mellon University Software Engineering Institute (CMU SEI), a Federally Funded Research and Development Center (FFDC), offers technical CPS validation and testing support while conducting research to improve CPS validation and testing capabilities [42][2]. The HACMS research [35] provides these hints: focus on the foundation and use a high-assurance operating system for controllers, emphasize secure interfaces, follow best practices for software development, and develop mitigations for the high-probability-of-exploit vulnerabilities (e.g., buffer-stack overflow and input validation) first and foremost. The RTCA's guidance for commercial aviation software development to pass flight safety certification requirements includes a set of verification and

[2] The CMU SEI is also a source for more information on the latest work in software development processes [101].

testing requirements [31][3]. The document helps the developer determine which level of rigor needs to be applied based on the criticality and the impact of each individual function, device, and software component as well as their interactions from a system-of-systems perspective. This type of document, if adopted by the DoD's operational energy acquisition community, can help ensure that individual vendors are all delivering the same level of cyber security and safety protections in their operational energy system controls software.

The last hint from the HACMS research [35] is perhaps the most challenging: developing a high-assurance culture and processes within the organizations charged with the development and acquisition of cyber-physical systems. This is the acknowledgement that many system vulnerabilities are the result of mistakes during development as opposed to design flaws. The current accepted guidance for instilling a high-assurance culture, whether to prevent accidents or improve cyber security, is a summary of the approach taken by the Navy submarine safety program and captured in the NASA/Navy Benchmarking Exchange, Volume 2 progress report [34]. Table 5-1 lists a set of selected best practices from the report that could be applicable to the DoD's operational energy community; many of the practices are not specific to the E&P CoI but necessarily include the acquisition community, as well.

Table 5-1 Selected best practices observed within the Navy's submarine safety program for instilling a high-assurance culture for system design and development [34].

Personnel	Flat organizations with quick and assured access to leadership
	"Freedom to Dissent" is a primary element; managers are responsible for finding dissenting opinions
	Highly trained and qualified people are held personally accountable for safety/security
	Recurrent training based on latest outside experiences
Design & Requirements	Safety, security, and quality processes embedded within all pipeline organizations so that related goals are mainstreamed
	There is not a stand-alone document for safety criteria or requirements, which are instead embedded in all technical requirements and documents
	Separate safety and security analysis organization/section that reports directly to leadership with an independent and equal voice in design and operational decisions (but no responsibility for product safety, itself; that remains with the engineering organization)
	A heavy emphasis is placed on operational human factors and interface design as a pathway to ensure safety and security, with heavy involvement from operational user community, to prevent user mistakes/errors
	Recognition that there is no "Silver Bullet" tool or technique and an "all-of-the-above" approach is absolutely necessary

[3] The RTCA commercial aviation software development guidance documentation also contains a set of best practices on how to manage parameter data items, instances of user-modifiable or option-selectable software, and even a device's ability to accept field-loadable software [31].

	Maintaining a slate of experts in specific technical areas that can be consulted by design engineers in different organizations
Oversight & Auditing	Rigorous change control ensuring recommended changes are reviewed by all appropriate stakeholders from system, component, and support technical managers in addition to the program manager
	Strong headquarters oversight of problems plus having a corrective action system in place to encourage dealing with small problems before they become larger ones warranting leadership attention
	Audit teams include the technical requirements owner, themselves, to compare results against their intentions
	Embedded closed-loop lessons learned process that institutionalizes built-up knowledge

A follow-on program to HACMS is the DARPA Cyber Assured Systems Engineering (CASE) program, first announced in May 2017 (see section 9.5). It aims to achieve systems engineering breakthroughs to better enable complex embedded systems design and acquisition processes to "design-in" system cyber resiliency. Put another way, CASE aims to facilitate the application of the high assurance design technologies researched during the HACMS program and should be monitored by those tasked with ensuring the cyber security and resiliency of operational energy systems.

5.3 Redundancy with Diversity

Another resilient system development best practice recommended in RTCA's guide for developing commercial aviation software to obtain flight safety certification is called multiple-version dissimilar software, essentially applying the concept of redundancy with diversity [31]. This concept is based on NASA's 1990 N-version programming experiment, with the recommendation to have multiple pieces of code developed, and even fielded, that use differing approaches to execute the same function [43]. Differences between the output of the two approaches will help identify potential errors and mistakes during testing. Also, a failure mode contained in one of the approaches might not impact the other approach(es), allowing for continued safe operation. The concept of multi-version programming helps solve the byzantine fault[4] challenge, but it needs another secure mechanism to reach operational consensus between the non-failed software modules. Applying these concepts to cyber security, not just safety and mission assurance, would greatly increase the difficult for a malicious actor to be able to exploit cyber access and cause negative consequences to the system or mission.

The "Fly-By-Wire" avionics architecture illustrates how this concept can be implemented in CPS [44]. Figure 5-2 illustrates the general characteristics of the architecture: there are three electrically and physically isolated primary flight computers, with each one sending its messages to only one of the isolated communications channels but receiving and deconflicting messages from all three. Each flight computer has three dissimilar (hardware and software) processing lanes, each with its own power supply and connection to each of the three communications

[4] A Byzantine Failure is when one computing system communicates conflicting information to other computing systems and can occur due to hardware failure, software bugs, architecture limitations, and malicious attacks [17].

channels. This configuration allows for error and fault checking both during development and real-time across different computers, their lanes, and the different communications channels. With the proper design, such as having different communication keys or even different protocols for the different channels, it would require a malicious actor to potentially exploit all three to be able to take control of the system and send out malicious command signals and messages.

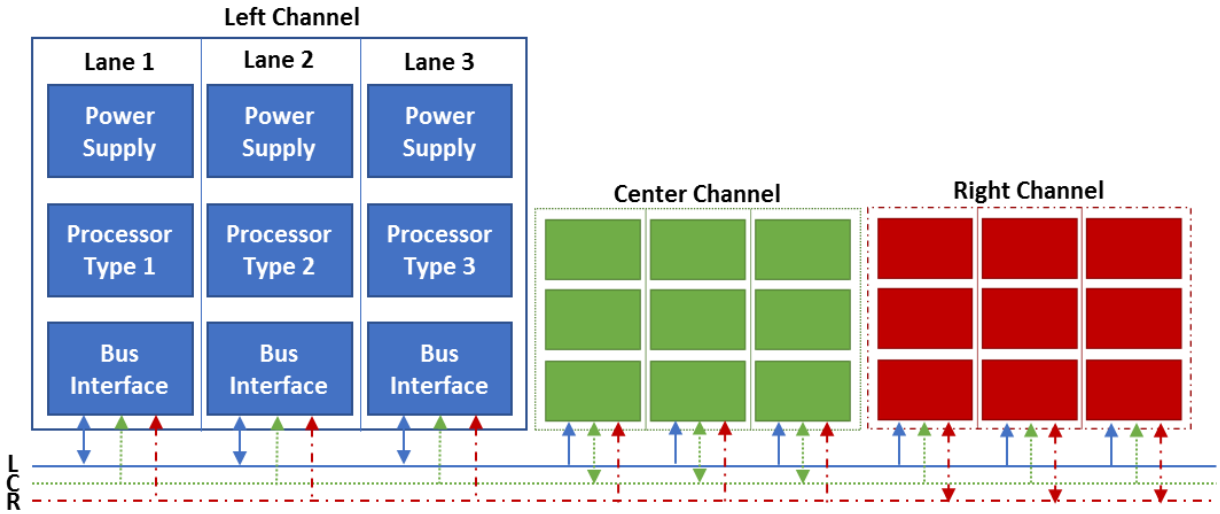

Figure 5-2 A general schematic of a flight controls architecture [29].

The RHIMES FNC is developing complementary technologies to leverage redundancy with diversity technologies in the individual controllers (see section 9.9) [45]. The approach, at its base, uses multiple dissimilar controllers to execute the same function with at least one serving as a back-up. It should be mentioned that a disadvantage of applying the principle of redundancy is the potential for a corresponding increase in the attack surface presented to a malicious actor. If a malicious actor can exploit only one controller and generate negative effects or faults in the system, then the vulnerability has not been mitigated and the risk actually increased. Care should be taken to ensure that any application of redundancy with diversity to actually decrease the risk posed by a vulnerability by not increasing the attack surface. The Artificial Diversity and Defense Security (ADDSec) project led by Sandia National Laboratories, part of the DOE CRED program, is looking to add diversity by randomizing instruction sets to gain some of the benefits of redundancy with diversity without increasing the attack surface [46].

6 Cyber Resiliency Design Principles

While section 5 focused on the cyber security of CPS in operational energy systems, this section highlights the broader concept of cyber resiliency. Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources [47]. While the approaches to cyber security for CPS discussed in section 5 share some of the same goals, particularly as part of a Defense-in-Depth strategy, they do not address the ability to withstand and in some instances recover from attacks.

A challenge of increasing cyber resiliency of CPS is that its ability to anticipate and adapt are severely limited by their differences from IT systems, as originally outlined in Table 1-1. The limited computing power available at the individual device level and the strict timing requirements necessary to maintain physical system stability are significant challenges to be overcome. Also, as mentioned previously, operational energy systems must be able to perform in complex and chaotic tactical environments. The artificial intelligence capabilities being explored for IT systems and large-scale, fixed ICS have not yet matured to the point where they would be able to anticipate or adapt to adversary behaviors while successfully differentiating them from operator actions or commands.

However, many cyber resiliency design principles were discussed as part of the approaches to cyber security recommended for operational energy systems in section 5. Some examples of overlap are designing to limit the need for trust (least privileges), containing behaviors (segmentation), planning and managing diversity, and maintaining redundancy [47]. Some cyber resiliency design principles are also already incorporated as part of an intelligent operational energy system, such as leveraging health and status information to adaptively manage resources to complete the mission. As such, improving the cyber security of operational energy systems will also improve their cyber resiliency, particularly to less sophisticated attacks. As most any attacker will have limited resources available to them when targeting operational energy systems, a cyber-secure and high-assurance operational energy system will already have a significant level of cyber resiliency.

7 Vulnerability Identification & Assessment

The identification of potential high risk vulnerabilities is a key aspect of a defense-in-depth security strategy (see section 5.1) and needs to be a component of an overall risk management program. The list of high-risk vulnerabilities is used to identify the level of security that is required for each component or function to allow for a more targeted approach as opposed to a potentially disastrous blanket approach. However, development of such a list needs to be based on the impact to a specific intelligent operational energy system's mission (which differs from the published high-risk IT vulnerabilities [48]). The E&P CoI needs to be involved in these activities to ensure that the operational energy system functions and components are properly understood during the analysis and assessment, and that any proposed mitigations do not interfere with the operational energy system performance or safety.

7.1 Red- and Blue-Teaming

Red- and Blue-Teaming are two approaches that can be used as part of a vulnerability assessment. They can be used individually, successively, or even combined into a hybrid approach. They can also use a variety of specific methodologies to identify and assess vulnerabilities. A rigorous effort would start with a full Blue Team effort to collect all of the necessary information into a "knowledge-of-self" report, enabling the Blue Team to develop a testing plan and conduct their own vulnerability assessments that contain potential system and mission consequences of cyberattacks. The Blue Team would be composed of a variety of mission and system experts. The Red Team would then be provided with a set of potential system and mission consequences from the Blue Team to try and replicate in a manner a malicious actor would. The amount of system and mission intelligence provided to the Red Team can be tailored to fit the assessment needs. This can range from providing minimal details, to determine how an adversary might react to a completely unknown system, all the way to providing the full Blue Team product. The Red Team would be comprised primarily of cyber experts and, in the case of operational energy systems, some energy and power SMEs not associated with the system development effort (i.e., independent). The combination of the two efforts helps determine the identified vulnerabilities that carry the highest risk for the system and mission.

The Cyber Blue Book™ is a reporting template developed by the Air Force Research Labs (AFRL) Information Directorate (see section 9.15) to help consolidate and communicate the outcome of a systematic cyber vulnerability identification and assessment effort [17]. The template follows a specific model for relating the individual cyber-physical components to the missions, described in section 9.15, and the template sections outline the steps the Blue Team must go through to develop a comprehensive "knowledge-of-self," which can then be used for the vulnerability identification and assessment:

Scoping steps:

1. Identify missions of system under test (SUT)
2. Map the SUT MEF and their operational activities to the identified missions
3. Define the information exchange boundary (IEB) for the SUT
4. Identify the information flow across the IEB for the SUT

5. Characterize the information flows by detailing technical information such as protocols, directions, encoding, etc.

Vulnerability identification and assessment steps:

6. Map the dependence of the MEF on the cyber-enabled systems and actions
7. Using the dependency mapping, identify vulnerabilities and specify their type: architecture, specification, implementation
8. For each vulnerability, identify the type of compromise: confidentiality, integrity, availability
9. For each vulnerability, estimate the impact of one of the five types of effects (D5): disruption, degradation, denial, destruction, and deception
10. For each impact of each vulnerability, estimate the mission impact

A large number of methods have been developed for identifying and assessing the vulnerabilities using the full cyber-physical dependency mapping, and some are discussed in section 7.2. Based on the manner with which the individual vulnerabilities are assessed, the resulting data can be used to identify high risk ones that should be prioritized for developing mitigation strategies and potential counter measures. The list of high risk vulnerabilities can then be used by the Blue Team to develop a testing strategy to further inform and validate the information in the Cyber Blue Book™.

The Sandia National Laboratories Information Design Assurance Red Team (IDART) has developed a Red Teaming methodology, referred to as the IDART Methodology, based on their decades of experience conducting Red Team assessments [49]. The overall, iterative process is relatively simple:

1. Planning
2. Data collection
3. System and mission characterization
4. Analysis (return to step 2 as necessary)
5. Report

The unique aspects of the IDART Methodology are the specific steps they have compiled for each individual phase of the process. The planning phase is the most critical. A Red Team plan would consider questions such as: what is the specific need for the Red Team, which of the eight different types of Red Teaming are applicable (design assurance, hypothesis testing, gaming, behavioral, benchmarking, operational, analytical, and penetration), who are the adversaries of concern, what is the appropriate team composition based on the previous steps, which Red Team metrics will be used, and what the Red Team deliverables will be and how they will be used to report the findings (e.g., attack plans or adversary behavior narratives).

The next two steps (data collection plus system and mission characterization) are defined by the goals of the Red Team and how much data access and system exposure the program manager decides they are to be given. For example, if it is assumed an adversary has full access to the system specifications from open source or leaked information, the Red Team would be able to collect a large amount of data from different stakeholders. The analysis step is also where IDART has contributed a lot of knowledge based on their experiences, and they make use of multiple digital tools to facilitate the analysis. The initial brainstorming sessions start out by

building an attack diagram, linking adversary starting points to potential consequences with a series of attack steps in between. The IDART Methodology then takes the attack diagram and converts it into a form of system state diagram to discover potential mitigation strategies (i.e., a system view). The attack diagrams are also converted into fault-like attack trees to model the adversary capability required to exploit vulnerabilities and cause impacts (i.e., an adversary view). All of the resulting information and products are compiled into the report based on the goals stipulated in the original planning stage. Sandia's IDART offers courses to help train qualified prospective Red Teams or program managers on this methodology.

7.2 Vulnerability Identification and Assessment Methods

There are multiple systems engineering methods that focus on stepping through a rigorous process for vulnerability identification and assessment. For example, the System-Theoretic Process Analysis for Security (STPA-Sec) is one that specifically leverages hazard analysis techniques and applies them to CPS (see section 9.16). It has many similarities with the process outlined by the Cyber Blue Book™, but for simplicity and continuity with the section 7.1, the rest of this section will generally continue to follow the lead of the Cyber Blue Book™.

As described in the Cyber Blue Book™, the first step of conducting the vulnerability identification and assessment process is to map the dependency of MEFs on the individual system components, in this case the operational energy system cyber-physical components. One method for developing this mapping is a dependency mapping technique used by the MITRE Crown Jewels Analysis (CJA) [50]. It leverages a similar model to that used by the Cyber Blue Book™ to relate the MEF to the cyber-physical components (see section 9.15) and defines each dependency qualitatively as: "If <*child*> fails or is degraded, the impact on <*parent*> is <*failure, degrade, work-around, nominal*>." Figure 7-1 illustrates what a resulting view would be given the failure of an individual CPS. Iterating through all of the CPS and building out their dependency relationships with the MEFs will result is the list of mission-critical assets, or the crown jewels. A more rigorous approach would be to use the MITRE Cyber Mission Impact Assessment (CMIA) and its associated software tool, which requires a more detailed understanding and description of the system [51, 52]. Overall, the dependency mapping step would require the involvement of the E&P CoI to be able to properly link the impacts on CPS to the operational energy systems and to their respective operational activities.

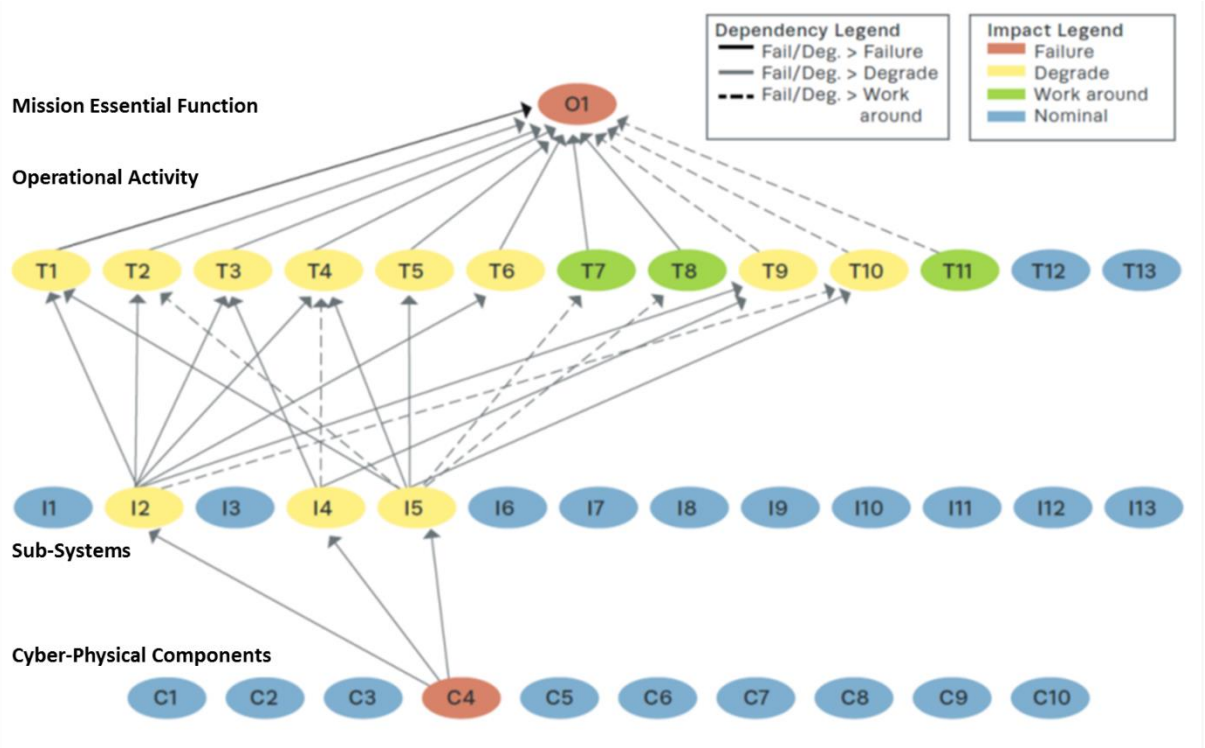

Figure 7-1 A example dependency mapping from the CJA process to predict the impact of a cyber-physical asset failure.

The Cyber Blue Book™ sections are based on the NIST Guide for Conducting Risk Assessments [18]. However, their risk model and assessment framework depend upon significant information on known threat sources (e.g., nation-states, non-state actors) and some determination of the likelihood that a threat source would try and initiate a specific cyberattack against a system; both items are problematic for practically executing a threat assessment. Many organizations do not have ready access to the detailed and highly controlled threat information necessary to understand a threat's capabilities, and determining the likelihood that an adversary will attempt a specific attack is highly subjective and imprecise even with detailed controlled information. Researchers at Sandia National Laboratories proposed a modification to the NIST risk model that replaces these items with a more asset-focused parameter: the degree of difficulty to exploit a vulnerability and then cause an impact [53]. Figure 7-2 shows a revision of the Sandia adaptations to the NIST risk model tailored for intelligent operational energy systems. To summarize: risks materialize as a result of attack scenarios of varying degrees of difficulty, each of which takes advantage of one or more vulnerabilities in CPS to cause a physical impact that results in consequences for system operation.

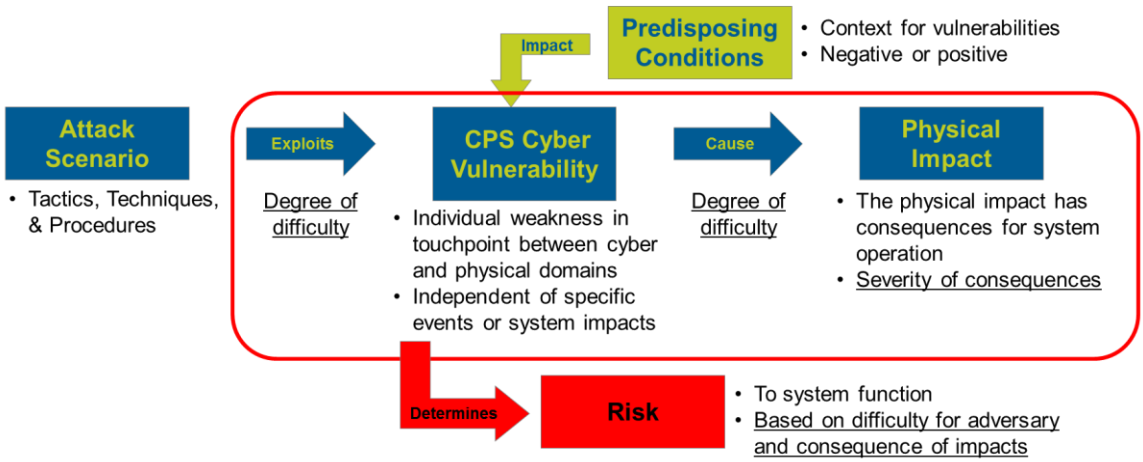

Figure 7-2 An adaptation of the NIST and Sandia generic risk models to cyber vulnerabilities for CPS in operational energy systems.

The risk model shown in Figure 7-2 can be used to evaluate the level of risk associated with each cyber vulnerability by iterating through known or brainstormed attack scenarios. There are multiple open source catalogs available for both attack scenarios and vulnerabilities, including their TTPs: common attack pattern enumeration and classification (CAPEC), common weakness enumeration (CWE), common vulnerabilities and exposures (CVE) [50]. A list of relevant attack scenarios for the specific operational energy SUT would need to be culled from those and other available catalogs to build a model of potential adversary behavior. The MITRE ATT&CK Matrix is a curated model of potential adversary behaviors specific to different systems [54]. The matrix graphically categorizes the different types of techniques that an adversary can use as the columns and lists specific techniques underneath. As the assessment team is developing the list of attack scenarios to evaluate, an ATT&CK Matrix can be used to ensure that they have a representative sample as opposed to one that potentially overlooks known adversary techniques that would be relevant to the system. A version for ICS is currently under development that could be leveraged to develop one specifically for CPS. Figure 7-3 illustrates how an ATT&CK Matrix could be used to develop the catalog of attack scenarios for use during a cyber vulnerabilities assessment of an operational energy system, with gray highlighting for the tactics a specific attack scenario employs.

Health & Safety	Physical Deception	Business Logic	Supply Chain	Financial
Physical Destruction	Timing Manipulation	Data Integrity Attack	Quality	Supply/Demand Manipulation
Alert Suppression	PNT Manipulation	Inference Attack (behavior of device)	Sabotage	…
…	….	…	….	

Figure 7-3 A high-level, initial ATT&CK Matrix for CPS with the elements of a potential attack scenario highlighted in gray.

For each unique attack scenario, the assembled vulnerability assessment team would evaluate the difficulty to exploit a cyber vulnerability, the difficulty to cause an impact once exploited, and the severity of the consequences if the attack is successful. The three major risk model parameter values are combined to develop an overall risk metric. It is a challenge to evaluate the parameters of the risk model in a systematic, repeatable, and accurate manner. This can be done qualitatively (low, med, high), semi-qualitatively (numeric range associated with different criteria), and, in rare instances, quantitatively based on an extremely rigorous assessment methodology with a very detailed model of the SUT. There are also a number of potential options for inputs to the three primary parameters. Table 7-1 lists a set of general factors, adopted from MITRE cyber Threat Susceptibility Assessment (TSA), that can be used to generate the values for the three primary parameters. The assessment team would develop criteria for either qualitative or semi-qualitative scoring levels for each based on the SUT and its missions. In a semi-qualitative example, if the recovery time from an attack scenario is inconsequential relative to the MEF, that attack scenario would be assigned a 1 for that factor, whereas if the recovery time causes the MEF to fail and the overall mission to be a failure then that attack scenario would be assigned the maximum numeric value possible in the assigned range, e.g., a 5 on a 1-5 scale. It is important for the E&P CoI to participate in the development of the set of factors and their scoring to ensure they properly reflect the operational energy system behaviors and impacts on the MEFs and overall mission.

Table 7-1 An example set of general factors that can be used to assess the risk of a specific attack scenario on an operational energy system.

Factor Name	Description
Proximity	What level of physical/cyber access is required?
Locality	Are the effects isolated to a single unit or widespread across a group?
Recovery Time	How long would it take to recover once attack detected?
Restoration Costs	How much would it cost to restore operation?
Impact	How serious are the impacts to the system performance?
Prior Use	Has this attack scenario (TTP) been used before (i.e., widely known)?
Required Skills	What level of skills/knowledge would an adversary require?
Req. Resources	The level of required money, assets, personnel, etc. to execute.
Stealth	Could this attack be easily detected given system security?
Attribution	How likely is it the attacker's identity would be discovered?

The most common method used to determine the values for the three main parameters and the overall level of risk to the system posed by a specific attack scenario are simple qualitative risk matrices (see Figure 7-4). The columns represent the possible values for one parameter or factor, and the rows represent another. There are many options for the grid pattern, some which evenly weight the two parameters and some which more heavily weight one over the other. However, there are multiple documented limitations of tabular risk matrices: poor resolution, errors, potentially suboptimal resource allocation for mitigation measures, and ambiguous

inputs/outputs [55]. Given the known limitations, they are extremely useful for communicating highly-sensitive findings to a general audience who do not have a need-to-know of the specifics.

Difficulty	Consequences				
	Very Low	Low	Moderate	High	Very High
Very Low	Very Low	Low	Moderate	High	Very High
Low	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
High	Very Low	Low	Low	Low	Moderate
Very High	Very Low	Very Low	Very Low	Low	Low

Figure 7-4 An example risk assessment matrix for qualitatively determining the overall risk score for an attack scenario.

Using a semi-qualitative assessment method can address some of the concerns with qualitative risk matrices. In a semi-qualitative method, the various factors listed in Table 7-1 are assigned agree-upon numeric values based on descriptions of the different levels of each for the SUT and associated missions, with the lowest value being the least risk/impact/consequential and the highest value being the most. The assessment team then generates equations to combine the different factors into the three main parameters, and then the three main parameters into the overall risk score. If properly designed, these equations can help reduce ambiguity, the likelihood of errors, and potentially other shortcomings of a fully qualitative approach when assessing an attack. There is still significant opportunity for suboptimal mitigation resources allocation, though, in part because the descriptions of the different numeric scores for the factors can still be ambiguous and subjective, the generation of the equations are subjective, and the final cut-off value for what is considered a high risk attack scenario for the SUT and its mission is also subjective.

Table 7-2 shows the final results of carrying out a full TSA and how those results are used for the vulnerability assessment. The TSA is a semi-qualitative method that starts out by assigning numeric values for each of the factors listed in Table 7-1 and then using an equation to compute the overall risk score for that attack scenario on the specific CPS as executed by different types of threats (i.e., external, insider, trusted insider). These values are combined using another equation into a risk score for that attack scenario and, more importantly for the E&P CoI, into an aggregate susceptibility, or risk, for each CPS. The overall CPS risk scores are used to prioritize which systems to focus on for remediation to mitigate their risk.

Table 7-2 A sample threat susceptibility matrix from the MITRE Threat Susceptibility Assessment method [50].

Attack ID	Risk Score	Cyber-Physical Asset 1			Cyber-Physical Asset 2		
		External	Insider	Trusted Insider	External	Insider	Trusted Insider
ID#1	4.4		4.4	4.4		4.3	4.3
ID #2	4.2		4.1	4.1		4.1	4.1
ID #n	…	…	…	…	…	…	…
Aggregate Susceptibility		14.9	22.1	12.8	21.6	30.4	18.6
			49.8			70.6	

The MITRE Risk Remediation Assessment (RRA) method [50] is one example of how the prioritized lists of attack scenarios and CPS can be used to decide upon a set of cyber security counter measures to implement. A catalog of available countermeasures are evaluated against each attack scenario for each CPS to determine whether it would fully neutralize an attack, be able to detect an attack, limit the attack's effectiveness, or allow a CPS to recover from that attack with a high, medium, or low degree of effectiveness. A scoring system is developed to calculate the utility of that counter measure (e.g., a highly effective neutralization would be the highest score, whereas a minimally effective detection would be the lowest score). Each counter measure would be assigned an implementation cost based on a variety of factors chosen by the assembled team (e.g., time, resources, impact on CPS performance). The ratio of the utility over the cost would allow for them to be ranked and a set of highly-ranked counter measures to be chosen to fully address all of the high risk attack scenarios for that CPS. This is also another area where the ATT&CK Matrix can be leveraged: marking each proposed countermeasure relative to its ability to fully, partially, or minimally (green, yellow, red) mitigate or detect the techniques laid out in the matrix (see Figure 7-5). An ideal set of countermeasures would have at least one "green" per cell among them.

Health & Safety	Physical Deception	Business Logic	Supply Chain	Financial
Physical Destruction	Timing Manipulation	Data Integrity Attack	Quality	Supply/Demand Manipulation
Alert Suppression	PNT Manipulation	Inference Attack (behavior of device)	Sabotage	…
…	….	…	….	

Figure 7-5 A high-level, initial ATT&CK Matrix for CPS used to evaluate the effectiveness of a proposed counter measure to mitigate or detect each adversary technique (red = minimal, yellow = partial, green = full).

This is just one example to show how the knowledge of the prioritized CPS vulnerabilities for a system can be translated into an effective set of cyber security counter measures. Another challenge is how to measure the potential effectiveness of a counter measure. It is important for the E&P CoI to be involved in this step particularly to ensure that the "cost" metric for each counter measure properly incorporates the expected negative impact on the operational energy system performance.

7.3 Related Technologies Under Development

Conducting rigorous and systematic vulnerability assessments is currently a significant challenge due to the time and resources required to fully execute all of the steps outlined in section 7.2. Most of the time these activities are limited to what are termed cyber table top exercises, involving a large amount of documentation but little-to-no interaction or testing with the system itself beyond the initial system identification steps.

Part of the challenge is due to the inherent risks with conducting cyber vulnerability assessments on the system, itself. The MITRE Corporation has ongoing research examining the ability to develop an effects simulator layer that would prevent malware from being inserted onto the systems and negative effects from happening on the targeted physical systems [56, 57]. The simulation layer contains models of attacked and evaluated components that can interact with the actual system components for a hardware-in-the-loop emulation of the attack. Rigorous model-, software- and hardware-in-the-loop assessments could be performed on unique or expensive systems to better assess vulnerabilities and test mitigation strategies.

Other limitations of a cyber table top exercise are its lack of repeatability, significant reliance upon the expertise assembled for the assessment, and time requirements. Model-based systems security engineering (MBSSE) is an approach that can be leveraged to address these challenges, and there are multiple ongoing research projects to develop technologies to apply MBSSE to CPS vulnerability assessments and security testing. The MBSSE approach centers around the repeatable injection of faults into a model of the SUT, using automated results analysis tools to assist in the security analysis, and allowing proposed mitigation strategies to be integrated into the model to evaluate their effectiveness.

The Cyber Security and Risk Analysis Workbench for CPS (SCAPS) is a software tool developed by The MITRE Corporation that uses architecture analysis and design language (AADL) models of the system, informed by MATLAB Simulink models of the controls behavior and physical system behavior, to accurately represent the entire CPS system [58]. It can also leverage MATLAB's hardware-in-the-loop capabilities in place of models of the controls or physical systems. The user inputs a proposed attack scenario into the AADL system model and SCAPS runs a comprehensive impact assessment that can then be analyzed by the user. The user can evaluate proposed counter measures and mitigation strategies by adding to the system model and repeating the analysis. There is also ongoing research at The MITRE Corporation that similarly follows the MBSSE approach but centers around an emulation environment that can contain commercial controls, interface, and other types of software as well as hardware-in-the-loop capabilities [59]. A system CPS model and a cyber effects library are used by the emulation environment to simulate their interactions with the contained software and hardware. In addition to the same ability to evaluate the performance of proposed counter measures and mitigation strategies, there is a filter that will show the information and data displayed to a potential user or operator, allowing the analyst to predict the potential human actions during an attack.

The ability to use MBSSE processes for operational energy system vulnerability assessments and for the iterative development of mitigation strategies and counter measures would be extremely beneficial to the E&P CoI. The primary reason for this, beyond the advantages already mentioned above, is that the E&P CoI is primarily concerned with the Applied Research, Advanced Technology Development, and initial Demonstration and Validation phases (6.2 through early 6.4). During these phases, the specifications for operational energy systems are constantly changing and evolving. Initiating a cyber table top that can take roughly 6 months or longer means that by the time the findings are reported out, the underlying model of the SUT could have changed drastically, negating the previous work. Leveraging the models and hardware prototypes developed throughout research activities allows the vulnerability assessments to keep pace with the system specifications. The portability of the cyber-physical models, as well, simplifies independent vulnerability assessments conducted by cyber and energy and power SMEs not affiliated with the development effort.

Please note that MBSSE does not take the place of rigorous experimental vulnerability testing on the final implemented system. Overall supply chain vulnerabilities for hardware systems are a significant concern that could introduce vulnerabilities not identified during the MBSSE efforts to the final system. However, the cost-effectiveness of the experimental testing can be greatly improved by leveraging the outcome of the MBSSE efforts to better tailor the experiments to high risk vulnerabilities.

8 Way Ahead

As the E&P CoI designs new intelligent operational energy systems, each effort needs to consider the cyber security and resiliency of its CPS. This is partly because cyber security and resiliency measures incorporated earlier in the design process will likely have the largest impact for the least cost. The field of high-assurance design needs to be leveraged, with the component operation and behaviors comprehensively mapped out so that the CPS and their interfaces can be fully constrained and simplified. Technology development activities often prototype on overly capable and flexible systems. However, limiting an adversary's ability to leverage CPS for unintended behaviors is the first and greatest step that can be taken for cyber security and resiliency of operational energy systems, and it needs to start with the individual researchers. Asking an acquisitions organization to rigorously constrain the behavior of a complex EMS, etc. will not be nearly as successful and could easily lead to unintended consequences; it needs to start bottom-up from the base-level components and be done throughout the entire system.

The E&P CoI researchers also need to start thinking about how to build a secure controls network architecture for their specific EMS, etc. A comprehensive operation and behavior mapping for a system design would allow implementation of many simple, yet very effective, techniques. The concepts of least privileges, network segmentation, and DMZs would greatly improve the cyber security and resiliency of operational energy systems. Assuming that a capable adversary with significant resources will gain access to a system, these concepts would limit the adversary's ability to leverage that access to generate impacts with significant consequences for the system and its mission. Attacks could be isolated, critical components and functions would be inaccessible, and the operational energy system itself would not become a high risk vulnerability for the rest of the platform.

Researchers should expand the activity logging capabilities of their systems to not only capture the necessary power and thermal system status but also the relevant cyber activities that occur. The original energy and power system researchers are better able to make sure that every important activity, whether it is a command or a changed setting, is logged so that anomalous behaviors can be better understood for debugging, forensics after a cyber event, and to prepare for when IPS and IDS capabilities mature enough to be deployed in tactical environments.

The last necessary next step for the individual E&P CoI researcher is to develop, or require comprehensive cyber-physical models of their operational energy systems. This would not only aid in EMS, etc. controls development, but could be leveraged with maturing MBSSE capabilities to conduct rigorous, independent, cyber vulnerability assessments both during system development and final prototype experimental testing. Again, a cyber security and resiliency measure incorporated earlier in the design process will likely be more effective and less costly to implement. Conducting vulnerability assessments as part of the iterative design process will allow vulnerabilities to be identified earlier and more cost-effective mitigation strategies determined and incorporated.

9 Completed or On-going Related Cyber-Physical Security Efforts

This section is intended to serve as a reference for the E&P CoI of the relevant efforts explored during the course of this study. The information compiled through the course of the outreach to these efforts plus other research was used to inform the report and its recommendations.

9.1 Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) Joint Capability Technology Demonstration (JCTD)

SPIDERS was a multi-phase program that culminated in 2015 to demonstrate the ability to construct and operate cyber secure microgrids on military installations with local energy storage and renewable resources with the intent to operate as islands for weeks at a time [60]. A "do no harm" policy required the existing electrical architecture to be able to continue to operate as originally intended in the case of a microgrid controller or system failure. Therefore, the effort leveraged a separate cyber-secure management system supplied by the Intelligent Power & Energy Research Corporation (IPERC) that sat on top of the existing industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. The overall approach to cybersecurity is reported as part of the Sandia National Laboratory (SNL) Microgrid Cyber Security Reference Architecture, which revolves around the application of the cyber security principles of "defense-in-depth" using network segmentation, actor authentication, and encryption [27]. The "defense-in-depth" principles are:

- Defense in multiple places
- Layered defenses
- Defensive strength as appropriate to asset value and its applicable threat
- Robust encryption and access key management
- Intrusion detection, analysis, and response

The SNL Microgrid Cyber Security Reference Architecture breaks up the microgrid computing systems into what are called enclaves, which can be organized by any combination of microgrid system function, geographical location, and/or security concerns. For example, all of the systems in one location can belong to a single geographical enclave, or they can be split into multiple enclaves based on both system function (e.g., cyber versus energy control versus energy distribution monitoring) and geography. Each enclave has its own security requirements that joining computing systems must either match or exceed as all intra-enclave communications and activities are inherently trusted. This is done to significantly reduce the potential attack surface to the enclave boundaries, which reduces the areas that need to be monitored for attempted unauthorized access or successful intrusions.

The other degree of segmentation in the SNL Microgrid Cyber Security Reference Architecture is accomplished with what are referred to as functional domains. Examples of possible purposes for a functional domain include overall microgrid monitoring and control, interfacing with all energy consumption, power generation, or energy storage subsystems, as well as interfacing with the electrical distribution components such as phasor measurement units. Segmenting the microgrid operations cyber management and monitoring into separate functional domains as opposed to a single all-encompassing cyber system greatly simplifies the necessary software

required to monitor and manage each microgrid operation, making it easier to identify unexpected activity and prevent adversaries from getting access to critical functions from intrusions into less secure parts of the microgrid. All inter-enclave communications occur within these functional domains and are prescribed using data exchange worksheets that detail the type of network traffic that will occur between two or more enclaves and the level of security that needs to be maintained for those communications. The use of functional domains limits the inter-enclave communications to only those that are specifically identified in the worksheets as operationally necessary, significantly reducing the opportunity for malicious activities to be lost in the noise and the likelihood that if an adversary compromises one enclave they'll be able to extend that control to others. Figure 9-1 provides a generalized example of a microgrid segmented by both enclaves and functional domains.

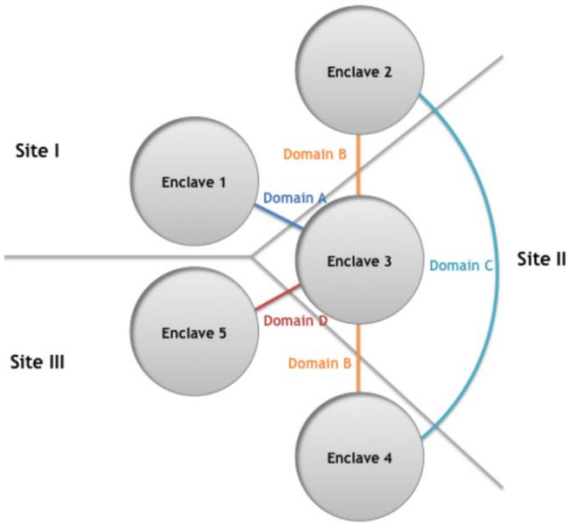

Figure 9-1 A generalized example implementation of the SNL Microgrid Cyber Security Reference Architecture's enclaves and functional domains [27].

9.2 Tactical Microgrid Standards Consortium (TMSC)

The Tactical Microgrid Standards Consortium (TMSC) is a public-private consortium started with funding provided through the Operational Energy Capability Improvement Fund (OECIF), which is managed by the Office of the Secretary of Defense's (OSD) Operational Energy Office (ODASD(OE)). The objective of the TMSC is to develop standards for the safe and assured operations of dynamic tactical microgrids, including: safety, protection, human factors, electrical interconnection, communications, controls, and cybersecurity [61]. Figure 9-2 shows a schematic of the TMSC tactical microgrid control architecture. There are three levels of digital controllers, which can all simultaneously exist on the same electronic hardware known as the local controller [10]. The local controller has a microgrid controller interface (MCI) that enables it to operate as part of the tactical microgrid.

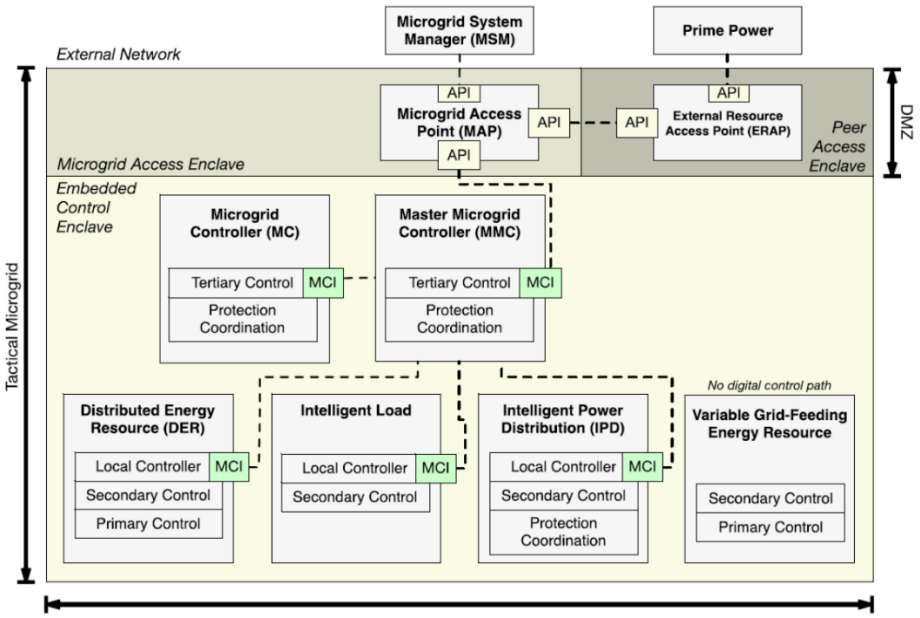

Figure 9-2 The TMSC Digital Control Architecture [10]

The primary controllers perform device-specific internal control functions [10]. The secondary controllers receive, interpret, and pass control information based on set rules and policies to the primary controllers. The tertiary controllers manage the microgrid-level operations by receiving data from and sending commands to the secondary controllers. The primary and secondary controllers are specific to each individual device and are often completely locked down by the vendor as proprietary. As such, the adoption of the TMSC standards is necessary to form a microgrid using components from a variety of vendors. The master microgrid controller serves the function of the tertiary controller and can exist on any of the devices' local controllers, enabling dynamic microgrid reconfiguration. In fact, devices that do not have the active master microgrid controller might maintain a separate tertiary controller in standby mode, ready to take over in case of the failure of the active master.

The standards leverage the NIST Special Publications 800-53 Rev 4 "Security and Privacy Controls for Federal Information Systems and Organizations" and 800-82 Rev 2 "Guide to Industrial Control Systems (ICS) Security" to enable the TMSC core cybersecurity principles and identify existing applicable standards for the necessary cybersecurity functional capabilities, some of which are described in Table 9-1.

Table 9-1 A summary of some of the necessary cybersecurity functional capabilities required by the TMSC standards [10]

Name	Description
Timekeeping	Robust and synchronized timekeeping allows for the sequential tracking and time-based initiation of events that are essential to troubleshooting and forensics across multiple physical devices.
Logging	The maintaining of trusted and chronological records of all microgrid physical and cyber activities enable troubleshooting and forensic analysis after anomalies are detected.
Cryptographic Identities	The use of cryptographic keys to identify both microgrid devices and users helps ensure that only authorized users and devices are present on the microgrid controls network.

Authentication & Authorization	Using the cryptographic identities to restrict device and user access to specific microgrid components and functionalities helps prevent unauthorized and potentially malicious access.
Zones and Conduits	Segmenting the microgrid controller network into functional enclaves that define and restrict inter-device communications helps to contain the effects of a successful cyber-attack to one enclave.

9.3 National Rural Electric Cooperative Association's (NRECA) Resilient and Agile Grid: Essence

Although a cooperative association, the National Rural Electric Cooperative Association (NRECA) has a very robust small-scale electric grid cyber security research and development portfolio funded by projects with the Department of Energy, ARPA-E, and DARPA [62]. The primary driver of their various research efforts is the concept of a "reactive" approach to cyber security that complements the more common "prescriptive" approach [63]. The NRECA "reactive" method is encapsulated by their *Essence* prototype, which abstracts the grid control system into five layers:

- Data: raw information
- Information: formatted databases
- Analysis: planning, operations, diagnostics, and research
- Decision: determine possible remediation steps
- Action: execute remediation steps

The key to this system is combining of the data and information layers into a single, real-time, status of the grid called the Common Grid State Database (CGSD). Each different microgrid operation would then be developed as its own software application that combines the analysis, decision, and action layers. Figure 9-3 illustrates the resulting relationship between the CGSD and each software application.

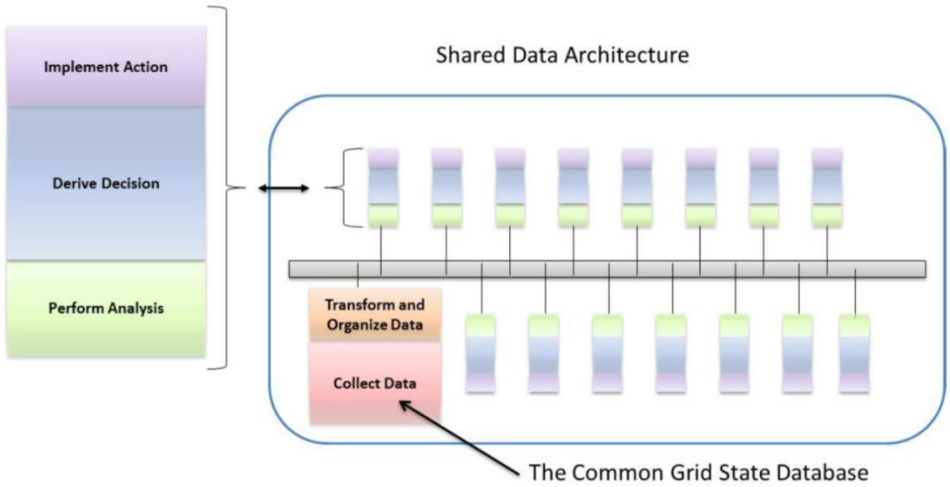

Figure 9-3 A schematic of the fully data-abstracted grid controller architecture as envisioned by the NRECA Essence prototype [63].

The presence of the CGSD allows for the development of three main types of cyber security applications that require a single picture of the actual state of the grid:

1. Applications that monitor for internal control system consistency with the grid's design by examining reports from individual sub-systems and the observed system settings
2. Applications that monitor the behavior and performance of individual systems against models of expected behavior
3. Applications that monitor for deviations from a mathematically derived model of the normal grid operations and information flow

The *Essence* prototype included two applications that leveraged the CGSD to demonstrate the first steps in a "reactive" cybersecurity approach: one that maps the grid communications and control network in real time and a second that uses machine-learning algorithms with the map to characterize the normal grid operation and detect anomalies. The prototype demonstrated the ability to detect anomalies on the order of minutes as compared to the hundreds of days it can take otherwise [64]. It is now being commercialized in partnership with N-Dimension Solutions, Inc., Milsoft Utility Solutions, and National Rural Telecommunications Cooperative (NRTC) [65].

The NRECA researchers also advocate for leveraging the agility afforded by the *Essence* prototype's abstraction layers to implement what is referred to as a "fractal grid" [63]. The grid would take on the characteristics of a fractal by segmenting into smaller units and having its behavior governed in the exact same manner no matter whether it is operating as a single unit, two units together, or multiple integrated units. Figure 9-4 illustrates an example fractal grid configuration composed of three distinct units. In the face of a cyber-attack or another stressor, the grid would immediately separate into its individual autonomous units to isolate the impact. The unaffected units would slowly recombine to form a more efficient, integrated grid and finally incorporate any impacted segments after they have returned to normal operation.

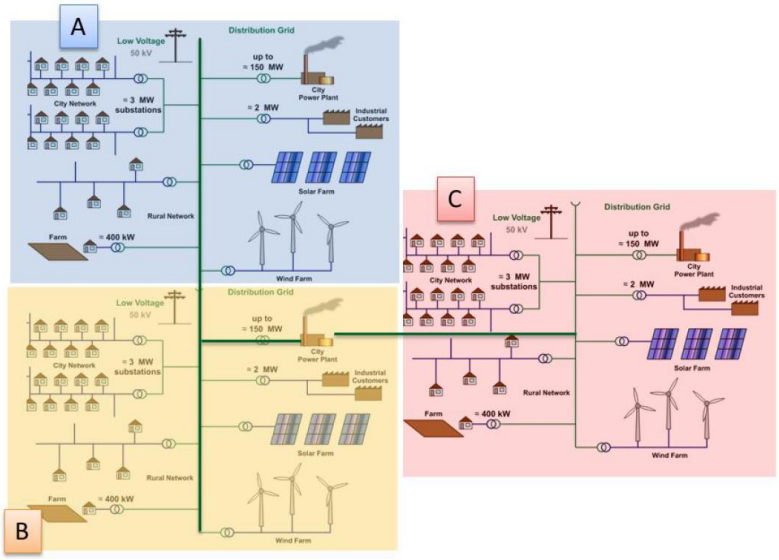

Figure 9-4 An example of the configuration of a fractal grid, segmented into three separate units (A, B, C) that can operate autonomously or as an integrated system [63].

9.4 Defense Advanced Research Projects Agency (DARPA) High-Assurance Cyber Military Systems (HACMS)

The goal of the High-Assurance Cyber Military Systems (HACMS) program is to develop semi-automated code synthesis capabilities that generate high-assurance cyber-physical operating systems and control systems software components using military vehicles as the demonstration platform [66] [67] [68]. It was a 4.5-year effort initiated at the end of 2012 and brought together performers working along three major thrusts:

1. High-assurance operating systems synthesis and verification tools
2. High-assurance control systems synthesis and verification tools
3. Producing a high-assurance current or future military vehicle

High-assurance cyber-physical systems are those where there is a high degree of confidence in its performance and security, even in the face of malicious cyber activities. The behavior of the software components is specified during the original code synthesis, and the ability to hijack the application and introduce new behaviors is extremely limited. In addition to the software synthesis technologies, the program targeted verification tools that could be used to check that the generated software meets its functional and security requirements and was successfully integrated with the rest of the operating or control system software.

Initial demonstrations on quadcopters and the Boeing Unmanned Little Bird showed no discovered security flaws after Red Team efforts and demonstrated the ability to isolate live attacks to unsecured applications. The active technology transition efforts include the Army Tank and Automotive Research, Development, and Engineering Center (TARDEC) Autonomous Mobility Appliqué System (AMAS) and GVRBot efforts, the NSWC Philadelphia Platform Independent Machinery Control System (PIMCS) effort, the Air Force Research Laboratory (AFRL) Loyal Wingman Project, and the Future Vertical Lift (FVL) program.

Based on these successes, a researcher who worked on the HACMS program published five major “hints” for how to design high-assurance cyber-physical systems, with the acknowledgement that they do not represent a one-size-fits-all approach [35].

1. Use Turing-incomplete programming languages to prevent undefined behaviors from producing unintended results
2. Simple interfaces that avoid ambiguous or user-constrained messages are secure interfaces
3. Automate repetitive system functions and interface boundaries to limit the ability to leverage bugs to produce systemic failures
4. System verification is a probabilistic game eliminating high-probability-of-exploit vulnerabilities dramatically improves security
5. High-assurance systems require a high-assurance culture to provide a strong foundation that incorporates basic best practices

9.5 DARPA Cyber Assured Systems Engineering (CASE)

The DARPA Cyber Assured Systems Engineering (CASE) program was announced in May 2017 and is focused on the systems engineering breakthroughs to better "design-in" cyber resiliency when designing complex embedded computing systems [69] [70]. One of the primary challenges these technologies would address is the shift from the traditional requirements writing axiom that functional behaviors are described using positive *'shall'* legal statements. Engineering cyber resilient systems in this manner is challenging because the capabilities are more naturally described using negative *'shall not'* statements. The goals over the course of the planned 4 year efforts are breakthroughs in:

- the elicitation of cyber resiliency requirements before the system is built;
- the design and verification of systems when requirements are expressed in '*shall not'* statements;
- tools to automatically adapt software to new non-functional requirements; and
- techniques to scale and provide meaningful feedback from analysis tools that reside low in the development tool chain.

It is important to note that one of the technical thrusts for the program is focused on support for legacy components.

9.6 DARPA Rapid Attack Detection Isolation & Characterization Systems (RADICS)

The goal of the Rapid Attack Detection Isolation & Characterization Systems (RADICS) program is to develop technologies for the rapid detection of and recovery from widespread cyber-attacks on the U.S. power grid and its cyber-physical ICS and SCADA systems [71]. It is a 4-year program that started in 2016 and consists of four major technical areas:

1. Situation Awareness
2. Network Isolation
3. Threat Analysis
4. Testbed & Sandbox Development

The situation awareness technical area is focused on providing as early of a warning as possible of malicious cyber activity in an effort to allow the grid operators to mitigate the potential consequences of an attack. The core challenge is successfully detecting anomalous cyber behavior with a low false positive rate. The U.S. power grid is constantly bombarded with unpredictable and unplanned events during its normal operation, including component failures and even improper system configurations. Differentiating between a "normal" incident and malicious activity is a fundamental research question. In the event of a successful cyber-attack, the operators must maintain situation awareness over their portion of the grid to be able to restore operations, extending the challenge both to the left and right of an attack.

An advanced grid power sensor, specifically a micro phasor measurement unit (PMU) developed by UC-Berkley and Lawrence Berkley National Laboratory (LBNL), is being provided to all of the situation awareness technical area performers to develop their software around [72]. The micro-PMU costs $5,500 each and is able to measure power line voltage and current levels as

well as phase angles to within 2-millidegrees of precision, all at a 4 GHz measurement frequency.

The network isolation technical area looks to tackle the challenge of coordinating the restoration of power across all of the different affected utilities. Ad hoc yet secure emergency communication networks are necessary to address the three primary challenges to doing so: completely disconnecting exploited systems, establishing new connections between both clean and exploited systems, and securing those connections into an emergency network. Significant challenges arise because pre-coordination is impractical and could expose critical system information to adversaries.

The testbed & sandbox technical area performer acts predominantly in support of the threat analysis technical area performers, providing a common development, testing, and evaluation environment complete with a range of ICS protocols and emulated equipment. The threat analysis performers are tasked with developing capabilities to map the ICS network, discover unexpected behaviors, and rapidly identify and characterize cyber-weapons. These methods must be compatible with ICS networks to not disrupt their proper function and detect potential set point, software, and firmware changes on devices for which they have little-to-no available technical specifications and information.

9.7 United Kingdom Ministry of Defense Land Open Systems Architecture

The United Kingdom (UK) Ministry of Defense (MOD) has required the use of open systems architecture to improve design cost and optimal integration across various systems with the implementation of open standards. To this end, the Land Open Systems Architecture (LOSA) is an approach aimed at efficiently integrating equipment and services within a brigade. “The vision for LOSA is one where, using defined open system architectures and mandated standards, developed in conjunction with industry, the efficient integration of sub-systems on vehicles, bases and soldiers, and the interoperability between them, is achieved. Realization of this vision is aimed at maximizing the operational agility of force elements to respond to change, while reducing the cost of ownership” [73]. LOSA can be categorized in three distinct areas: Generic Base Architecture (GBA), Generic Vehicle Architecture (GVA), and Generic Soldier Architecture (GSA) with Figure 9-5 illustrating the possible interactions between them.

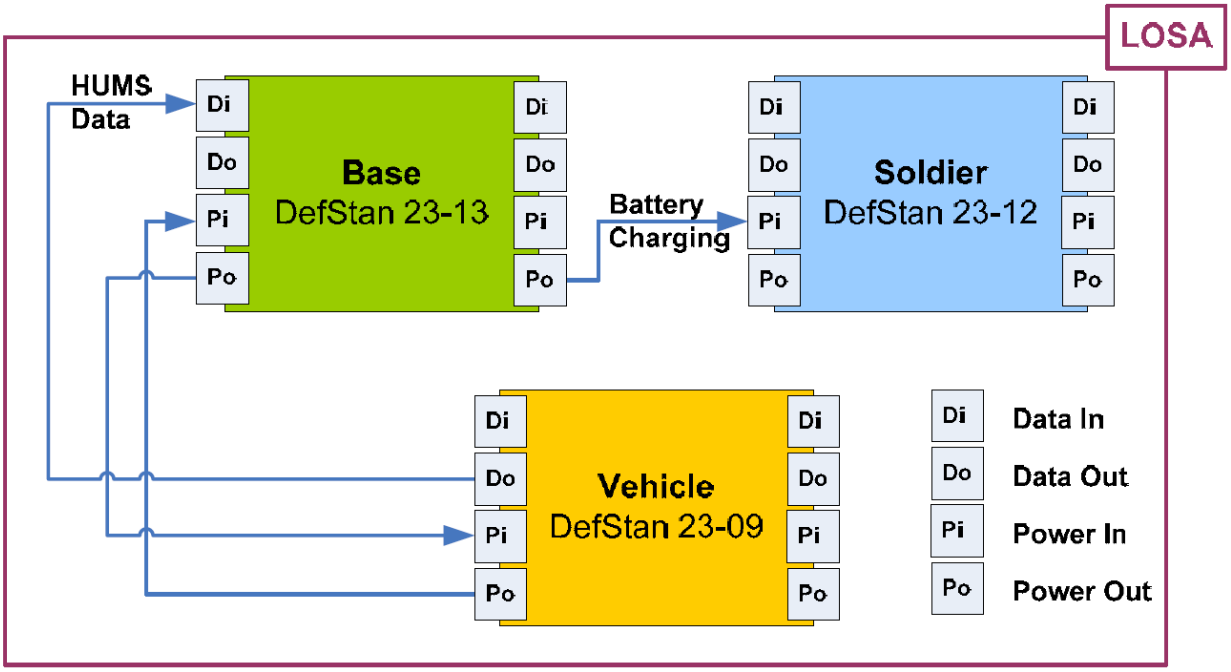

Figure 9-5 Anticipated future interfaces between base, vehicle & soldier architectures [73]

9.7.1 Generic Base Architecture (GBA)

The GBA standards are intended to interface with several infrastructures including: power, water, waste, and fuel. In terms of the power infrastructure, the GBA standards are like those outlined in the Tactical Microgrid Standards Consortium (TMSC) and will not be discussed in further detail.

9.7.2 Generic Vehicle Architecture (GVA)

The GVA standards dictate how Health and Usage Monitoring System (HUMS), Human Machine Interface (HMI), data, and power should interface in a vehicle platform. This architecture is shown in Figure 9-6. HUMS represents technologies that are used to retrieve, process, and store data in a platform. HMI provides display and control (i.e. monitors, keyboards, buttons) to the crew to use various vehicle platform sub-systems. The GVA data infrastructure consists of: one or more Local Area Networks (LANs) for data distribution, video distribution and subsystem control; network connectors including Universal Serial Bus (USB) for peripheral devices; time service; Data Distribution Service (DDS) / Data Distribution Service Interoperability (DDSI) wire protocol and the GVA data model. A simplified GVA data structure is shown in Figure 9-7 where the black boxes represent data connection points that are constrained by GVA requirements. Lastly, standards are provided for the power infrastructure which contains physical cables, connectors, and any other devices that distribute or control electrical power in a vehicle platform. The power architecture is defined as having two types of equipment: Platform Equipment[5] (PE) and Terminal Equipment[6] (TE), and an Auxiliary Power

[5] Original equipment fitted to COTS and MOTS platforms at procurement. These systems are permanent and connected to the Platform Power Distribution System.**Invalid source specified.**

[6] Equipment that is fitted to COTS and MOTS platforms for a specific purpose. These systems can be permanent or temporary, and are connected to the platform or APU using the TE Power Distribution System. **Invalid source specified.**

Unit (APU) to charge both the PE and TE batteries (see Figure 9-8 for a sample power architecture).

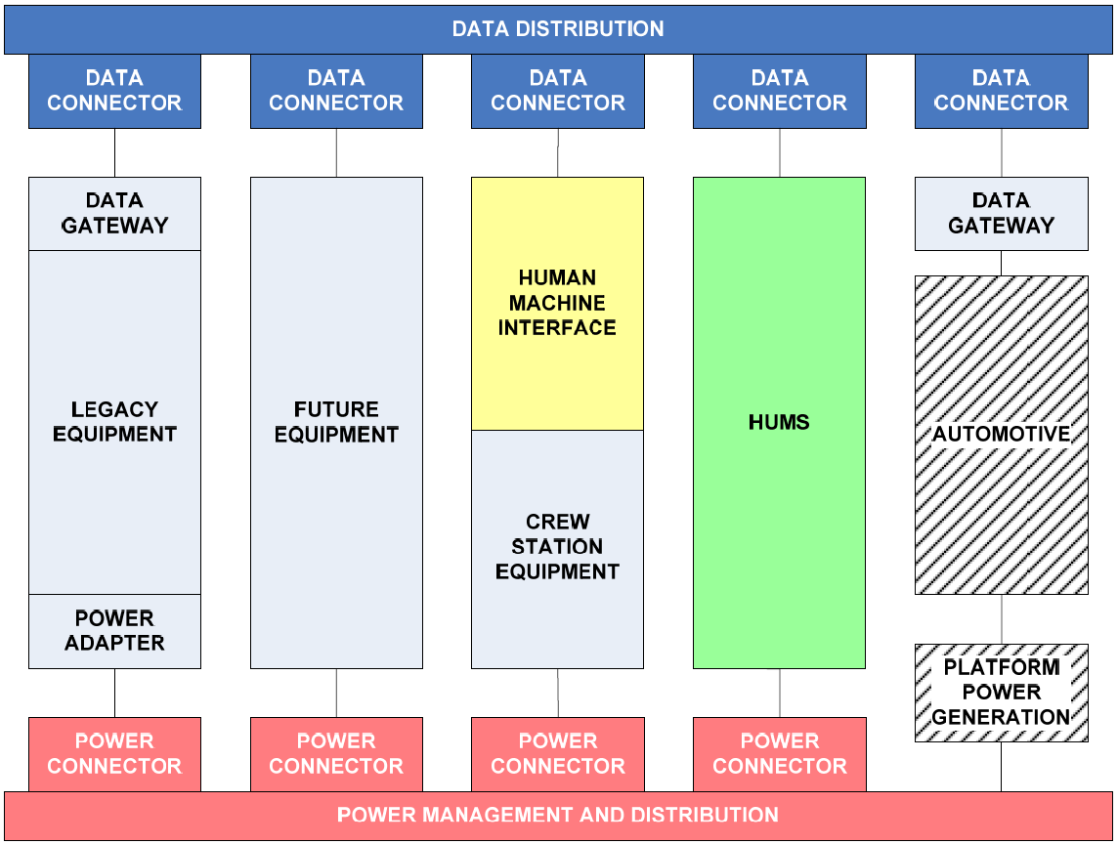

Figure 9-6 GVA sample architecture [74]

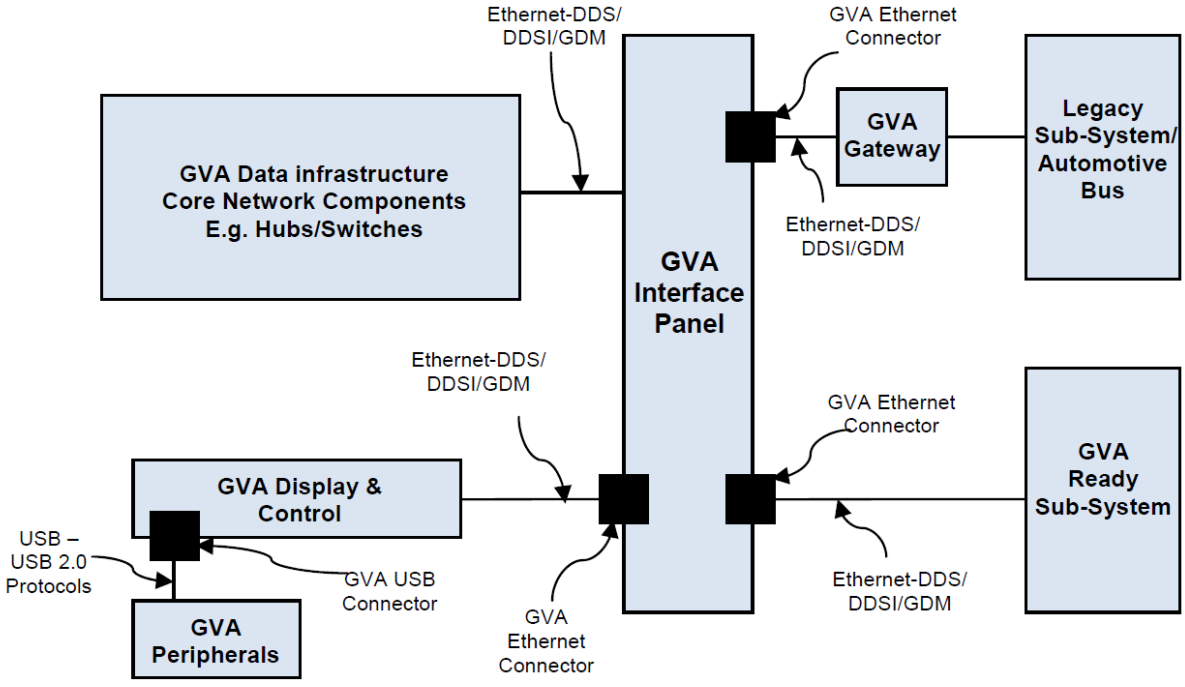

Figure 9-7 Simplified GVA data infrastructure [74]

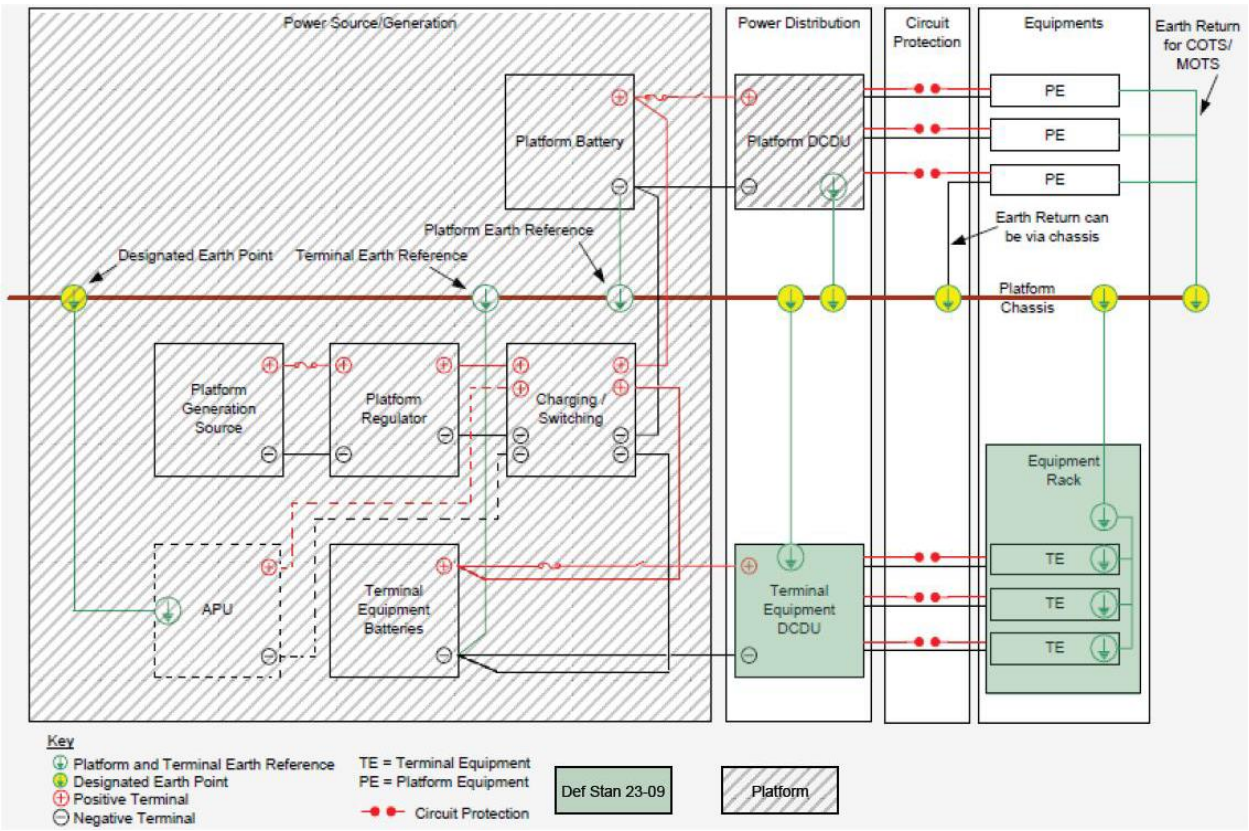

Figure 9-8 Power system architecture example [74]

9.7.3 Generic Soldier Architecture (GSA)

The Generic Soldier Architecture is a set of standards that provide system coherence and interoperability across multiple domains (i.e. land, air, and sea) and platforms (i.e. base and vehicle). The GSA is designed to support a range of functionality, from simple low functionality to a sophisticated system offering full Situational Awareness (SA). To enable this functionality flexibility, open standards for power and data infrastructure must be used together with physical interfaces and human factors guidelines. The GSA power and data architecture is shown in Figure 9-9 with three main subsystems: weapon, helmet, and torso.

The torso subsystem is the most critical from an energy and power perspective, and it is comprised of the following components: data hub, personal unit processor, power hub, central energy storage, auxiliary energy storage, and role equipment. The torso data hub provides data connections to the various components using a USB2.0 standard. This component will also provide 5V power as an additional power source. The personal processor unit collects, processes and routes data around the architecture, as well as monitors, reports, and controls the power to various other components. The power hub is responsible for the power distribution as well as containing a power strategy between the various energy storage devices. The central energy storage device should be a high specific energy rechargeable device, but also allows for primary energy providers (i.e., not rechargeable) and smart batteries with an additional USB interface. An auxiliary energy storage can also be connected through the standard role equipment connector to provide additional energy with energy storage devices or a power scavenging device. Various role equipment, depending on the soldier's mission, may be connected to the torso subsystem for power and data support. Lastly, the off-platform interface provides a data and power interface

with other LOSA compliant architectures such as GVA or GBA through the Common Open Interface (Land) standards [75].

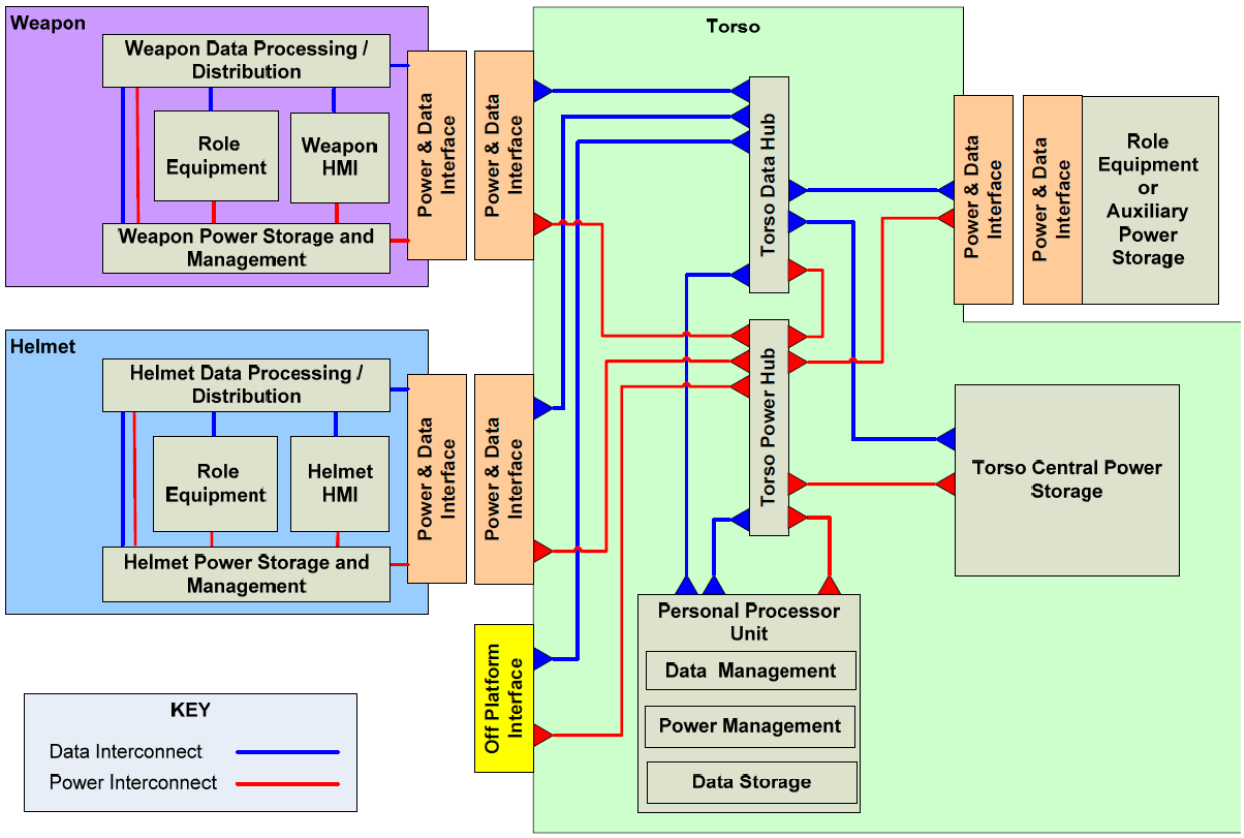

Figure 9-9 Generic soldier data and power architecture [75]

9.8 Robot Operating System (ROS)

The Robot Operating System provides libraries and tools to help software developers create robot applications. It provides hardware abstraction, device drivers, libraries, visualizers, message-passing, package management, and more [76]. The first version of ROS focused on providing software tools for users to quickly deploy research and development robot projects. These software tools were designed to allow most of the software to be reused in various applications.

The main characteristics of the original ROS architecture were: “single robot; workstation-class computational resources on board; no real-time requirements (or, any real-time requirements would be met in a special-purpose manner); excellent network connectivity; applications in research, mostly academia; and maximum flexibility” [77]. However, ROS was adopted in several other areas like manufacturing, agricultural, and government agencies such as NASA and the military. With the expansion of the ROS community and to support ongoing/future growth, ROS 2.0 is being developed to address new use cases such as: teams of multiple robots, small embedded platforms, real-time systems, non-ideal networks, production environment, and mechanisms for life cycle management and static configurations. One of the major changes of the ROS 2.0 architecture is in the reliance on Data-Distribution Service (DDS) and Real-Time Publish Subscribe (RTPS) protocols as the underlying communication standard.

Other implementations of ROS are ROS-Secure and ROS-Military. ROS-Secure (SROS) is a set of security enhancements for ROS containing the following features: Transport Layer Security (TLS) cryptographic protocols, certificates permitting chains of trust, node restrictions and permitted roles, tools to auto generate node key pairs, audit ROS networks, construct/train access control policies, and harden or quarantine ROS based processes running on a Linux kernel. SROS is currently under development and is not considered mature enough for deployment [78]. ROS-Military (ROS-M) is a military instance of ROS in which military software is managed outside of the open source ecosystem of ROS. ROS-M has the following organizational components: software repository, community, documentation, documentation, continuous integration, validation & certification, and registry. Figure 9-10 shows the conceptual model of ROS-M. ROS-M is currently in its last phase of development to be completed by November 2017 [79].

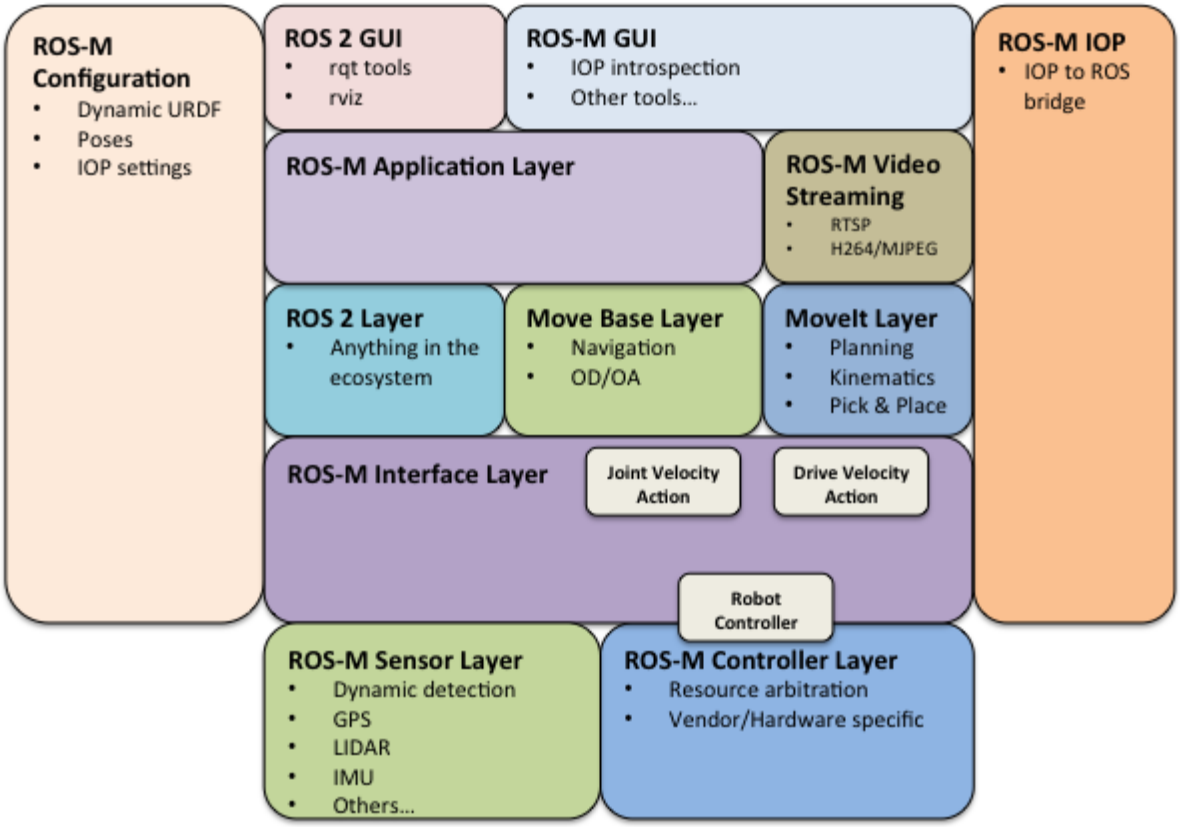

Figure 9-10 ROS-M Conceptual Model [79]

9.9 Office of Naval Research (ONR) Resilient Hull, Mechanical, Infrastructure, and Electrical Security (RHIMES) Future Naval Capability (FNC) Program

The Resilient Hull, Mechanical, Infrastructure, and Electrical Security (RHIMES) Future Naval Capability (FNC) Program led by the Office of Naval Research (ONR) aims to improve cyber-physical system resiliency for its shipboard electrical and mechanical control systems [45]. The approach leverages the already installed redundant back-up controllers to increase the level of effort required for a malicious actor to affect the targeted system. Introducing small differences

to the software and hardware of the primary and backup controllers requires a malicious actor to determine how to affect each individually before they can cause their desired effect, instead of being able to affect both simultaneously using the same techniques.

9.10 U.S.S. Secure

The U.S.S. Secure effort is a collaboration between 28 different groups (NSWC Dahlgren, Philadelphia, Corona, and Crane; NAWC Lakehurst, Patuxent River; National Cyber Range, DoD TRMC, Joint Staff, and Navy Red Team) to realize a distributed hardware-in-the-loop cyber testing range [80]. The goal is to allow the development and testing of cyber resiliency capabilities in a process that is separate from the overall platform accreditation and certification process, which limits malicious cyber effect testing of the systems.

9.11 Naval Surface Warfare Center Crane Division (NSWC Crane) and Purdue University Cooperative Research & Development Agreement (CRADA) on cyber-secure intelligent battery

The Naval Surface Warfare Center, Crane Division (NSWC Crane) and Purdue University researchers entered into a Cooperative Research & Development Agreement (CRADA) in August 2017 to jointly develop a cyber-secure, intelligent battery energy storage system [81]. The focus will be on concurrently developing microstructured solid-state electrodes for Lithium-Sulfur batteries, new methodologies for measuring the state-of-charge (SOC) and state-of-health (SOH) and other metrics real-time, and using that information to optimize battery performance and prevent detected faults from turning into battery system failures. This type of intelligent battery monitoring and management system introduces cyber vulnerabilities and so the effort will collaborate with cyber security researchers and subject matter experts (SMEs) at Purdue University and NSWC-Crane to incorporate mitigation strategies and incorporate cyber resilience into the intelligent battery energy storage system.

9.12 Data Distribution Service (DDS)

Data Distribution Service (DDS) is a standard developed by the Object Management Group (OMG) that describes a Data-Centric Publish-Subscribe (DCPS) model for distributed application communication and integration in real time. The purpose of the DDS standard is to enable efficient and robust delivery of the right information to the right place at the right time. The DCPS model accomplishes this by building a global data space that is accessible to all interested applications. Applications that wish to contribute information to the data space become Publishers while applications that want access to part of the data space become Subscribers. Every time a Publisher posts new data, the middleware[7] spreads the information to all interested Subscribers. Many applications rely on the DDS standard, such as, C4I (Command, Control, Communication, Computers and Intelligence), industrial automation, distributed control and simulation, telecom equipment control, sensor networks, network management systems, and internet of things [82].

However, DDS does not address message exchange over transports (i.e., TCP, UDP, IP). This means different implementations of DDS will not interoperate with each other without additional vendor-specific communication methods. With the deployment of DDS across many systems, a standard DDS wire protocol was required to allow DDS implementations from multiple vendors to interoperate. The Real-Time Publish Subscribe (RTPS) protocol is already in use in many industrial automation systems making it a proven technology, and it was selected to become the DDS wire-protocol [83].

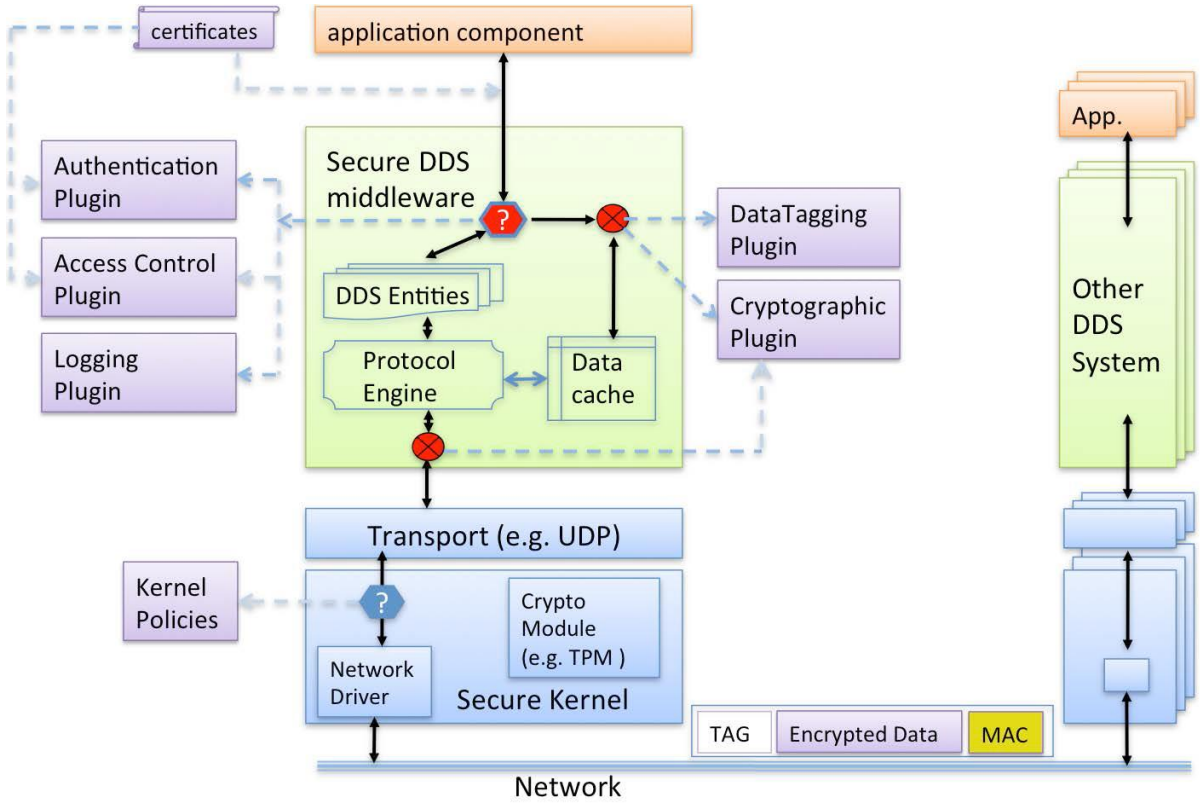

Figure 9-11 Overall DDS Security architecture [84]

[7] Middleware is a computer software that provides services to software applications beyond those available from the operating system.

DDS Security Support is an additional standard to the DDS standard to provide additional security features. DDS Security defines the Security Model and Service Plugin Interface (SPI) to enable out-of-the box security and interoperability between compliant DDS applications (see Figure 9-11 for overall system architecture). The following five SPIs are defined in the protocol to provide Information Assurance to DDS systems [84]:

1. Authentication – Means to verify the identity of the application and/or user, including mutual authentication between participants to established a shared secret
2. Access Control – Only allow authenticated users to perform certain operations based on policy decisions
3. Cryptographic – Provide encryption, decryption, hashing, and digital signatures
4. Logging – Audit of all DDS security-relevant events
5. Data Tagging – Provides a way to add tags to data samples

9.13 Vehicular Integration for C4ISR / EW Interoperability (VICTORY)

The Tank Automotive Research, Development, and Engineering Center (TARDEC) has created a vehicle standard named VICTORY to enable the use of C4ISR/EW technology in ground vehicles. In previous deployments C4ISR technology was "bolted-on" to the vehicle as standalone equipment. This led to an increase in the overall vehicle weight and consumed significant space which reduced the crew space. The VICTORY standard requires an open plug-and-play architecture such that C4ISR/EW technology can interact with one another and draw power from the vehicle platform. This will significantly reduce Size, Weight, and Power (SWAP) by removing the number of repeating components (e.g., one GPS device will be used to provide data to all other devices versus each device having their own GPS technology) and individual powering devices (e.g., batteries). The VICTORY framework is composed of the following:

1. Define common terminology, systems, components and interfaces architecture
2. Provide standard technical specifications for items in the architecture
3. Reference designs to guide the implementation of the architecture and standards

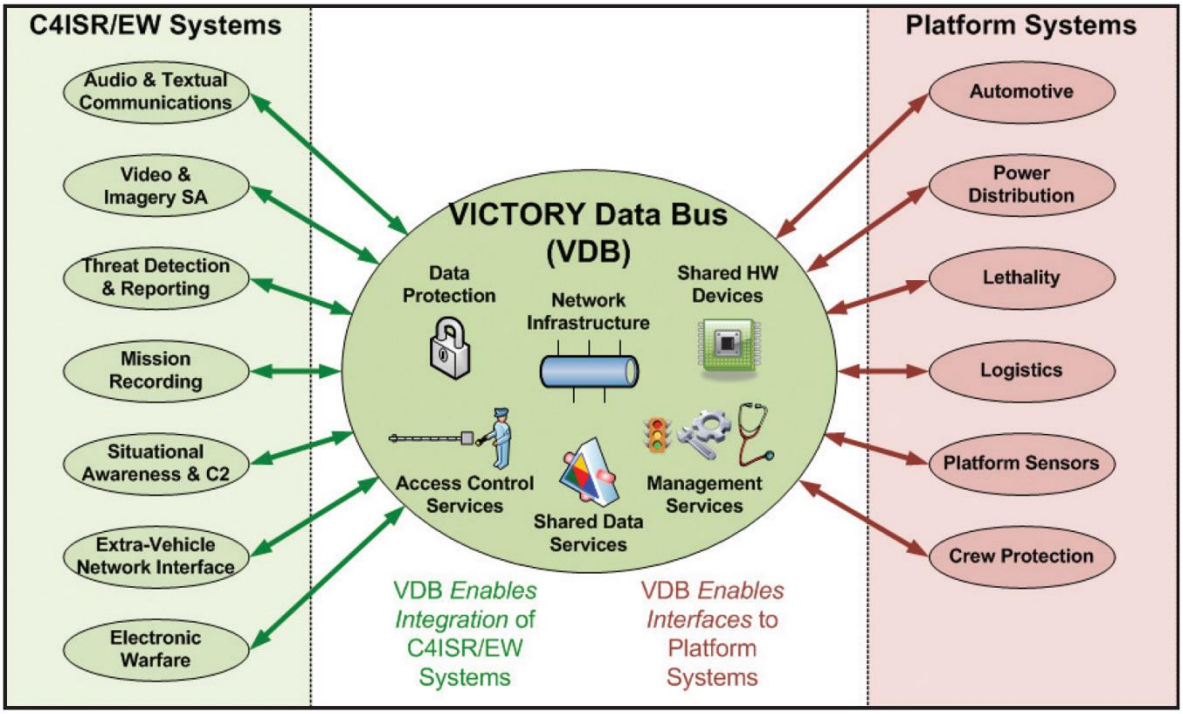

Figure 9-12 VICTORY Data Bus Concept [85]

9.14 USAF Cyber Resiliency Office for Weapon Systems (CROWS)

The Air Force Life Cycle Management Center stood up the Cyber Resiliency Office for Weapons Systems (CROWS), which reached initial operating capability in Dec 2016 and expects to reach full operating capability in Oct 2017, to help manage the execution of the AF Cyber Campaign Plan as well as to integrate activities across all Air Force communities that acquire, field, operate, and sustain weapons systems [86] [87]. Their goal is to manage the risk of an adversary exploiting weapon systems cyber intelligence and enable weapon systems to maintain their mission effectiveness even in the face of malicious cyber operations. These goals are directly related to the execution of Section 1647 of the FY16 NDAA [9]. The office will provide integrated program management and execution oversight for a set of 7 complementary Lines of Action (LOA):

1. Conduct mission-level cyber risk analysis
2. Integrate cyber-resiliency into systems engineering
3. Recruit, hire, and train cyber workforce
4. Improve weapon system agility & adaptability
5. Develop a common security environment to enable collaboration
6. Assess & protect the fielded fleet
7. Provide cyber intelligence support

The general process for CROWS can be understood as originating in LOA 1, which determines the critical systems with cyber characteristics that are required to execute a specific mission. The considered systems cover the entire mission thread and are not necessarily directly associated with a specific weapon but could be related to what they are referring to as the infrastructure:

logistics, sustainment, maintenance, communications, etc. This group is also charged with developing a mission thread cyber assessment methodology and framework. The list of critical systems for a specific mission thread is then handed off to LOA 6 to determine the critical cyber vulnerabilities and develop and implement techniques to secure them, mitigating the potential threats. This is all done in collaboration with LOA 7 to make sure the mission thread analysis and mitigation activities are informed by the latest threat intelligence. The office is also concerned with institutionalizing cyber-resiliency beyond the specific mission threads that are investigated: LOA 2 is working to ensure that cyber-resiliency is address throughout the capability development and acquisition lifecycle; LOA 4 is working to make weapons system designs more cyber-resilient through agile and adaptive architectures. The CROWS effort also looks to define what they call a cyber resiliency for weapon systems technical reference architecture (CRWS TRA) to use for developing integrated technical standards.

This effort includes cyber-physical considerations as their working definition for "cyber aspects" includes: software, firmware, electronic data, and associated hardware [87]. There are also stated objectives to incorporate ICS/SCADA cyber protection methods into their activities. However, the scope of these efforts has not yet been formalized. Depending on how these efforts are applied in practice to the platform operational energy systems this office could be a significant partner with the DoD Energy & Power community in ensuring cyber resiliency is embedded in the next generation of advanced operational energy systems.

9.15 Air Force Research Laboratory (AFRL) Cyber Blue Book™

The Air Force Research Laboratory (AFRL) Information Directorate developed the Cyber Blue Book™ as a template to assist and drive cooperative Blue Team and adversarial Red Team testing of distributed information systems [17]. The goal of the Cyber Blue Book™ is to provide the Blue Team with comprehensive knowledge of the system-under-test, containing a mapping of the mission functions of all sub-systems and their cyber components, their information exchange requirements with the outside world, the vulnerabilities critical to mission success, and the potential estimated mission impacts of successful exploitation.

The Blue Team uses this information to design their cyber vulnerability and resiliency testing of the system, aiming to validate and quantify the potential mission impacts of vulnerability exploitation. The Red Team lacks comprehensive knowledge of the system and its mission and is primarily composed of cyber-attack subject matter experts. Using only descriptions of the cyber-attacks and their mission impacts from the Cyber Blue Book™, the Red Team attempts to replicate the impacts of exploiting a vulnerability while determining the necessary adversary capabilities in terms of time, talent, and treasure. All together the information from the cooperative Blue Team and adversarial Red Team testing helps drive the development of mitigation strategies for the identified cyber vulnerabilities for the system-under-test.

9.16 System-Theoretic Process Analysis for Security (STPA-Sec)

One of the challenges to addressing cyber security of operational energy systems is that its continued fundamental operation is paramount in an unsure and rapidly evolving environment where it is practically impossible to be fully aware of every single threat the system faces. Even if a system designer has full knowledge of an operational energy system, he or she will still be severely limited when using many traditional cyber vulnerability identification, analysis, and assessment processes by their ability to imagine all of the possible threats that system will face. The System-Theoretic Process Analysis for Security (STPA-Sec) is a systems engineering

methodology adapted from work on hazard analysis that attempts to address this shortcoming, and others, by approaching a vulnerability analysis from the top-down on vulnerable system states as opposed to from the bottom-up on specific threats [88]. The authors frame this as a difference between a tactical focus on preventing specific threats versus a strategic focus on preventing the potential negative outcomes of a threat.

The underlying systems engineering approach is to treat each system as a hierarchical structure of control actions where each level enforces behavior constraints on the level below it according to built-in models on how the lower levels are expected to operate. The process is also designed to require collaboration between the cyber security experts, the system designers, and the operational experts; the key motivation being that any cyber security technology or methodology will have potential trade-offs with the fundamental system functionality that needs to be considered. The STPA-Sec process has 5 major steps:

1. Establish the systems engineering foundation:

   Identify the essential services and functions provided by the overall system. Develop a list of the system states that could lead to the loss of one or more of the essential services and functions.

2. Generate a model of the high-level control structure:

   For each of the vulnerable systems states identified above, map out the functional controls involved and their general actions. Start at the high level controls before decomposing, when necessary, to smaller sub-element controls. The five basic components of these models are: the operator, the digital control system that interprets the operator inputs and sending control signals, the actuator, the physical system itself, and any sensors used to monitor the system.

3. Identify unsafe or unsecure control actions

   Each of the general actions from the high-level control structure model needs to be evaluated to determine whether they can lead to unsafe or unintended systems states. The four different categories of potentially unsafe or unsecure control actions are: those that are provided when they should not be, those that are not when they should be, those that occur at the incorrect time or in the incorrect order, and those that are stopped too soon or continued too long. Evaluating the potential system behavior to each of the four types of unsafe or unsecure control actions will allow the analysts to filter down the list to those control actions that are vulnerable to resulting in unsafe or unintended system states.

4. Develop security requirements and potential constraints

   Requirements and constraints need to be developed for each of the identified vulnerable control actions that, if followed, would prevent the system from entering an unsafe or unintended system state. For example, a remotely-controlled source breaker on a TMG IPD unit should not be opened when the current load is within allowable limits and the power source is not experiencing any negative performance behaviors, such as overheating.

5. Identify causal scenarios

   The last step in the analysis involves identifying how the control action requirements and constraints could potentially be violated, generating scenarios for how malicious actors

could exploit the vulnerable control actions to cause a negative impact to the system. These scenarios could then be used by system designers to device mitigation measures to prevent the violation of the control action requirements and constraints. Figure 9-13 *is a generalized control action loop that can be used as an aid by the analysts to develop the casual scenarios, as well as beyond the STPA-Sec analysis to design system safe modes and other mitigation strategies* [89].

It is important to understand the limitations of this approach and realize that in many instances it only represents one tool in a toolbox [89]. First and foremost, it does not fully consider the potential negative ramifications due to the loss of confidentiality of data. For example, STPA-Sec would not cover the instance where a malicious actor gains access to the system and determines the identity of the operator and potentially steals his or her credentials. This action in itself would not directly impact the operation of the system and so therefore would not be uncovered during the analysis. This type of attack is potentially a concern for system designers because the identified operator could then be targeted for foreign intelligence purposes, or his or her credentials could be used to pose as a legitimate actor on the system and take control of it. Second, it would need to be expanded to those interactions and interfaces that are outside of the specific control action to fully account for the potential cyber pathways a malicious actor could take to negatively impact the system. such as via a denial-of-service (DoS) attack using an exploited but networked non-critical computing system.

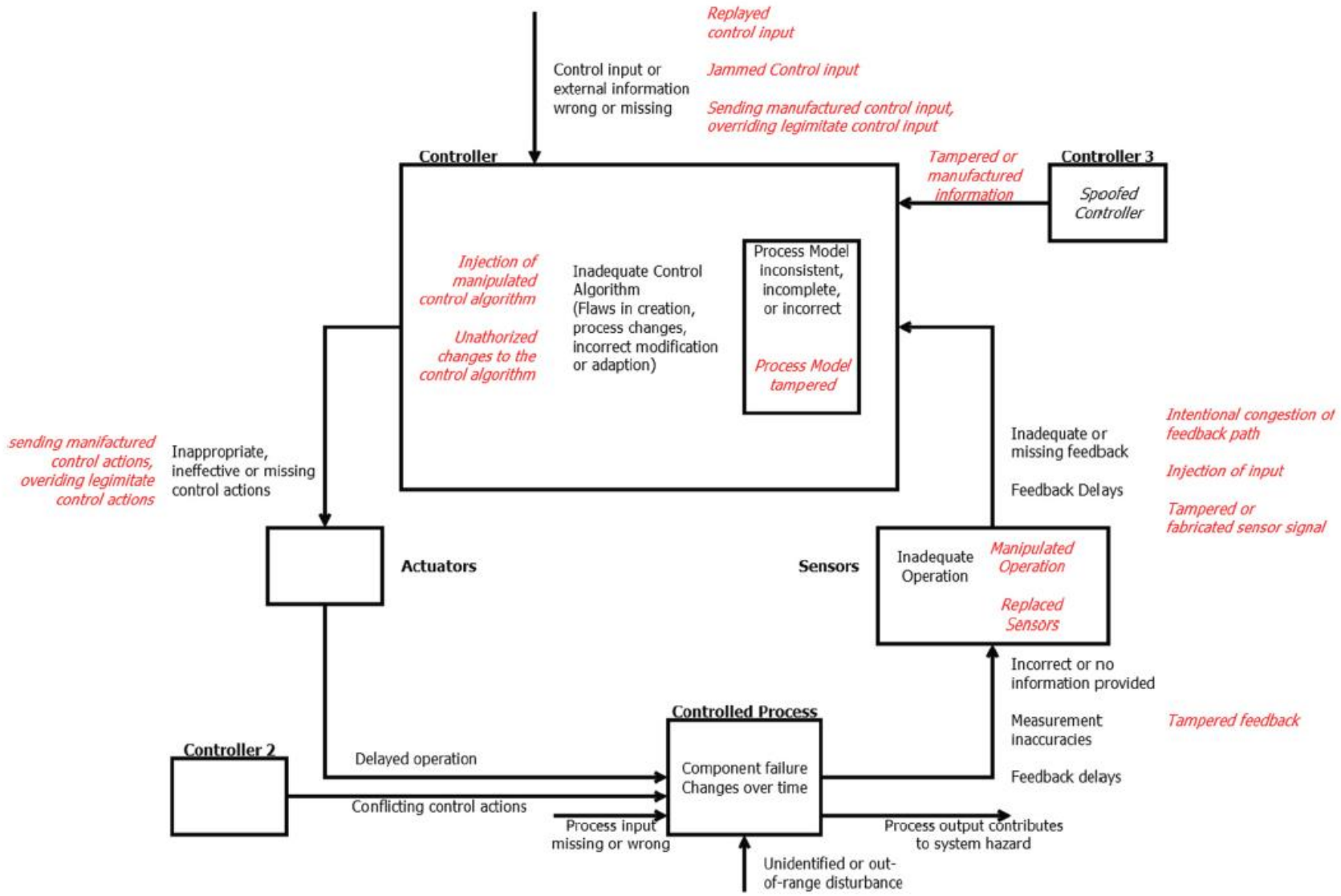

Figure 9-13 Expanded generalized control loop used as part of the STPA-Sec vulnerability analysis process [89].

9.17 Software Considerations in Airborne Systems and Equipment Certification RTCA DO-178C

The Radio Technical Commission for Aeronautics (RTCA) is a private, non-profit organization that supports the Federal Aviation Administration (FAA) through public-private partnerships to develop recommendations on a range of civil aviation issues. Its efforts to develop guidelines for producing aviation software systems that would meet flight certification requirements are maintained in "Software Considerations in Airborne Systems and Equipment Certification," DO-178 [90] [31]. This includes the software that interacts with aircraft engines, propellers, auxiliary power units, etc.; DO-178 applies to the software written for CPS. The guidelines are meant to be used during the software development lifecycle (requirements generation, design, coding, and integration) as well as other ancillary processes (verification, configuration management, quality assurance, and certification liaison). These guidelines can potentially be adopted for the development of resilient and secure operational energy system software.

The tables in Appendix A of DO-178 outline the various process steps that need to be taken in each of the phases just listed for each software level and to what degree of rigor (at applicants discretion, should be satisfied, and satisfied with independence). The different software levels are determined by that piece of software's potential aircraft failure conditions, outlined in Table 9-2. One example is that for Software Levels A & B, independent verification should occur that the software algorithm calculations are accurate, however for Software Level C internal verification is sufficient. Another is that for Software Level A, independent verification should concur that the verification tests cover all low-level software requirements, however for Software Levels B & C internal verification of the verification test coverage is sufficient.

Table 9-2 A summary of the software failure condition categories and their associated software levels [31].

Failure Condition	Software Level	Description
Catastrophic	A	Failure conditions would result in multiple fatalities, usually with the loss of the airplane.
Hazardous	B	Failure conditions would reduce the capability of the airplane or the flight crew to cope with adverse operating conditions to the extent that there would be: • A large reduction in safety margins or functional capabilities; • Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely, or • Serious or fatal injury to a relatively small number of the occupants other than the crew.

Major	C	Failure conditions would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be: • A significant reduction in safety margins or functional capabilities; • A significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or • Physical distress to passengers or cabin crew, possibly including injuries.
Minor	D	Failure conditions which would not significantly reduce airplane safety, and which involve crew actions that are well within their capabilities.
No Safety Effect	E	Failure conditions that would have no effect on safety.

In addition to outlining the necessary process steps to meet the safety certification requirements for civil aviation CPS software development, DO-178 also outlines some recommended software architecture best practices that would help limit the impacts of any faults. These practices are also extensible to limiting the impact of any malicious cyber intrusion or activity as should also be considered a form of cyber-physical security. The first is the concept of partitioning: isolating different software components from one another as much as is feasible to help contain any faults within the overall software. This is typically done by isolating software components around the interface with unique hardware components and minimizing the commands and data that can be passed between them to the bare minimum. The second is the concept of multiple-version dissimilar software or software diversity: having more than one software component complete the same function but using fundamentally different methods. The ability to compare the performance of multiple dissimilar pieces of software helps to isolate potential errors. Using multiple-version dissimilar software during operation by comparing their respective outputs can help head off and isolate malicious cyber activity because it now requires the attacker to learn how to manipulate multiple software components simultaneously to produce the desired fault. The third is that monitoring processes, whether in hardware, software, or a combination of the two, should be implemented for critical software functions to identify when errors have occurred so that they can be corrected.

Other sections of the document worth mentioning are those that provide initial guidance on how to deal with specific potential software features and characteristics: parameter data items, user-modifiable software, commercial-of-the-shelf (COTS) software, option-selectable software, and field-loadable software. Parameter data items covered include configuration tables and databases and they should be assigned the same Software Level from Table 9-2 as highest level software component that uses it. User-modifiable software entails those sections of code where a user would actually be able to manipulate them in the field without subsequent certification, and the document primarily focuses on proving how those software components would not be able to negatively impact safety (or security). Option-selectable software refers to the ability for the user to effectively deactivate sections of code based on the options he or she selects and verifying that her or she would not be able to accidentally (or purposefully) disable the software using

unaccounted for option combinations. The section of field-loadable software is concerned with ensuring that the certified software would be able to protect itself from incorrectly configured, corrupted, or malicious code that a user or cyber attacker attempts to install while the system is deployed.

9.18 Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC)

The primary organization of interest for the DoD operational energy community within the Department of Homeland Security (DHS) is the National Cybersecurity and Communications Integration Center (NCCIC) [91]. This organization has effectively taken the place of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [29]. The organization performs the following activities:

- Respond to and analyze control systems-related incidents
- Conduct vulnerability, malware, and digital media analysis
- Provide on-site incident response services
- Provide actionable intelligence
- Coordinate responsible disclosure of vulnerabilities and their associated mitigations
- Share and coordinate vulnerability information and threat analysis by producing informational products and community alerts.

In the course of performing these activities, NCCIC partners with law enforcement and intelligence agencies while coordinating across all levels of government plus with ICS owners, operators, and vendors. They also provide a number of services for the ICS community, all of which do not involve granting DHS direct access to the ICS network [92]:

- Advanced Analytical Laboratory (AAL) to conduct the vulnerability, malware, and digital media analysis, etc.
- Cyber Security Evaluation Tool (CSET), a desktop software that allows ICS owners to perform a self-assessment of their ICS network and architecture against applicable standards
- Design Architecture Reviews (DAR) can be requested to have an NCCIC team perform a 2-3 day comprehensive technical review of the network architecture and components
- Network Architecture Verification and Validation (NAVV) efforts leverage and NCCIC team to passively analyze the ICS network data and traffic to identify behavioral baselines, high value assets, etc.

As a result of their combined activities, NCCIC released annual vulnerability coordination reports; the 2016 report shows a steady increase in the number of vulnerability tickets opened by the community, approximately around 400 over the past two years [38]. However, by leveraging an automated scanning tool in 2016 they discovered over 2,000 distinct vulnerabilities. The most frequently reported vulnerability, by far, is a stack-based buffer overflow. Based on all of their activities, they have released a document advising the community on its recommended Defense-in-Depth practices across an entire organization that utilizes ICS networks [20]. They have also released a document that can be used by capability developers as a one-stop shop reference for

language to use and questions to ask of suppliers and vendors of ICS [93]. The NCCIC also provide more active technical assessments and testing of an ICS network, including vulnerability scanning, penetration testing, and database testing; those services are provided by the National Cybersecurity Assessment and Technical Services (NCATS) team [94].

9.19 Anomaly Detection of Cyber-Physical Systems (ADCPS)

The Anomaly Detection of Cyber-Physical Systems (ADCPS) project, partially funded by the Office of Naval Research (ONR), is a collaboration between the United States Military Academy (USMA) at West Point, United States Naval Academy (USNA) at Annapolis, Idaho National Laboratory (INL), the Army Communications-Electronics Research, Development, and Engineering Center (CERDEC), the United Stated Air Force Academy (USAFA), and the Army Research Laboratory (ARL) [95, 96]. The aim is to develop state estimation capabilities for cyber-physical systems to enable IDS and IPS. Initial efforts will focus on developing open systems models of the transient system dynamics of the microgrid test beds at USMA, USNA, USAFA, ARL, and INL. If successful, the five microgrids will be networked together for the development of anomaly detection approaches, benchmarks and metrics for anomaly detection, and sets of time and frequency event scenarios for further development.

9.20 Department of Energy (DOE) Cybersecurity for Energy Delivery Systems (CEDS) Research & Development Program

The DOE CEDS research and development program in the Office of Electricity Delivery & Energy Reliability (OE) manages the DOE's work and funding in cyber security and resiliency of ICS for utility energy systems [97, 98]. The CEDS efforts are aligned with the strategies and milestones set out in the roadmap published by the Energy Sector Control Systems Working Group (ESCSWG), a public-private partnership, on behalf of the DOE [99]. Table 9-3 outlines the strategies, their original 2011 milestones, and the goals of each strategy area.

There are a number of projects funded through the CEDS program that are of potential interest to the E&P CoI for improving the cyber security and resiliency of the CPS in intelligent operational energy systems. Some of the various projects are referenced throughout the report, but fact sheets for all of the projects can be found on the CEDS website [100].

Table 9-3 An overview of the CEDS strategies and milestones as set out by the 2011 ESCSWG Roadmap [99].

Strategies	1. Build a Culture of Security	2. Assess and Monitor Risk	3. New Protective Measures to Reduce Risk	4. Manage Incidents	5. Sustain Security Improvements
Near-Term Milestones (0-3 years; by 2013)	1.1 Executive engagement and support of cyber resilience efforts 1.2 Industry-driven safe code development and software assurance awareness workforce training campaign launched	2.1 Common terms and measures specific to each energy subsector available for baselining security posture in operational settings	3.1 Capabilities to evaluate the robustness and survivability of new platforms, systems, networks, architectures, policies, and other system changes commercially available	4.1 Tools to identify cyber events across all levels of energy delivery system networks commercially available 4.2 Tools to support and implement cyber attack response decision making for the human operator commercially available	5.1 Cyber threats, vulnerability, mitigation strategies, and incidents timely shared among appropriate sector stakeholders 5.2 Federal and state incentives available to accelerate investment in and adoption of resilient energy delivery systems
Mid-Term Milestones (4-7 years; by 2017)	1.3 Vendor systems and components using sophisticated secure coding and software assurance practices widely available 1.4 Field-proven best practices for energy delivery systems security widely employed 1.5 Compelling business case developed for investment in energy delivery systems security	2.2 Majority of asset owners baselining their security posture using energy subsector specific metrics	3.2 Scalable access control for all energy delivery system devices available 3.3 Next-generation, interoperable, and upgradeable solutions for secure serial and routable communications between devices at all levels of energy delivery system networks implemented	4.3 Incident reporting guidelines accepted and implemented by each energy subsector 4.4 Real-time forensics capabilities commercially available 4.5 Cyber event detection tools that evolve with the dynamic threat landscape commercially available	5.3 Collaborative environments, mechanisms, and resources available for connecting security and operations researchers, vendors, and asset owners 5.4 Federally funded partnerships and organizations focused on energy sector cybersecurity become self-sustaining
Long-Term Milestones (8-10 years; by 2020)	1.6 Significant increase in the number of workers skilled in energy delivery, information systems, and cybersecurity employed by industry	2.3 Tools for real-time security state monitoring and risk assessment of all energy delivery system architecture levels and across cyber-physical domains commercially available	3.4 Self-configuring energy delivery system network architectures widely available 3.5 Capabilities that enable security solutions to continue operation during a cyber attack available as upgrades and built-in to new security solutions 3.6 Next-generation, interoperable, and upgradeable solutions for secure wireless communications between devices at all levels of energy delivery system networks implemented	4.6 Lessons learned from cyber incidents shared and implemented throughout the energy sector 4.7 Capabilities for automated response to cyber incidents, including best practices for implementing these capabilities available	5.5 Private sector investment surpasses Federal investment in developing cybersecurity solutions for energy delivery systems 5.6 Mature, proactive processes to rapidly share threat, vulnerabilities, and mitigation strategies are implemented throughout the energy sector
Goals	Cybersecurity practices are reflexive and expected among all energy sector stakeholders.	Continuous security state monitoring of all energy delivery system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators.	Next-generation energy delivery system architectures provide ``defense-in-depth'' and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident.	Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment.	Collaboration between industry, academia, and government maintains cybersecurity advances.

10 References

[1] D. R. Harp and B. Gregory-Brown, "IT/OT Convergence: Bridging the Divide," NexDefense, Inc..

[2] National Science Foundation, "Program Solicitation NSF 17-529: Cyber-Physical Systems (CPS)," 2017. [Online]. Available: https://www.nsf.gov/pubs/2017/nsf17529/nsf17529.pdf.

[3] R. Satter, "Researchers discover Russia-linked power grid-wrecking software," 12 June 2017. [Online]. Available: https://www.fifthdomain.com/home/2017/06/12/russian-hackers-possess-malware-capable-of-disrupting-us-electrical-systems/.

[4] A. Cherepanov, "WIN32/INDUSTROYER: A new threat for industrial control systems," ESET, 12 June 2017. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.

[5] Dragos, Inc., "CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations," 13 June 2017. [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf.

[6] A. Greenberg, "'Crash Override': The malware that took down a power grid," 12 June 2017. [Online]. Available: https://www.wired.com/story/crash-override-malware/?mbid=nl_61217_p3&CNDID=31272795.

[7] C. Baraniuk, "Hackers 'could target electricity grid' via solar panel tech," 8 August 2017. [Online]. Available: http://www.bbc.com/news/technology-40861976.

[8] N. Perlroth, "Hackers are targeting nuclear facilities, homeland security dept. and F.B.I. say," 6 July 2017. [Online]. Available: https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?_r=0.

[9] 114th United States Congress, *National Defense Authorization Act for Fiscal Year 2016,* Washington, D.C., 2015.

[10] Tactical Microgrid Standards Consortium, "Emerging Interoperability Standardization of Tactical Microgrids," in *Operational Energy Summit*, Arlington, VA, 2017.

[11] M. Mickelson and S. Damordaran, "MITRE Cyber Resilient Systems Prototyping and Engineering (CRSPE)," The MITRE Corporation, 2017.

[12] J. Douglas and R. Ford, "How attackers used human error to hack the power grid [Commentary]," 7 September 2017. [Online]. Available: https://www.fifthdomain.com/opinion/2017/09/07/how-attackers-used-human-error-to-hack-the-power-grid-commentary/.

[13] W. J. I. Lynn, *DoD Directive 3020.40: DoD Policy and Responsibilities for Critical Infrastructure,* U.S. DoD, 2010.

[14] K. Jabbour and S. Muccio, "On Mission Assurance," in *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, CRC Press, 2013.

[15] K. Jabbour and S. Muccio, "The Science of Mission Assurance," *Journal of Strategic Security,* vol. 4, no. 2, pp. 61-74, Summer 2011.

[16] U.S. DoD, "Military Standard - Aircraft Internal Time Devision Command/Response Multiplex Data Bus, MIL-STD-1553b," 1975. [Online]. Available: http://ams.aeroflex.com/pagesproduct/appnotes/MILSTD1553b.pdf.

[17] K. Jabbour and J. Poisson, "Cyber Risk Assessment in Distributed Information Systems," *Cyber Defense Review*, pp. 79-100, Spring 2016.

[18] Computer Science Division: Information Technology Laboratory, "NIST Special Publication 800-30 Rev 1: Guide for Conducting Risk Assessments," National Institute of Standards and Technology, Gaithersburg, MD, 2012.

[19] Wikipedia, "Shodan (website)," [Online]. Available: https://en.wikipedia.org/wiki/Shodan_(website). [Accessed 5 October 2017].

[20] DHS Control Systems Security Program, "Common Cybersecurity Vulnerabilities in Industrial Control Systems," 2011.

[21] W. Young and N. Leveson, "Systems thinking for safety and security," in *29th Annual Computer Security Applications Conference*, New York, New York, 2013.

[22] J. Meserve, "Mouse click could plunge city into darkness," 27 September 2007. [Online]. Available: http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.

[23] SANS Institute, "An Introduction to TEMPEST," [Online]. Available: https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981.

[24] U.S. National Security Agency, "TEMPEST," [Online]. Available: https://www.iad.gov/iad/programs/iad-initiatives/tempest.cfm. [Accessed 16 October 2017].

[25] U.S. DHS ICS-CERT, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 2016.

[26] TARDEC, "TARDEC 30-Year Strategy v3," 2017.

[27] C. K. Veitch, J. M. Henry, B. T. Richardson and D. H. Hart, "Micgrogrid Cyber Security Reference Architecture Version 1.0," Sandia National Laboratories, 2013.

[28] DHS NCCIC, "Guidelines for Application Whitelisting in Industrial Control Systems," [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf.

[29] R. Timpany, Interviewee, *DHS NCCIC.* [Interview]. 16 October 2017.

[30] DOE Office of Electricity Delivery and Energy Reliability, "Software Defined Networking (SDN) Project," May 2015. [Online]. Available: https://energy.gov/sites/prod/files/2015/12/f27/Software%20Defined%20Networking%20fact%20sheet%20May%202015.pdf. [Accessed 18 Jan 2018].

[31] RTCA, Inc., "Software Considerations in Airborne Systems and Equipment Certification: RTCA DO-178C," Washington, D.C., 2011.

[32] Office of Electricity Delivery and Energy Reliability, "A Resilient Self-Healing Cyber Security Framework for Power Grid," June 2016. [Online]. Available: https://energy.gov/sites/prod/files/2016/09/f33/ANL%20Self-Healing%20Fact%20Sheet%20September%202016.pdf. [Accessed 9 November 2017].

[33] Office of Electricity Delivery and Energy Reliability, "Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA)," September 2014. [Online]. Available: https://energy.gov/sites/prod/files/2015/12/f27/CYMSA%20fact%20sheet%20September%202014.pdf. [Accessed 9 November 2017].

[34] NNBE Benchmarking Team, "NASA/Navy Benchmarking Exchange Vol 2 Progress Report - Naval Reactors Safety Assurance," 2003.

[35] L. Pike, "Hints for High-Assurance Cyber-Physical System Design," *IEEE Cybersecurity Development*, pp. 25-29, 2016.

[36] Intermetrics, Inc. and The MITRE Corporation, "Ada Reference Manual ISO/IEC 8652:1995(E)," 2000. [Online]. Available: http://www.adaic.org/resources/add_content/standards/95lrm/ARM_HTML/RM-TTL.html. [Accessed 5 December 2017].

[37] Free Software Foundation, "GNAT (GNU Ada)," 2014. [Online]. Available: https://www.gnu.org/software/gnat/. [Accessed 5 December 2017].

[38] DHS NCCIC, "ICS-CERT Annual Vulnerability Coordination Report," 2016. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf.

[39] Synopsys, Inc., "Coverity Scan Static Analysis," [Online]. Available: https://scan.coverity.com/. [Accessed 5 December 2017].

[40] Network Design & Management, Inc., "HP Fortify," [Online]. Available: http://www.ndm.net/sast/hp-fortify. [Accessed 5 December 2017].

[41] Common Criteria Recognition Arrangement Signatories, "The Common Criteria," [Online]. Available: http://www.commoncriteriaportal.org/. [Accessed 30 October 2017].

[42] Software Engineering Institute, "Cyber-Physical Systems: Overview," Carnegie Mellon University, [Online]. Available: https://www.sei.cmu.edu/cyber-physical/. [Accessed 1 November 2017].

[43] S. S. Brilliant, J. C. Knight and N. G. Leveson, "Analysis of faults in an N-version software experiment," 1 February 1990. [Online]. Available: https://ntrs.nasa.gov/search.jsp?R=19900041359. [Accessed 5 December 2017].

[44] Y. Yeh, "Safety critical avionics for the 777 prmiary flight controls system," in *20th IEEE Digital Avionics Systems Conference*, 2001.

[45] B. Freeman, "A New Defense for Navy Ships: Protection from Cyber Attacks," Office of Naval Research, 17 September 2015. [Online]. Available: https://www.onr.navy.mil/en/Media-Center/Press-Releases/2015/RHIMES-Cyber-Attack-Protection.aspx. [Accessed 18 January 2018].

[46] Office of Electricity Delivery and Energy Reliability, "Artificial Diversity and Defense Security (ADDSec)," May 2016. [Online]. Available: https://energy.gov/sites/prod/files/2016/09/f33/SNL%20ADD%20Sec%20Fact%20Sheet%20September%202016.pdf. [Accessed 9 November 2017].

[47] D. Bodeau and R. Graubart, "Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines," 2017. [Online]. Available: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf.

[48] NIST Information Technology Laboratory, "Common Vulnerability Scoring System," [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss. [Accessed 5 December 2017].

[49] Information Design Assurance Red Team, "The IDART Methodology," Sandia National Laboratories, [Online]. Available: http://www.idart.sandia.gov/methodology/IDART.html. [Accessed 1 November 2017].

[50] The MITRE Corporation, "Systems Engineering Guide," 2014. [Online]. Available: https://www.mitre.org/publications/technical-papers/the-mitre-systems-engineering-guide.

[51] S. Musman, A. Temin, M. Tanner, D. Fox and B. Pridemore, "Evaluating the Mission Impact of Cyber Attacks on Missions," 2010. [Online]. Available: https://www.mitre.org/sites/default/files/pdf/09_4577.pdf.

[52] S. Musman and A. Temin, "A cyber mission impact assessment tool," in *IEEE International Symposium on Technologies for Homeland Security*, 2015.

[53] G. D. Wyss, J. F. Clem, J. L. Darby, K. Dunphy-Guzman, J. P. Hinton and K. W. Mitchiner, "Risk-Based Cost-Benefit Analysis for Security Assessment Problems," in *IEEE International Carnahan Conference on Security Technology (ICCST)*, 2010.

[54] The MITRE Corporation, "Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Matrix," [Online]. Available: https://attack.mitre.org/w/index.php?title=Main_Page&oldid=1345. [Accessed 3 November 2017].

[55] L. A. J. Cox, "What's wrong with rick matrices?," *Risk Analysis*, vol. 28, no. 2, pp. 497-512, 2008.

[56] S. K. Damodaran and S. Mittal, "Modeling cyber effects in cyber-physical systems with DEVS," in *Proceedings of the Symposium on Theory of Modeling & Simulation by the Society for Computer Simulation International*, 2017.

[57] S. K. Damodaran and S. Mittal, "Controlled environments for cyber risk assessment of cyber-physical systems," in *Proceedings of the Summer Simulation Multi-Conference by the Society for Computer Simulation International*, 2017.

[58] R. Thomas, "Cyber-Physical Systems Security Testing and Evaluation Using Model-based Engineering (The SCAPS Project)," The MITRE Corporation, McLean, VA, 2017.

[59] J. Ferraro, "Embedded Systems Security: Avionics Platforms Example for Cyber Resiliency Evaluation and Experimentation," The MITRE Corporation, Bedford, MA, 2017.

[60] W. W. Anderson, "Technology Transition Final Public Report, Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS), Joint Capability Technology Demonstration (JCTD) Version 1.0," Naval Facilities Engineering Command, 2015.

[61] Tactical Microgrid Standards Consortium, *TMSC Updates to the EGSA Government Relations Committee,* 2017.

[62] C. Hsu and C. Miller, Interviewees, *Discussion on NRECA Cybersecurity Research & Development Efforts.* [Interview]. 16 May 2017.

[63] C. Miller, M. Martin, D. Pinney and G. Walker, "Achieving a Resilient and Agile Grid Ver 1.0," NRECA, Arlington, VA, 2014.

[64] NRECA Business & Technology Strategies, "Portfolio of Business and Technology Projects, Products, and Services," April 2017. [Online]. Available: https://www.cooperative.com/public/bts/Documents/bts_portfolio.pdf.

[65] NRECA, "NRECA Announces Team for REACT Cybersecurity Project," 24 February 2017. [Online]. Available: https://www.electric.coop/nreca-announces-team-for-react-cybersecurity-project/. [Accessed 26 May 2017].

[66] R. Richards, "High Assurance Cyber Military Systems (HACMS)," in *NDIA Cyber Resilient & Secure Weapons Systems Summit*, 2017.

[67] R. Richard, "High-Assurance Cyber Military Systems (HACMS)," Defense Advanced Research Projects Agency, [Online]. Available: http://www.darpa.mil/program/high-assurance-cyber-military-systems. [Accessed 2017 June 5].

[68] Defense Advanced Research Projects Agency, *Broad Agency Announcement: High-Assurance Cyber Military Systems (HACMS) - Amendment 1*, 2012.

[69] R. Richards, "Cyber Assured Systems Engineering (CASE)," Defense Advanced Research Projects Agency, [Online]. Available: https://www.darpa.mil/program/cyber-assured-systems-engineering. [Accessed 8 December 2017].

[70] Defense Advanced Research Projects Agency, "Cyber Assured Systems Engineering (CASE) Solicitation Number HR001117S0033," 13 June 2017. [Online]. Available: https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=f9b07c2e52646d521922318ac40b5136&_cview=1. [Accessed 8 December 2017].

[71] Defense Advanced Research Projects Agency, *Broad Agency Announcement: Rapid Attack Detection, Isoluation, and Characterization Systems (RADICS), DARPA-BAA-16-14, Amendment 2*, 2016.

[72] P. Fairley, "Sniffing out grid attacks: A $77 million DARPA program is building automated cyberdefenses for power grids," 22 July 2016. [Online]. Available: http://spectrum.ieee.org/energy/the-smarter-grid/sniffing-out-grid-attacks.

[73] UK Ministry of Defense, "Defence Standard 23-13 Part 1 Generic Base Architecture : Approach," 2014.

[74] UK Ministry of Defense, " Defense Standard 23-09 Part 1 Generic Vehicle Architecture Infrastructure," 2013.

[75] UK Ministry of Defense, "Defence Standard 23-12 Generic Soldier Architecture," 2013.

[76] ROS.org, "Documentation," 31 March 2017. [Online]. Available: http://wiki.ros.org/. [Accessed 1 June 2017].

[77] B. Gerkey, "Why ROS 2.0?," [Online]. Available: http://design.ros2.org/articles/why_ros2.html. [Accessed 1 June 2017].

[78] Open Source Robotics Foundation, "SROS," 9 August 2016. [Online]. Available: http://wiki.ros.org/SROS. [Accessed 1 June 2017].

[79] M. Mazzara, "RAS-G IOP Update," in *NDIA Robotics DivisionDecember*, 2016.

[80] J. Joyce, "Navy coalition building cybersafe USS Secure to protect fleet warships and weapon systems," Jan-Mar 2016. [Online]. Available: http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=7461.

[81] M. Iriarte, "Navy signs agreement with Purdue University to develop cybersecure energy storage systems," 17 August 2017. [Online]. Available: http://mil-embedded.com/news/navy-signs-agreement-with-purdue-university-to-develop-cybersecurity-energy-storage-systems/.

[82] Object Management Group, "Data Distribution Service (DDS) Version 1.4," 2015.

[83] Object Management Group, "The Real-time Publish-Subscribe Protocol (RTPS) DDS Interoperability Wire Protocol Specification Version 2.2," 2014.

[84] Object Management Group, "DDS Security Version 1.0," 2016.

[85] Program Executive Officer Land Systems, "Open Plug-and-Play Communications Architecture," 2016.

[86] P. Welsh, "AF looks to ensure cyber resiliency in weapons systems through new office," 4 January 2017. [Online]. Available: http://www.af.mil/News/Article-Display/Article/1041426/af-looks-to-ensure-cyber-resiliency-in-weapons-systems-through-new-office/.

[87] D. Holtzman, "Cyber Resiliency Office for Weapon Systems (CROWS)," in *NDIA Cyber Resilient & Secure Weapon Systems Summit*, McLean, VA, 2017.

[88] W. Young and N. Leveson, "Systems thinking for safety and security," in *Proceedings of the 29th Annual Computer Security Applications Conference*, New York, NY, USA, 2013.

[89] C. Schmittner, Z. Ma and P. Puschner, "Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis," in *International Conference on Computer Safety, Reliability, and Security*, 2016.

[90] U.S. Department of Transportation Federal Aviation Administration, "Advisory Circular No. 20-115C," Washington, D.C., 2013.

[91] DHS NCCIC, "Industrial Control Systems Cyber Emergency Response Team Fact Sheet," [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICS-CERT_S508C.pdf.

[92] DHS NCCIC, "NCCIC/ICS-CERT Assessment FAQs," [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/NCCIC%20ICS-CERT%20Assessment%20FAQ_S508C.pdf.

[93] DHS National Cyber Security Division Control Systems Security Program, "Cyber Security Procurement Language for Control Systems," 2009. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf.

[94] DHS NCCIC, "National Cybersecurity Assessment and Technical Services Team," [Online]. Available: https://www.lba.org//files/DHS_NCATS_Fact_Sheet_2014.pdf.

[95] J. James, M. Lanham, F. Mabry, T. Cook, A. St. Leger, D. Opila and K. Kiriakides, "Anomaly Detection of Cyber-Physical Systems," in *MORS Symposium*, 2017.

[96] J. James, Interviewee, *Anomaly Detection of Cyber-Physical Systems research efforts.* [Interview]. 1 Februrary 2018.

[97] Office of Electricity Delivery & Energy Reliability, "Cybersecurity Research, Development and Demonstration for Energy Delivery Systems," U.S. Department of Energy, [Online]. Available: https://energy.gov/oe/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and. [Accessed 9 November 2017].

[98] C. Hawk, "Cybersecurity for Energy Delivery Systems (CEDS) R&D: Following the Energy Sector's Roadmap," 2016.

[99] Energy Sector Control Systems Working Group, "Roadmap to Achieve Energy Delivery Systems Cybersecurity," Critical Infrastructure Partnership Advsiory Council, 2011.

[100] Office of Electricity Delivery & Energy Reliability, "Cybersecurity for Energy Delivery Systems Fact Sheets," U.S. DOE, [Online]. Available: https://energy.gov/oe/downloads/cybersecurity-energy-delivery-systems-ceds-fact-sheets. [Accessed 9 November 2017].

[101] Software Engineering Institute, "Process & Performance Overview," Carnegie Mellon University, [Online]. Available: https://www.sei.cmu.edu/process/. [Accessed 1 November 2017].

This page intentionally left blank.

Appendix A Abbreviations and Acronyms

AADL	Architecture Analysis And Design Language
ADCPS	Anomaly Detection For Cyber-Physical Systems
ADDSec	Artificial Diversity And Defense Security
AFRL	Air Force Research Labs
ARL-PSU	Applied Research Laboratories At Pennsylvania State University
ASD(R&E)	Assistant Secretary Of Defense For Research & Engineering
BMS	Battery Management System
C2	Command And Control
C4I	Command, Control, Communication, Computers and Intelligence
C4ISR	C4I, Surveillance, and Reconnaissance
CAPEC	Common Attack Pattern Enumeration And Classification
CEDS	Cybersecurity For Energy Delivery Systems
CERDEC	Communications-Electronics Research, Development, And Engineering Center
CGSD	Common Grid State Database
CJA	Crown Jewels Analysis
CMIA	Cyber Mission Impact Assessment
CMU SEI	Carnegie Mellon University Software Engineering Institute
COTS	Commercially Off-The-Shelf
CP&I	Command, Power, And Integration
CPS	Cyber-Physical Systems
CROWS	Cyber Resiliency Office For Weapon Systems
CSSP	Control Systems Security Program
CVE	Common Vulnerabilities And Exposures
CWB	Conformal Wearable Batteries
CWE	Common Weakness Enumeration
CYMSA	Cyber-Physical Modeling And Simulation For Situational Awareness
DARPA	Defense Advanced Research Projects Agency
DC	Direct Current
DCPS	Data-Centric Publish-Subscribe

DDS	Data-Distribution Service
DHS	U.S. Department Of Homeland Security
DMZ	Demilitarized Zones
DoD	Department Of Defense
DOE	Department Of Energy
DoS	Denial Of Service
E&P CoI	Energy & Power Community Of Interest
ECU	Electronic Control Unit
EIO	Energy Informed Operations
EMS	Energy Management System
EOP	Energy Optimized Platforms
FFDC	Federally Funded Research And Development Center
GBA	Generic Base Architecture
GenSets	Combustion Engine And Electric Generator Combinations
GSA	Generic Soldier Architecture
GVA	Generic Vehicle Architecture
HACMS	High-Assurance Cyber Military Systems
HMI	Human Machine Interface
HUMS	Health and Usage Monitoring System
IA	Information Assurance
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDART	Information Design Assurance Red Team
IDS	Intrusion Detection System
IEB	Information Exchange Boundary
INL	Idaho National Laboratory
IPD	Intelligent Power Distribution
IPERC	Intelligent Power & Energy Research Corporation
IPS	Intrusion Prevention Systems
IT	Information Technology
JCTD	Joint Capability Technology Demonstration

LAN	Local Area Network
LOSA	Land Open Systems Architecture
MA	Mission Assurance
MBSSE	Model-Based Systems Security Engineering
MEF	Mission Essential Functions
METT-TC	Mission, Enemy, Terrain, Troops Available, Time, And Civilian Considerations
MOD	Ministry of Defense
MOTS	Military Off-The-Shelf
MTVR	Medium Tactical Vehicle Replacement
NCCIC	National Cybersecurity And Communications Integration Center
NDAA	National Defense Authorization Act
NRECA	National Rural Electric Cooperative Association
NRTC	National Rural Telecommunications Cooperative
NSA	U.S. National Security Agency
OE	Office Of Electricity Delivery & Energy Reliability
OMG	Object Management Group
OPR	Office Of Principal Responsibility
OT	Operational Technology
PD SS&I	Project Director For Soldier Systems And Integration
PEO Soldier	Program Executive Office Soldier
PLCs	Programmable Logic Controllers
PM SWAR	Product Manager Soldier Warrior
PNT	Positioning, Navigation, And Timing
RADICS	Rapid Attack Detection Isolation & Characterization Systems
ROS	Robot Operating System
RRA	Risk Remediation Assessment
RTPS	Real-Time Publish Subscribe
S&T	Science And Technology
SA	Situational Awareness
SCADA	Supervisory Control And Data Acquisition
SCAPS	Cyber Security And Risk Analysis Workbench For CPS

SDN	Software-Defined Networking
SDR	Dismounted Soldiers
SMBus	System Management Communications Bus
SMEs	Subject Matter Experts
SNL	Sandia National Laboratory
SOC	State-Of-Charge
SPI	Service Plugin Interface
SPIDERS	Smart Power Infrastructure Demonstration for Energy Reliability and Security
SROS	ROS-Secure
SUT	System Under Test
SWAP	Size, Weight, And Power
TARDEC	Tank Automotive Research, Development, And Engineering Center
TLS	Transport Layer Security
TMG	Tactical Microgrids
TMS	Thermal Management System
TMSC	Tactical Microgrid Standards Consortium
TSA	Threat Susceptibility Assessment
TTPs	Tactics, Techniques, And Procedures
U.S.	United States
UK	United Kingdom
USAF	U.S. Air Force
USB	Universal Serial Bus
US-CERT	Us Computer Emergency Readiness Team
USMC	U.S. Marine Corps
VLAN	Virtual Local Area Networks

This page intentionally left blank.