Control Systems Cyber Security Reference Architecture (RA) for Critical Infrastructure: Healthcare and Hospital Vertical Example

Aleksandra Scalco,[1, 2] David Flanigan,[3] Steven Simske[4]

[1] Engineer, Naval Information Warfare Center (NIWC) Atlantic

[2] Corresponding Author, aleksandrascalco@gmail.com

[3] Principal Professional Staff, Johns Hopkins University Applied Physics Laboratory

[4] Professor of Systems Engineering, Colorado State University

[*see Author Capsule Bios below*]

Abstract

A reference architecture (RA) provides a common frame of reference with a common vocabulary, reusable designs, and principles that may be applied to future architectures. It can promote re-use of best practices, improve interoperability, and improve awareness of a system under development of the same mindset. The next version of the Department of Defense (DoD) Chief Information Officer (CIO) Cyber Security Reference Architecture (CSRA) will include an appendix for control systems. It provides a frame of reference for cybersecurity implementations based on generalizations of common principles that can provide a starting point for an organization's architecture effort, inform decision-making, suggest governance, and help define future policy decisions for control systems. The appendix is based on the outcome of the MOSIACS Joint Capability Technology Demonstration (JCTD), which provides the initial cyber defensive capability framework for integrations of Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) components to form a control system cyber defensive solution. The MOSAICS capability was successfully demonstrated in the energy sector critical infrastructure vertical on a power system in August 2021. Its applicability embodied delivery methods for technologies in other essential infrastructure sectors, repeatable playbooks for automated Courses of Action (COA), best practices, and templates for cyber security requirements for control systems. The advantages of the RA are to enable better decision-making and policy-making support about cybersecurity for control systems. This paper demonstrates the RA used in the Healthcare and Public Health sector's critical infrastructure vertical to evaluate concepts

 doi: 10.18278/jcip.2.2.7

such as Zero Trust (ZT) and Defense-in-Depth (DiD) architecture principles related to policymaking.

Keywords: Critical Infrastructure, Control Systems, Cyber Security Reference Architecture (CSRA), Defense-in-Depth, DiD, Information Technology, IT, Internet of Things, IoT, Machine Learning, ML, MOSAICS, Policy, Reference Architecture, RA, Zero Trust, ZT

Introduction

Healthcare and hospital organizations globally are under siege by the stresses of a worldwide pandemic, migrating populations seeking healthcare, and an alarming increase in the number of cyberattacks on the healthcare infrastructure (more than doubled in 2020). Ransomware accounted for 28 percent of attacks on healthcare organizations in 2020 (Davis 2021). While finance and insurance continue to be the most targeted critical infrastructure sectors, cyber adversaries pivoted on the global pandemic to cause healthcare organizations to be the seventh-most targeted sector in 2020 (Davis 2021).

An alarming example is a 2020 ransomware attack on George Washington University Hospital that forced the hospital to shift its networks offline (Glick 2021). The hospital staff could not process new admissions. Physicians and staff diverted ambulances to other facilities and were forced to rely on old paper files. Last year, a clinic in Düsseldorf, Germany, blamed the death of a patient on a system compromised by a cyberattack. The patient was transported to another facility and passed away after experiencing an aneurysm that required immediate treatment (Glick 2021).

The increase of ransomware activity targeting the Healthcare and Public Health Sector led to a joint cybersecurity advisory coauthored by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (DHHS) in 2020 (Cybersecurity and Infrastructure Security Agency (CISA) 2020). The advisory highlighted TrickBot and BazarLoader malware that can lead to healthcare service disruption and the substantial organizational challenge of addressing the cybersecurity risk during a global pandemic. The rise in the prevalence of malware ransomware attacks on healthcare infrastructure demonstrates the vulnerability of vital patient services to cybersecurity threats. Further, it highlights the pressing need for a control systems framework for the critical infrastructure healthcare and hospital vertical to support decision-making, governance, and future policy decisions for control systems.

This paper introduces a common Reference Architecture (RA) leveraged from the Department of Defense (DOD) Chief Information Officer (CIO) Cyber

Security Reference Architecture (CSRA), which is currently in revision and that includes an appendix for control systems to defend networks from cyberattacks. This paper will apply these concepts to the healthcare domain and evaluate different strategies such as Defense-in-Depth (DiD), Zero Trust (ZT), and security orchestration and provide some thoughts on how policymakers could utilize these concepts.

Key Healthcare Network System Architecture Requirements

Healthcare and hospital organizations require reliable communication, timely and efficient data delivery, multi-node mobility, multicast technology, and energy efficiency. In addition, on-time delivery of accurate patient information is critical (Egbogah and Fapojuwo 2011). The Internet of Things (IoT) enables healthcare professionals to connect and monitor patients using near real-time sensors and equipment for remote patient monitoring. Furthermore, during the global pandemic, IoT devices offer the potential for enhanced delivery of healthcare services outside the hospital setting.

The need for speed, efficiency, low cost, and relative simplicity of maintenance leads to a single network, also known as a "flat network." Flat networks potentially increase network throughput and potential vulnerability conditions to cyberattacks. For example, many of today's healthcare and hospital organizations rely on Media Access Control (MAC) addresses to network communications in a single "flat" network segment using networking technologies such as Wi-Fi and Bluetooth found in most medical settings, as shown in Figure 1 Healthcare Single, "Flat Network," Design. This approach to a network design makes systems particularly vulnerable to potential malware attacks. A layered cyber defense security approach can be better. However, a layered approach is more expensive, challenging to maintain, and susceptible to attackers using phishing techniques (Diogenes and Ozkaya 2019).

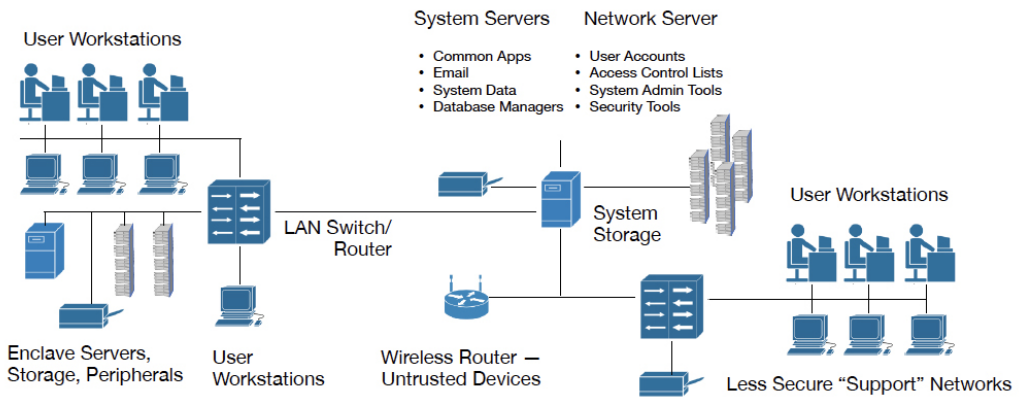

Figure 1. Healthcare Single, "Flat Network," Design

Monitoring these network connections for malware such as TrickBot and BazarLoader in any useful way is a governance challenge for any organization. The increased bandwidth of a flat network is realized when traditional firewall and access-list controls are removed from the Layer 3 routing, moving filters and connections to the lower Layer 2 of the network (Networking 2012). An endpoint user on a workstation working in less secure support network environments may not notice system infection symptoms as the TrickBot or BazarLoader malware, among other examples, communicates with command-and-control tasks. The malware can spread laterally throughout the flat network design by sharing infected file attachments, as shown in Figure 2 Healthcare Single, "Flat Network," Design. As a result, any infected machine on the network can spread the malware throughout the healthcare network. The system administrator must identify the infected workstations, disconnect infected assets, patch, disable administrative shares, remove the malware, and change account credentials. Remediation is tedious and can force a hospital to shift network systems offline, costing precious patient treatment time, as demonstrated in the 2020 ransomware attack on George Washington University Hospital.

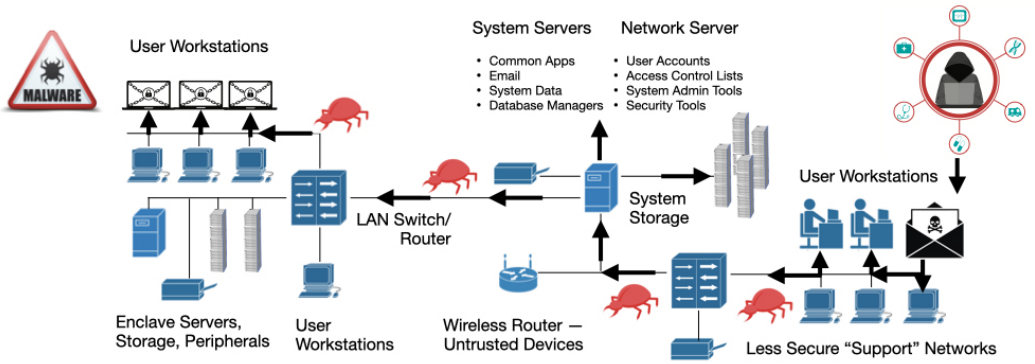

Figure 2. Healthcare Flat Network Malware Attack

Flat networks inherently permit insecurity. Introducing capabilities such as Defense-in-Depth (DiD), Zero Trust (ZT), and security orchestration strategies can reduce the estimated resources needed to secure a network (e.g., person-hours, training). For example, the median time to automatically score and publish indicators in the financial sector pilot was 1 minute, while the median time to manually score and publish indicators was 5 hours and 49 minutes. In addition, automation significantly improves total response time to indicators. For example, from the Integrated Financial Pilot performance, the entire time from generating an indicator, initiating a response, to remediating and closing a ticket was 3 hours and 7.3 minutes. The average manual process per Indicator of Compromise (IOC) was 9 hours and 59 minutes (Frick 2018).

A cost-benefit analysis might include the impacts of no control system cybersecurity. Loss of mission functions; personnel injury or loss of life; loss of as-

sets, environmental damage; economic damage due to unavailability of critical infrastructure (i.e., electrical power, water); and social by the potential loss of public confidence (Scalco 2021). Risk Identification (RI) includes asset valuation of both the quantitative (i.e., cost) and qualitative (i.e., relative importance). It includes initial and maintenance costs, significance to the organization, and a Business Impact Analysis (BIA) assessment of consequence of loss or disruption (Scalco 2021). A quantitative risk analysis starts with assigning a numerical value or cost to assets and threats in a risk analysis. This allows for a cost/benefit analysis and a clearer and concise risk characterization (Simske 2020). A governance body will want to see the estimated Return of Investment (ROI). The ROI for the capability that includes full lifecycle support might be sought through one of the critical infrastructure Information Sharing and Analysis Centers (ISAC).

Cyber Reference Architecture (RA) Concepts

An improved defense strategy uses DiD, network segmentation, ZT, and security automation. A DiD architecture strategy suggests cybersecurity at each layer in an Open Systems Interconnection (OSI) model. Network segmentation reduces the network attack surface. Zero Trust (ZT) is a network security strategy to validate everything continuously. Finally, security automation integrates security processes and tools to rapidly address threats and perform mitigations. In addition, it introduces concepts such as security automation and Machine Learning (ML) capabilities to detect attacks and handle intrusion without Subject Matter Expert (SME) human intervention (Diogenes and Ozkaya 2019). ML capabilities are integral to emerging capabilities used in DiD strategies such as security orchestration. For example, ML capability analyzes encrypted data traffic using algorithms to identify hidden threat patterns without encrypting the traffic. It can also identify malware based on known malware behaviors.

A capability integrating security automation with these RA concepts was initially piloted in the financial sector and subsequently adapted to the enterprise level and piloted in the power sector. The financial industry integrated pilot discovery phase took place from October 2017 to January 2018. The Proof-of-Concept Design Phase extended from February 2018 to April 2018, and the Execution Phase took place from April 2018 to September 2018. Technical findings of the pilot results in the financial sector indicated that the automated feed scores are consistent with the manual process, automated scores are published approximately 6 hours faster than manual process response, and the analyst time is freed to focus on threat reports with deeper context and adversary Tactics, Techniques, and Procedures (TTP) knowledge. The result was that all financial partners subsequently deployed Security Automation and integrated IOC into the SOC (Frick 2018). The capability was piloted by Munson Healthcare & Sequris Group, a 9-hospital system with 12,000 users, 28,000 network nodes, and 2,000 patient-connected devic-

es. The pilot was initiated by invitation of the Governor of Michigan for critical infrastructure cybersecurity groups to form. Subsequently, the Michigan Healthcare Cybersecurity Council was established, and Integrated Adaptive Cyber Defense (IACD) was piloted (Eder and Winn 2018).

Similarly, the power sector pilot was successfully demonstrated in August 2021 (Rich Scalco 2021). The pilot site organization plans to deploy the reference architecture to additional sites and field the capability to a different water sector. The power site pilot will be transitioned into operations at NAVFAC Southwest in 2021 and deployed at NAVFAC Hawaii in 2023, NAVFAC Mid-Atlantic, and NAVFAC Southeast in 2024 (Kilcoyne 2021). During the power site, pilot 22 attacks against the target were conducted while monitoring the entire network. "MOSAICS successfully identified 20 of the attacks for a 90.5% success rate with less than 5% false positives" (Rich Scalco 2021).

Defense-in-Depth (DiD)

Defense-in-Depth (DiD) layers and security controls at each layer are at the perimeter security layer controls implemented are application gateways and firewalls, and secure demilitarized zones (DMZs) using the same techniques employed in the network security layer; network security layer enclave partitioning security controls are built on a segment of the network defined by common security, change, and service policies; endpoint security layer controls implemented are content security (e.g., anti-virus and anti-malware) and patch management; application security layer controls are used to protect externally facing interfaces such as web application firewalls, and automated patch management; data security layer controls are implemented for data classification and data/drive encryption, and mission-critical asset layer security controls are implemented are as part of Information Technology (IT) security governance and security policies and compliance, as shown in Figure 3 Defense-in-Depth (DiD) Healthcare Architecture Design.

Network Segmentation

The idea of network segmentation is part of a DiD strategy to reduce the network attack surface. Network segmentation can be accomplished either physically or virtually. In a traditional network, all servers and workstations reside on the same Local Area Network (LAN), which allows an attacker to move laterally from one system to another. An approach to network segmentation is to 1) use cryptographic segmentation; and 2) segregate networks using application-aware defense to protect and detect functions of cybersecurity as a mitigation strategy (e.g., application-aware firewalls, Virtual Local Area Networks (VLANS), Virtual Routing and Forwarding (VRF) instances), Software Defined Networking (SDN)). SDN leverages all available technologies (i.e., VLAN and VRF). However, VLAN and VRF do not equal SDN. VLAN and VRF may be used as part of an SDN solution.

VRF is simply a technology that allows multiple routing instances to coexist on the same router (i.e., the same IP subnet can be used in numerous VRF), using different outgoing interfaces simultaneously without conflict. VRF is like a VLAN network virtualization. However, VLAN has a different IP subnet.

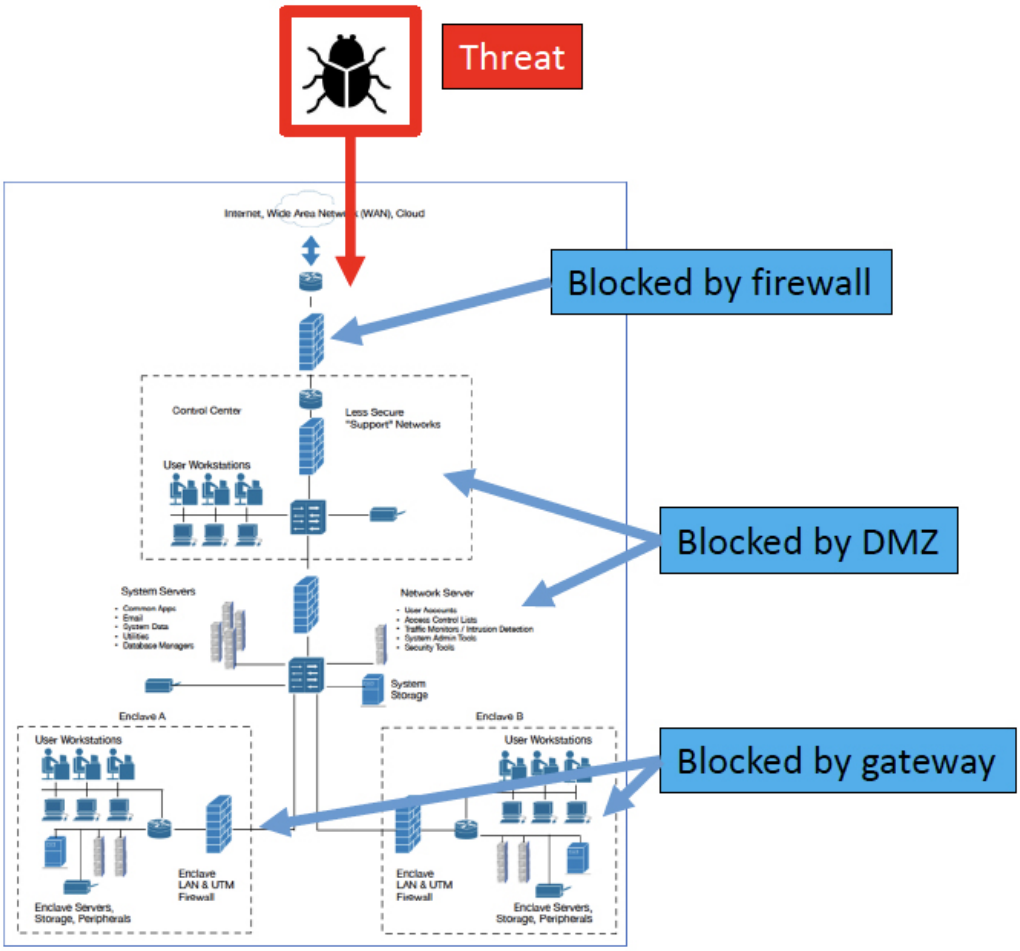

Figure 3. Defense-in-Depth (DiD) Healthcare Architecture Design

This approach can be implemented and effectively deployed on smaller, local networks, such as in the Healthcare and Public Health sector in a hospital where network security policies can be centralized in the network control plane, as shown in Figure 4 Malware Attack on a Segmented Healthcare Architecture. Application-aware network segmentation is an approach to manage cybersecurity risk and promote defense-in-depth security posture to segment network traffic within a network to reduce the attack surface. For example, the method to defend against a malware attack from traversing network boundaries is to segment the network into separate enclaves, as shown in Figure 4 Malware Attack on a Segmented Healthcare Architecture. A hospital Board of Directors (BOD) and Chief Executive Officer

(CEO) support network segmentation using application-aware defense as a deployment that blocks improperly formed network traffic and restricts content based on IT security policies. The first step is identifying all hospital assets, prioritizing critical assets, and mapping the current architecture and interfaces.

The hospital governance board directs and supports network segmentation using firewall rule sets, routing, and switching that can be used to protect a network similarly to perimeter defenses. An application-aware application approach allows network operations to be sorted according to the application or service the network traffic attempts to reach and based on specific traffic contents. How an organization implements the cybersecurity architecture depends on the organization's deployment, operational, maintenance, and sustainment strategy. The Health Information Sharing and Analysis Center (H-ISAC) is a resource for CISOs and healthcare organizations to obtain reliable risk-based decision-making, governance, and threat mitigation data. Today's organizations are connected to thousands of devices that may or may not be mapped and under configuration control. Yet there is a lack of awareness of what is on a network, a critical asset, and what needs to be prioritized in case of a breach is a problem. An approach is to identify essential assets in healthcare transactions such as patient care and life support systems, identify assets critical to healthcare business such as scheduling, administration, payroll, trace interfaces/activities to the above assets to determine and prioritize missing ancillary or rogue relationships. Governance and Leadership support are critical to addressing the challenge of identifying all critical assets. Emerging commercial tools are available on the market to help organizations identify system assets that need updates and allow the security team to prioritize vulnerability exposure. For example, a Governance policy might start with inventory and configuration control

Similarly, the Defense Health Agency (DHA) employs a Medical Community of Interest (Med-COI) security zone separation architecture, shown in Figure 5. The approach exemplifies how a RA can strengthen a healthcare and hospital network; the network is layered, providing a security zone segmentation between the operational locations and enterprise functions. The Med-COI Internet Protocol (IP) external to the Control Systems (CS) occurs at the higher levels of the security stack. Med-COI connection components are located at Level 4, the Logical Servers, and Level 5, the Enterprise Gateway. The boundary protection, or "DMZ," is at Level 3, and the system subnets, or segregated network zones, interface with the Facility Related Control Systems (FRCS) located in Levels 2 – 0. Level 0 is the non-network field control components.

Zero Trust Strategy

Zero Trust (ZT) is the antithesis of the traditional adage of "trust but verify." System owners consider everything untrusted in a ZT environment, similar to external re-

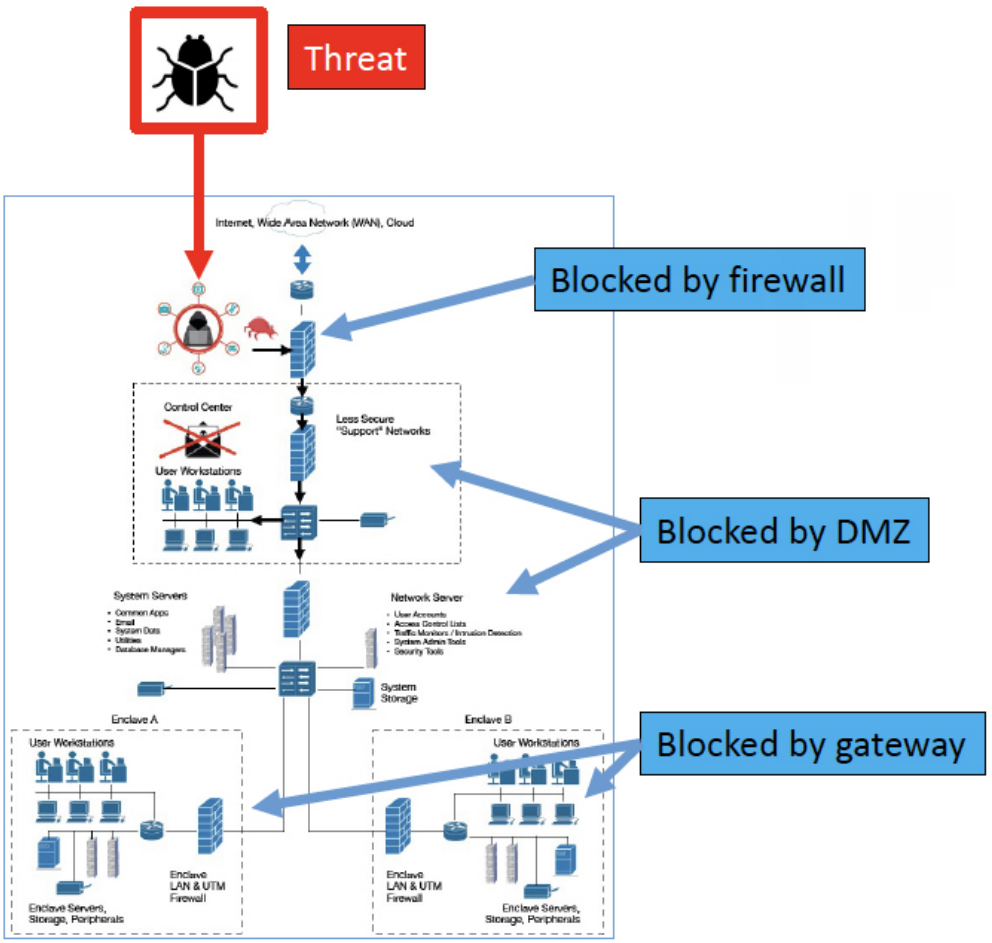

Figure 4. Malware Attack on a Segmented Healthcare Architecture

source connections (SecurID 2021). ZT is a network security strategy rather than a technology. The ZT strategy should permeate throughout the organization, from the architecture through operational processes to the culture of the professionals using connected devices on the system (Simos 2019). Everything starts from the point of a trust level of zero. That means that the trustworthiness of everything is continuously validated, from healthcare identities to applications and services used in a hospital, to connected mobile devices. Chuck Easttom and Nagi Mei propose a firmware solution of a "software shim," or code to intercept Application Program Interface (API) calls to mitigate security concerns on medical devices. The proposed solution uses existing technologies to implement security features such as maintaining an Allow and Accept List. The solution needs test for FDA compliance (Easttom and Mei 2019). Amir Djenna and Djamel Eddine Saidouni propose a new cyberattack classification for IoT-based Healthcare Infrastructure to support patient safety and connection to medical devices critical within the healthcare infrastructure (Djenna and Saidouni 2018).

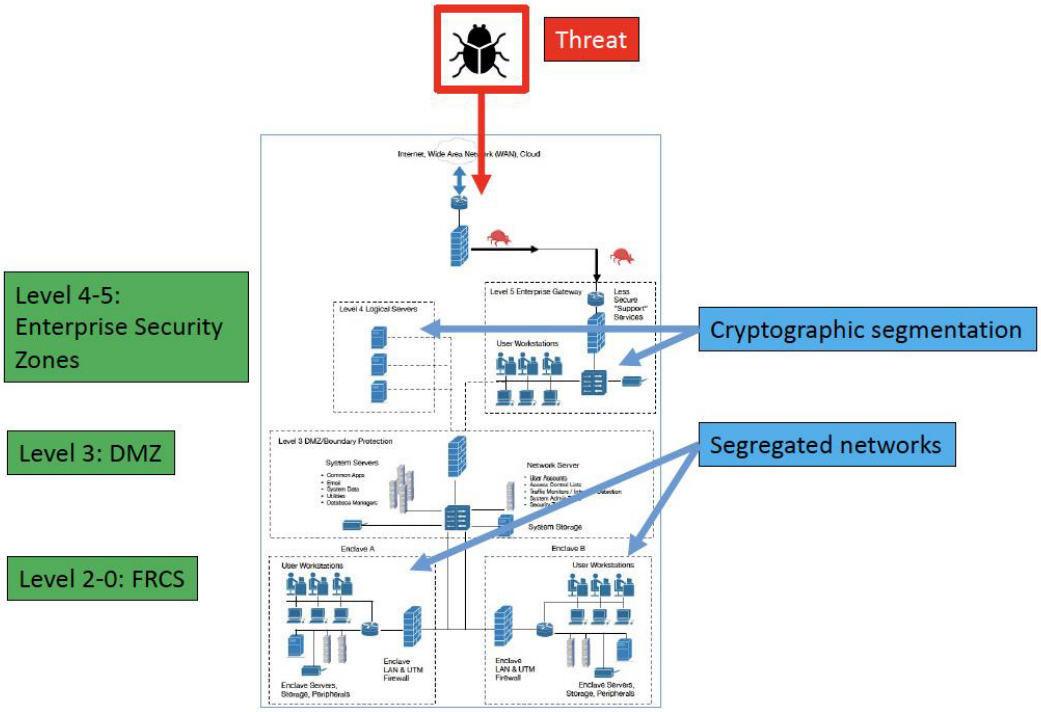

Figure 5. Malware Attack on a Segmented Med-COI Healthcare Architecture near here

The global pandemic has accelerated, enabling remote works, telemedicine, and satellite medicine practices. It has also increased ransomware attacks on healthcare and hospitals operations vulnerable to disruptions. A ZT strategy separates the control plane from external sources and uses trust algorithms to decide resource access to the network (e.g., grant, deny, or revoke). In addition, internal or external threat intelligence sources provide information about new and emerging threats that can trigger automated COAs, as found in the MOSAICS framework. Examples of threat intelligence include a user history, behavioral analytics, IP addresses, network traffic, and locations.

ZT moves the cyber defensive parameter from static perimeters to include users, assets, services, and workflows to continuous monitoring, automation, and detection response based on organizational policy and evolving threat intelligence, as shown in Figure 6 Zero Trust (ZT) Network Strategy. "The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted" (Team 2021). The ZT strategy recognizes that the prime component of a threat is not necessarily external. Insiders may also compromise the security posture intentionally (e.g., a disgruntled employee) or unintentionally (e.g., phishing attack) (Rose et al. 2020). A Zero Trust RA provides detail about core concepts and Zero Trust tenets, emerging, mandated, and active standards, and provides patterns for implementation (i.e., capability

dependencies, mapping of capabilities with operational activities, description of services mapping, operational resource flow, and operational activity model (Team 2021). "Zero Trust (ZT) is a cybersecurity strategy and framework that embeds security throughout the architecture to prevent malicious personas from accessing the most critical assets. It provides zones for visibility and information technology (IT) mechanisms positioned throughout the architecture to secure, manage and monitor every device, user, application, and network transaction occurring at the perimeter and within a network enclave. Zero Trust is an enterprise consideration and is written from the perspective of cybersecurity" (Team 2021).

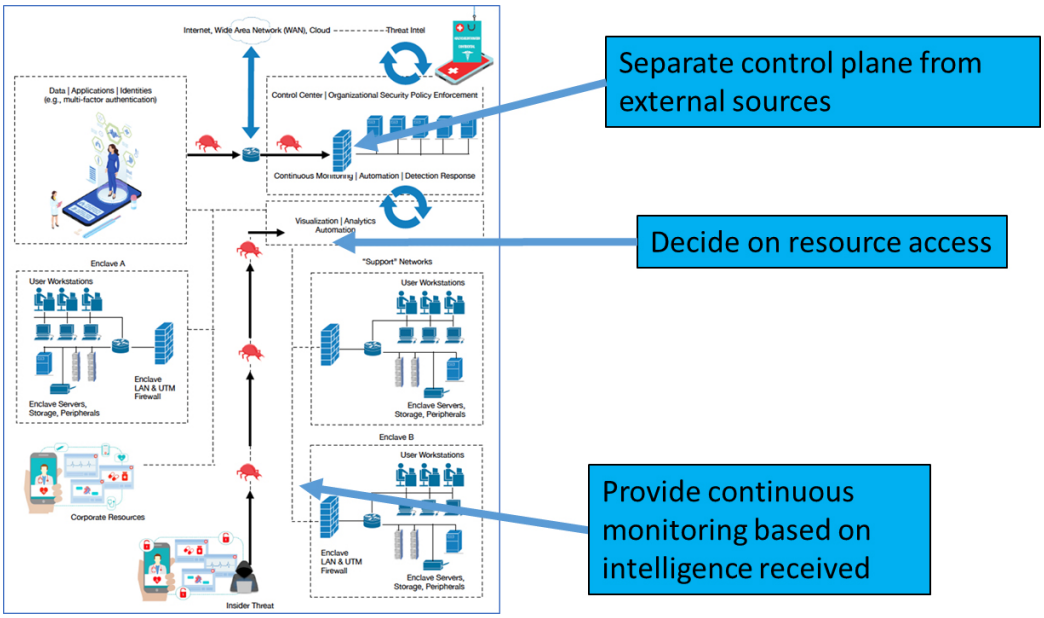

Figure 6. Zero Trust (ZT) Network Strategy

A hospital BOD can support an approach of network segmentation using application-aware defense. For example, the BOD may support a transition to a zero-trust architecture during a five-year network and application upgrade of all hospital systems. This upgrade represents a substantial resource (financial and personnel) investment that the hospital is making to protect mission-critical assets and its mission of caring for and protecting patients. Zero-trust advanced maturity model elements complement traditional DiD.

Zero-trust assumes that there are no trusted users, applications, or databases. All resources must be accessed securely using strong access controls regardless of the location, access control enforcement must be highly granular, and all network traffic must be inspected logged. Cybersecurity policies dynamically determine access driven by near real-time analytics with continuous and adaptive authentication and authorization to achieve this type of zero-trust architecture. Full micro-segmentation on an encrypted network with advanced analytics enables

automated and orchestrated threat detection and response. Other principles of how a zero-trust architecture can be implemented are utilizing just-in-time and just-enough administrative policy and privilege access workstations. All remote connections must operate without VPNs. Zero-trust elements can be enforced by the following toolsets used in the Healthcare and Public Health sectors: strong authentication by ensuring multi-factor solid authentication and session risk detection as access strategy to minimize the risk of identity compromise; policy-based adaptive access by defining acceptable access policies for resources and enforcement with consistent security policy; moving beyond the simple centralized network-based perimeter to comprehensive and distributed segmentation using software-defined micro-perimeters; investing in automate alerting and remediation to reduce Mean Time To Respond (MTTR) to attacks; using Artificial Intelligence (AI) to detect and respond to access anomalies in near real-time; and using data classification and protection to discover, classify, protect, and monitor sensitive data to minimize exposure from malicious or unintentional (accidental) exfiltration.

Security Automation and Orchestration

Security automation uses technology to integrate security processes, applications, and infrastructure. Security orchestration can then integrate existing security tools to address incidents and perform mitigations. The forthcoming DOD CIO CSRA Appendix D Control Systems Cyber Defense Reference Architecture (CSCDRA) introduces concepts of Zero Trust (ZT). In addition, it offers a better network design framework for use in critical infrastructure verticals by the MOSIACS Joint Capability Technology Demonstration (JCTD) to provide an initial cyber defensive capability framework for integrations of components from a control system cyber defensive solution. The MOSAICS capability offers security automation and recommended commercial products and services integrations in a RA reusable design to reduce Mean Time to Respond (MTTR) to attacks. MOSAICS is an integration of security tools and disparate systems to support security automation that prioritizes and drives response actions based on a pre-defined "Playbook" or "workflow." The security orchestration manages alerts and performs integrity checks against the detection of anomalies outside the system network boundaries, as shown in Figure 5 MOSAICS framework.

The template solution for the architecture was successfully demonstrated in the energy sector critical infrastructure vertical on a power system in August 2021. Its applicability embodied delivery methods for technologies in other essential infrastructure sectors, repeatable playbooks for automated Courses of Action (COA), best practices, and templates for cyber security requirements for control systems harmonized with concepts such as Zero Trust (ZT) and Defense-in-Depth (DiD) architecture principles related to policymaking. In addition, MOSAICS introduces Security Orchestration, Automation, and Response (SOAR) capability to

collect threat data and alerts from various security tools and disparate systems to support automation sequences for network defense. The automation sequences, known as "playbooks," provide immediate response efficiency for network operations and a consistent process to help administrators investigate and prioritize alert response actions (Rich Scalco 2018). SOAR is a technology. ZT pertains to framework principles. MOSAICS is an integrated, system-engineered solution that leverages SOAR technology and ZT principles to deliver a capability. This approach is a plan to find optimal network security using best practices for control systems. When paired with solutions such as MOSAICS, such an architecture offers a complete package for expeditious and economical implementation.

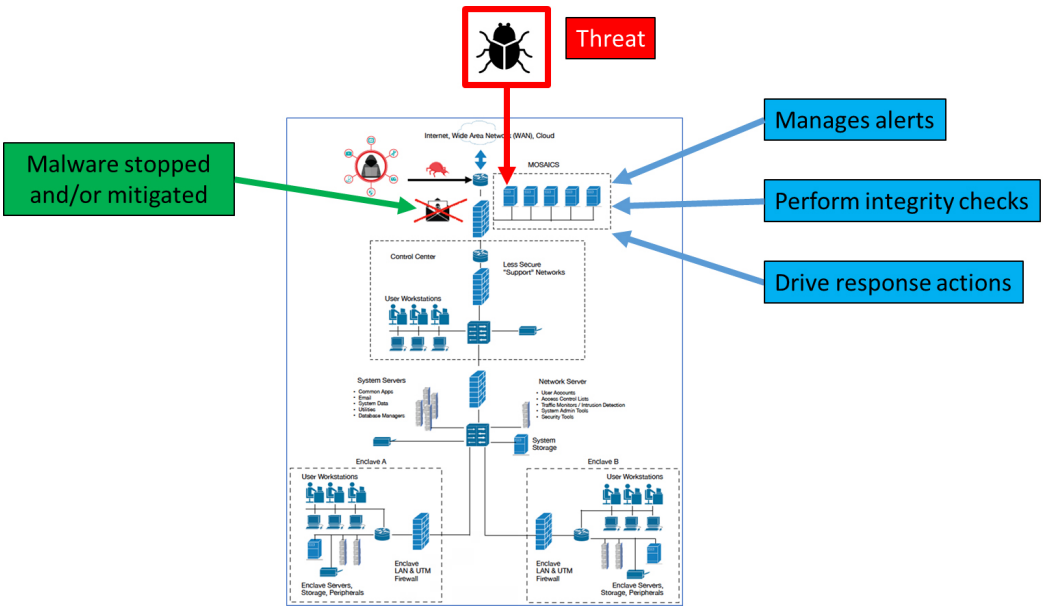

Figure 7. MOSAICS Security Orchestration Framework

Cyber Defense Strategies Way Ahead for Policy Making

Asset owners can better defend healthcare and public health sector networks from ransomware attacks if decision-makers decide to invest and use any of these strategies. For example, DiD, network segmentation, and ZT elements can be enforced by the following toolsets used in the healthcare and public health sectors: strong authentication by ensuring multi-factor solid authentication and session risk detection as access strategy to minimize the risk of identity compromise; policy-based adaptive access by defining acceptable access policies for resources and enforcement with consistent security policy; moving beyond the simple centralized network-based perimeter to comprehensive and distributed segmentation using software-defined micro-perimeters; investing in automating alerting and remediation such as demonstrated in the MOSAICS framework to reduce

MTTR to attacks; use of ML and artificial intelligence (AI) to detect and respond to access anomalies in near real-time; and data classification and protection to discover, classify, protect, and monitor sensitive data to minimize exposure from malicious or unintentional (accidental) exfiltration. Medical devices are generally classified by the US Food & Drug Administration (FDA) for the regulatory classes (i.e., Class I, II, or III). The FDA Product Classification Database provides device names and product codes searchable online and updated weekly. MOSAICS is a framework and does not address auto-classifying structured or unstructured data. The MOSAICS capability also does not create policy. Instead, hospital Governance creates an approach.

The policy is needed to implement technical capabilities to address the challenge of cyber-attacks on critical infrastructure. Long-term architectural policy design compels a response to an increase of ransomware activity targeting the healthcare and public health sector. "The architectural policy design perspective allows researchers to identify policy makers' long-term strategies in policy design, to evaluate the impact of agency on policy feedback processes, and to explain how policymakers can use policies to shape politics. [Moreover,] [a]pplying the framework makes different design strategies analytically tangible and classifiable" (Pechmann 2018). Assuming a percentage of the network is compromised may be a fallacy in cybersecurity as potential exploitation damage needs to be considered in the equation. For example, the mission impact of a compromise could be loss of life or inconvenience by loss of access (i.e., I am unable to remotely access my medical appointment information versus the ability to operate on a patient safely). Detecting malicious activity on a network is well documented, and technologies are available for monitoring networks for events and analyzing them for potential malicious activity. Malicious activity may be detected by unusual access patterns (i.e., prescriptions filled on non-working days after regular work hours), changes to files and databases, or commands issued actions to launch applications. Tools such as Intrusion Detection Systems (IDS) are readily commercially available to alert staff about system vulnerabilities and suspicious patterns or signs of known threats. Other tools such as Security Incident and Event Management (SIEM) help manage and correlate potential threat information to spot irregular network traffic. Intrusion Prevention System (IPS) helps detect and initiate responses to stop suspicious activity. For example, IPS software can be used to disrupt access by reconfiguration of a network firewall.

Using a Reference Architecture (RA) in Policymaking

Society depends on healthcare and hospital critical infrastructure. This infrastructure vertical is fragile with dependencies on life-line sectors such as power, water, communications, and transportation (e.g., ambulances) to function. Healthcare and hospital policy decision-making is unique from other sectors

because policymakers must consider services designed to protect people who work in the industry and serve the underlying needs of society during times of emergency, such as the current pandemic. The critical sector infrastructure is expanding access to services to communities, homes, and businesses beyond the traditional hospital environment, particularly leveraging IoT to support those functions, extending the cyber-attack threat surface. "Healthcare facilities are not only facing a changing environment, but the rules of the game are also changing. New players are, for instance, appearing in the market. They specialize in standardized treatments that could only be provided within a hospital in the past. In general, it can be said that there is a growing necessity for further specialization, amongst others, due to the increasing complexity of technology and rising treatment costs. In some cases, this is forcing clustering of healthcare providers, both horizontally (mergers) and vertically (chain integration). At the same time, patients are increasingly getting a better grip and control over their own healthcare process" (Atos). Such increasing complexity will continue to challenge policymakers in the near term.

There is a gap in knowledge about securing the support infrastructure cost-effectively and efficiently as the interface expands. Flat network architecture is the traditional approach. However, there is an opportunity to inform policymakers of emerging concepts such as DiD, network segmentation, and ZT. The feedback would ensure such clusters of healthcare providers have network infrastructures to help maintain safety and the well-being of the public they engage with and the professionals providing the services. In addition, policy feedback and policy design perspective about concepts such as mutual assistance, liability protections, and regulatory relief is a gap.

Emerging RA strategies can support the policy decision-making design process. An RA can play a vital role in a system solution and support policy decision-making. Architecture can contribute to successful system development by providing a consistent approach to dealing with a complex entity, maintaining traceability from requirements to physical components, and ensuring all system behaviors are captured and mapped to solution elements. The RA can provide insight into requirements refinement, prioritization, and design choices. In addition, it can provide insight into potential problems. More importantly, the cybersecurity RA provides an authoritative design and configuration management for performance and risk assessments. The RA also creates a shared, configuration-controlled design repository and normalizes processes (e.g., models, metrics, versions, reports, etc.) while allowing local options (e.g., the hospital Chief Security Officer). Thus, there is an opportunity to leverage a cybersecurity RA for "control systems to provide conceptual, theoretical, and methodological tools for the analysis of long-term strategic policymaking and considerations of policy feedback effects during policy design" (Pechmann 2018).

Conclusion

As of October 2021, seven cybersecurity breaches are under investigation in Maryland (Cabral 2021). The rise in cyberattacks signals a growing problem that could present life-or-death situations to society. New state law in Maryland, SB623, "prohibits a person from impairing or interrupting computer services of an organization and specifically mentions health care facilities" (Cabral 2021). As a starting point, there is an opportunity for hospital organizations to garner feedback from other critical infrastructure sectors such as power or financial services that already use more advanced network architecture frameworks for future policy decisions for control systems. Paying attention to feedback from the cybersecurity community about network architecture can help remedy some of the challenges in the healthcare and public health critical infrastructure sector. In addition, a RA provides a standard frame of reference that can inform what policy effects emerge and how to design policy effectively to ensure continued, uninterrupted operations and make sure essential societal services are readily available.

This paper sought to introduce the reader to the utility of a RA and how it could be applied to the healthcare cybersecurity domain. In addition, the merits of using this RA methodology for helping shape policymaking were also introduced to help decision-makers select the best cybersecurity choice for their facility.

Acknowledgments and Funding

Aspects of this research are being used to fulfill the requirements for a Systems Engineering PhD at Colorado State University. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acronyms and Abbreviations

AI	Artificial Intelligence
ALE	Annualized Loss Expectancy
ARO	Annualized Rate of Occurrence
BIA	Business Impact Analysis
BOD	Board of Directors
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
COA	Course of Action

COTS	Commercial-Off-The-Shelf
CS	Control Systems
CSCDRA	Systems Cyber Defense Reference Architecture
CSO	Chief Security Officer
CSRA	Cyber Security Reference Architecture
DHA	Defense Health Agency
DHHS	Department of Health and Human Services
DHS	Department of Homeland Security
DiD	Defense-in-Depth
DMZ	Demilitarized Zones
DoD	Department of Defense
EF	Estimated Frequency
EF	Exposure Factor
EF	Estimated Frequency
FBI	Federal Bureau of Investigation
FRCS	Facility Related Control Systems
HIPPA	Health Insurance Portability and Accountability Act
IOC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
ISAC	Information Sharing and Analysis Centers
IT	Information Technology
JCTD	Joint Capability Technology Demonstration
LAN	Local Area Network
MAC	Media Access Control
MED-COI	Medical Community of Interest
ML	Machine Learning
MTTR	Mean Time to Respond

OSI	Open Systems Interconnection
RA	Reference Architecture
RI	Risk Identification
ROI	Return on Investment
SDN	Software-Defined Networking
SIEM	Security Incident and Event Management
SLE	Single Loss Expectancy
SME	Subject Matter Expert
SOAR	Security Orchestration, Automation, and Response
TTP	Tactics, Techniques, and Procedures
VLAN	Virtual Local Area Networks
VRF	Virtual Routing and Forwarding
ZT	Zero Trust

Author Capsule Bios

Aleksandra Scalco received an M.ENG. degree in systems engineering from Iowa State University in 2012, an MBA (2009), and a BJ (1988). She is a Ph.D. candidate in systems engineering at Colorado State University, Fort Collins, CO. She is an engineer with the DOD. From 2012 to 2016, she was an Information System Security Designer (ISSD) and Client Advocate with the National Security Agency/Central Security Service (NSA/CSS). Since 2016, she has been an Engineer with the Naval Information Warfare Center Atlantic (NIWC Atlantic), United States Department of the Navy. She is a technical manager for intelligence-informed mitigations of control system vulnerabilities and leads the transition of new mitigation capabilities into fielded solutions. Her research interest includes the digital transformation of control systems, Software Defined Networking (SDN), and the development of Tactics, Techniques, and Procedures (TTP) using software orchestration for control systems. Ms. Scalco is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE). She is an International Council on Systems Engineering (INCOSE) Certified Systems Engineering Professional (CSEP) (Credential ID 30251735) and member of the seventh cohort of the INCOSE Institute for Technical Leadership. She is Information Technology Infrastructure Library (ITIL) Expert Certified in IT Service Management (Credential ID GR761012539AS). In addition, she is certified at the highest Defense Acquisition Workforce Improve-

ment Act (DAWIA) Certification in Engineering Level 3. She is certified in Science & Technology (S&T) Management and Program Management at Level I. She is an Industry Advisory Board Member at Charleston Southern University, Department of Computer Science for the 2021 – 2024 Term. Her honors included the NSA/CSS Crescent Performance Award for Mission Excellence in 2013.

David Flanigan is a member of the Principal Professional Staff for The Johns Hopkins University Applied Physics Laboratory, providing systems engineering services to various Department of Defense and Department of Homeland Security clients, and has 20 years of active duty and reserve service with the US Navy. A graduate of the University of Arizona, he holds a MS in Information Systems and Technology, a MS in Systems Engineering from the Johns Hopkins University, and a PhD in Systems Engineering and Operations Research from George Mason University. Dr. Flanigan is a member of INCOSE, INFORMS, and MORS.

Steve Simske is Professor of Systems Engineering at Colorado State University. Steve was at HP from 1994-2018, and was an HP Fellow, Vice President, and Director in HP Labs. He is the author of more than 450 publications and more than 200 U.S. patents. Steve is an IEEE Fellow and an NAI Fellow. He is an IS&T Fellow, and its immediate past President (2017–2019). Steve is the Steering Committee Chair for the ACM DocEng Symposium, which meets annually and benefits from University of Nottingham CS Professors Brailsford and Bagley being active leaders. Dr. Simske was a member of the World Economic Forum Global Agenda Councils from 2010-2016, including Illicit Trade, Illicit Economy and the Future of Electronics. In his 20+ years in industry, Steve directed teams in research on 3D printing, education, life sciences, sensing, authentication, packaging, analytics, imaging and manufacturing. His books "Meta-Algorithmics," "Meta-Analytics," and "Functional Applications of Text Analytics Systems" bring Computer Science patterns and principles to address intelligent (AI/ML) systems. At CSU, he has a cadre of on-campus students in Systems, Mechanical, and Biomedical Engineering, along with a larger contingent of on-line/remote graduate students researching in a wide variety of disciplines.

References

Atos. IT Reference Architecture for Healthcare.

Cabral, A. R. 2021. "CYBERSECURITY CONCERNS GROW IN HOSPITALS ACROSS MARYLAND." *MarylandReporter.com*.

Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of

Investigation (FBI), and the Department of Health and Human Services (HHS). 2020. Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector. edited by Department of Defense CISA: Cybersecurity and Infrastructure Security Agency (CISA).

Davis, Jessica. 2021. "Healthcare Cyberattacks Doubled in 2020, with 28% Tied to Ransomware." *Health IT Security*.

Diogenes, Yuri, and Erdal Ozkaya. 2019. *Cybersecurity—Attack and Defense Strategies*. Edited by Packt>. Vol. 2nd Edition. Birmingham, UK: Packt Publishing Ltd.

Djenna, Amir, and Djamel Eddine Saidouni. 2018. "Cyber Attacks Classification in IoT-based-Healthcare Infrastructure." 2nd Cyber Security in Networking Conference (CSNet).

Easttom, Chuck, and Nagi Mei. 2019. "Mitigating Implanted Medical Device Cybersecurity Risks." *IEEE*:4.

Eder, Eric, and Ryan Winn. 2018. "Reducing Healthcare Cyber Risk Using a Cooperative SOAR enabled Healthcare Community (HSOC)." Integrated Cyber, Laurel, Maryland, October 2 – 3, 2018.

Egbogah, Emeka E., and Abraham O. Fapojuwo. 2011. "A Survey of System Architecture Requirements for Health Care-Based Wireless Sensor Networks." *Sensors* (Basel) 11 (5).

Frick, Charlie. 2018. "IACD & FS ISAC Financial Pilot Results." Integrated Cyber, Laurel, Maryland, October 2018.

Glick, Molly. 2021. "Cyberattacks on Health Care Are Rising—But Many Hospitals Aren't Prepared." *Discover*.

Kilcoyne, Michael. 2021. "MOSAICS Transition Strategy." MOSAICS Industry Day #3/TechConnect, Washington, D.C.

Networking. 2012. "Flat Network Strength Also A Security Weakness." *Network Computing*.

Pechmann, Philipp. 2018. "Architectural Policy Design: How Policy Makers Try to Shape Policy Feedback Effects When Designing Policies." Department of Political Science, Aarhus University.

Rich Scalco, Dr. Bill Waugaman. 2021. "More Situational Awareness for Industrial

Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD) Overview Briefing." MOSAICS Industry Day #3/TechConnect, Washington, D.C., October 19, 2021.

Rich Scalco, Dr. Bill Waugaman, Jorge Lacoste, John Andrews, Bill Beary, and Ross Roley. 2018. "More Situational Awareness for Industrial Control Systems (MOSAICS) Joint Capability Technology Demonstration (JCTD)." [PowerPoint Brief]. Johns Hopkins University Applied Physics Laboratory (JHU APL), accessed October 2019. https://www.iacdautomate.org/may-2018-integrated-cyber.

Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connelly. 2020. "Zero Trust Architecture." *NIST Special Publication 800-207*:59.

Scalco, Aleksandra. 2021. "The Case for Control Systems Cybersecurity Capability." MOSAICS Industry Day #3/TechConnect, Washington, D.C., October 19, 2021.

SecurID. 2021. "What is zero trust?" SecurID, accessed October 30, 2021. https://www.securid.com/en-us/blog/the-language-of-cybersecurity/what-is-zero-trust.

Simos, Mark. 2019. "Zero Trust strategy—what good looks like." [website]. Microsoft, accessed October 30, 2021. https://www.microsoft.com/security/blog/2019/11/11/zero-trust-strategy-what-good-looks-like/.

Simske, Steven J. 2020. Cybersecurity Lectures. In *SYSE 569 Course*. Fort Collins, Colorado, USA: Colorado State University.

Team, Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering. 2021. Department of Defense (DOD) Zero Trust Reference Architecture. Edited by Department of Defense. Washington, D.C.