SANS | GIAC CERTIFICATIONS

WHITE PAPER

# ICS OT Systems Security Engineering Is Not Dead

Isiah Jones

# ICS OT Systems Security Engineering Is Not Dead

Written by

Isiah Jones, MPS, GICSP, CISSP, C|CISO

## Contents

## Systems Security Engineering? For ICS?

So, what exactly is Systems Security Engineering? How does it apply to ICS OT? What resources exist that should be used in a disciplined Systems Security Engineering culture and methodology? Systems Security Engineering has become in many cases a forgotten skillset and disciplined multidisciplinary art that merges multiple worlds into a methodical, rigorous set of practices. NIST SP 800-160 was created to educate the engineering and cyber communities on the basics of system security engineering. Now more than ever it must see a revival and more specifically that revival must occur within the ICS OT community to make all societies safer, more secure and more resilient long-term. ISA and IEC have worked together to create a life cycle of international security and safety standards such as ISA/IEC 62443 and ISA84/IEC 61511. Various parts of the 62443 such as 3-3 for system level security capabilities, 4-1 for secure by design systems development and 4-2 for component and device level security capabilities can and should be leveraged throughout a rigorous systems security engineering discipline and set of practices. The key stakeholders I must address in system security engineering for ICS OT are the vendors and OEMs, integrators and solutions providers, asset owners and operators and dedicated full-time ICS OT cybersecurity focused professionals. The chain is only as strong as its weakest link. Systems Security Engineering requires all stakeholders to participate throughout the lifecycle of assets and operations that directly impact the safety, security and resiliency of societies and the infrastructures they depend on.

# Why Do we need it?

Many in industry have appeared to have abandoned the idea that secure design, security hardening, in-depth and robust prevention and protection can be done for industrial control systems (ICS) or operational technology (OT) as it is known today. As a career systems and cybersecurity professional I believe otherwise. I believe it is a societal imperative, due care, due diligence, and standard of good practices responsibility for all ICS OT, Industrial Internet of Things (IIoT), Internet of Things (IoT) and critical embedded devices to be designed, acceptance tested, validated, integrated, implemented, operated and maintained with safe, secure and resilient functional capabilities. I believe all stakeholders throughout the asset, environment, societal and ICS OT dependent infrastructure ecosystems should develop and maintain a proactive security culture and mindset throughout the life cycle of assets and operations. I believe that to not do so would put the very infrastructures, raw materials, consumed products, goods and services that society depends on at unnecessary and preventable risk. I believe this is especially paramount in this new era of technology convergence and integration of the physical, electronic, communications, societal and digital worlds. To many Systems Security Engineering is a lost art and a forgotten skillset within cybersecurity. However, when it comes to ICS OT IIoT IoT and critical embedded devices such as chillers, boilers, pumps, valves, breakers, safety systems and implantable medical devices, systems security engineering is absolutely essential.

# Key Stakeholder Roles & Terms

Operational Technology (OT) in its broadest sense to include Industrial Control Systems (ICS), Instrumentation, Control and Automation Systems, Industrial Internet of Things (IIoT), Internet of Things (IoT) and critical embedded devices all of which are used to monitor, control, measure and or manipulate the physical world. OT also includes middleware and operational execution applications such as manufacturing execution systems (MES), data historians, Overall Equipment Effectiveness (OEE) systems, measuring systems, vision inspection and industrial printing systems and sometimes integrated SAP modules such as SAP PM.

Traditional ICS includes distributed control systems (DCS), process control systems (PCS), supervisory control and data acquisition (SCADA) systems, building or facility management control systems (BMS/BCS), safety instrumented systems (SIS), energy or electric control systems (ECS), programmable logic controllers (PLC), remote terminal units (RTU), intelligent electronic devices (IED), variable frequency drives (VFD), programmable relays, Human Machine Interfaces (HMI), motors, actuators, sensors, breakers, pumps, valves, engines, turbines, boilers, chillers, fire and lighting systems, meters etcetera.

A comprehensive BMS/BCS usually includes heating, ventilation and air condition (HVAC) which includes air handlers, dampers, chillers, boilers, air compressors etcetera. BMS/BCS also includes fire and life safety systems, lighting, indoor mass communication and alarming systems, camera systems such as CCTV and physical access control systems such as badging systems.

DCS and PCS are usually for specific operations areas, process loops and zones at specific sites and can be in some cases integrated with each other and or with a larger SCADA system at a regional, site and organizational level. DCS, PCS and SCADA are also sometimes directly integrated with SIS as well in certain use cases.

The primary distinction between IIoT and IoT is industrial versus consumer use cases. IIoT usually consists of traditional ICS components, devices and or systems that have in recent years been modified to include internet capable features that enables their users to converge and integrate with more traditionally IT systems and conduits. Some examples are the use of smart sensors and smart meters that now have cellular, Wi-Fi and Bluetooth communications abilities and support integration with cloud-based applications to allow for monitoring and control from anywhere the user has an internet connection. IoT use cases normally occur in consumer home environments such as having an Alexa device connected to the lights in your home. The lights, meters and solar invertors themselves were traditionally isolated ICS. However, they have of late become increasingly IIoT capable to support consumer IoT use cases such as Alexa being integrated with physical appliances within your home.

Critical embedded devices have in recent years been adopted by OT because devices such as insulin pumps and pacemakers are not your typical corporate IT systems but they for many years were not considered ICS either. However, with the fourth industrial revolution that has brought about convergence with IIoT and IoT use cases, critical embedded devices that directly impact the physical world are equally essential to be protected with the same levels of rigor as traditional ICS. Like ICS traditional critical medical devices in the past were not typically designed for IIoT and IoT use cases. However, like ICS, traditional critical embedded devices such as insulin pumps and pace makers have become more connected with more access to the internet, cloud, mobile tablet and phone applications etcetera turning them increasingly into an IIoT or IoT device.

Key terms and old versus new use cases have continuously reshaped what various stakeholders view as ICS OT overall. However, regardless of what industry calls it, control, manipulation, measurement and monitoring of the physical world in some way is what they all have in common. When it comes to ICS OT systems security engineering, there are some key stakeholders that hold up the chain of safe, secure and resilient ICS OT capabilities within society. These key stakeholders discussed in the following subsections are absolutely essential links in that chain. If any of these links are weak so too is the chain itself and thus all of society. In this new era of nation state conflicts where targeting ICS OT is fair game, where criminals, terrorists and individuals now have access to more public information, tools, trainings and leaked nation state toolkits, while the rapid pace of this fourth industrial revolution drives ever increased automation and convergence, systems security engineering has never been more vital.

## Product Vendors & OEM

It should go without saying that one of the most important links in the chain of a safe, secure and resilient society are the ICS OT product vendors and original equipment manufacturers (OEM) themselves. Afterall, every type of embedded device, ICS OT component, application, and product is created and pushed into the supply chain by vendors and OEMs. Thus, they have an essential responsibility in ensuring they adopt a systems security engineering culture in all aspects of their product and organizational practices. If the ICS OT vendors and OEMs do not provide, verify, document and educate other stakeholders in the chain on the right functional capabilities within their products it will be that much harder for society to have a leg up on threat actors who spend the time and money on reverse engineering the products, practices and supply chains of vendors and OEMs. It is absolutely critical that vendors and OEMs play their part in society with a proactive systems security engineering mindset.

In recent years industry has seen improvements from some of the vendors and OEMS such as Rockwell, Siemens, Schneider Electric, Emerson and others who have become more proactive in sharing discovered vulnerabilities with applicable tested and recommended remediations for each. While there have been improvements, more work remains to be done by all vendors and

OEMs. For example, many of the OEMs like to use the distributor model which in and of itself does not always enforce and verify systems security engineering practices for their products are being strictly followed. This essentially makes their efforts of improvement less impactful as they could and should be throughout the supply chain long-term.

## Integrators & Solution Providers

After the vendors and OEMs, themselves one could argue that the next most important stakeholder and often times an unfortunate weak link in the chain of a safe, secure and resilient society are the engineering construction, architecture, design and integration firms. Many of these firms do not have a robust cybersecurity experienced culture let alone a systems security engineering mature culture. Many of the critical infrastructures in societies around the world are designed, built, integrated, serviced and maintained by integrators and solution providers. Thus, making them the glue between vendors and OEMs as well as Asset Owners and Operators. Many of the integrators and solution providers, like the vendors and OEMs have in recent years attempted to build pockets of excellence within their organizations of trained and experienced cybersecurity professionals. However, areas for improvement still require that they scale these professionals, turn them into ICS OT focused and capable cyber professionals and create a robust end-to-end systems security engineering culture in all things that they do. This link in the chain has and will continue to weaken the rest of the chain and thus all of society if more of these firms are not consolidated and trained in ICS OT systems security engineering at scale.

It is an absolute must that the integrator and solutions provider community create dedicated well trained and multidisciplined groups of ICS OT focused cyber professionals who are deeply engrained in an ICS OT systems security engineering culture and set of practices.

## Asset Owners & Operators

When it comes to how ICS OT processes, equipment and systems are operated in production that responsibility ultimately falls to the asset owners and operators themselves. This stakeholder is the most liable and accountable to society especially end consumers of their products and services (e.g. water, electric, transportation, food and medicine) and in some cases also to regulators that oversee their sectors in countries around the globe. If the asset owners do not have an ICS OT focus security culture that includes a robust systems security engineering mindset, requirements, processes and operational procedures then all of the efforts and good will of the other stakeholders will be in vain. The vendors and OEMs, integrators and solutions providers can do all that is possible to ensure secure, safe and resilient ICS OT assets and solutions are created, tested, integrated, implemented and maintained but it is up the asset owners and operators to join in the chain as a strong link to ensure implementation, operations and continuous maintenance includes a very strong systems security engineering set of practices and enforcements. When asset owners and

operators are too small to do so, lack the understanding of the severity of having such a culture with dedicated ICS OT cybersecurity teams and or blatantly deviate from and or deter the other stakeholders in the chain from succeeding, they have essentially become the weakest link in the chain. Societies will be put at unnecessary often preventable risk due to failures of the asset owners and operators themselves despite the best efforts of all other stakeholders involved.

## ICS OT Cybersecurity Professionals

In recent years a dedicated global community of ICS OT focused, trained and experienced cybersecurity professionals has emerged. Unfortunately, this community, despite its gradual growth over the last couple of decades is relatively small in size, scope and persistent abilities when compared to the other key stakeholders. However, this link in the chain is the most dedicated and the most in tune with the consequences for society of failure. It is extremely necessary for vendors and OEMs, integrators and solutions providers and asset owners and operators to not only consult with organizations that contain such professionals but to also hire them and develop their own permanent in-house cadre of these trained, certified and dedicated ICS OT focused cybersecurity professionals. It is also essential that the other stakeholders do not limit these professionals to just security assessments and network monitoring, incident response and threat hunting. Those skillsets are important and essential but to prevent and protect society, ICS OT systems security engineering focused, and trained professionals must be part of any robust and serious ICS OT cybersecurity team.

This growing community of dedicated ICS OT professionals will be the key to helping ensure that the other three major stakeholders become stronger links in the chain and long-term remain as such. However, vendors and OEMs, integrators and solutions providers and asset owners and operators must be warned that these professionals are not collateral duty engineering and or IT professionals. They must be cross trained and diverse in their experiences and spend all of their time focused on understanding the nuanced technical details and functional abilities of ICS OT assets from an end-to-end security perspective with a purple mindset. Purple meaning, they must have career, education, training and or certification experiences that include both offensive and defensive tools, techniques, tactics, procedures, culture and mindset. They must have a tool independent and agnostic security and safety troubleshooting knack or instinct and constant desire for continuous learning. It is essential that organizations do not treat ICS OT as a subset of IT or Engineering but instead as a cross trained multidisciplinary and focused cadre or team of dedicated ICS OT security and safety professionals.

# Systems Security Engineering 101 – NIST SP 800-160

Besides being a forgotten old love of traditional 10 domains of systems security, INFOSEC and Information Assurance, Cyber professionals, what exactly is Systems Security Engineering? Alas it is written, and it is not new. Dr. Ron Ross at NIST led the charge in creating and authoring the "NIST SP 800-160 – "Systems Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems"[1] guidelines. Within SP 800-160, it is stated that Systems Engineering itself provides a multidisciplinary, structured and disciplined approach to engineering systems. Systems Security itself is thus applying "engineering and management principles, concepts, criteria, and techniques to optimize security within the constraints of operational effectiveness, time, and cost throughout all stages of the system life cycle." Therefore, Systems Security Engineering focuses on protecting assets and stakeholders from asset loss and unsafe consequences through a disciplined set of approaches throughout the lifecycle of an asset with the goal being to eliminate or reduce vulnerabilities and minimize or constrain threats, events, hazards, and exploits abilities in triggering such vulnerabilities to limit their impacts and consequences.

Systems Security Engineering may have been a forgotten art and disciplined demanding methodology in IT, but it is very important that it is remembered and revived specifically for ICS OT in this new error of IIoT and IoT during this societal convergent fourth industrial revolution. SP 800-160 does an excellent job in defining some of the discipline structure and practices needed to implement a systems security engineering culture. Some of the benefits and results of Systems Security Engineering that it lists are as follows:

- Defines stakeholder security objectives, protection needs and concerns, security requirements, and associated validation methods;
- Defines system security requirements and associated verification methods;
- Develops security views and viewpoints of the system architecture and design;
- Identifies and assesses vulnerabilities and susceptibility to life cycle disruptions, hazards, and threats;
- Designs proactive and reactive security functions encompassed within a balanced strategy to control asset loss and associated loss consequences;
- Provides security considerations to inform systems engineering efforts with the objective to reduce errors, flaws, and weakness that may constitute security vulnerability leading to unacceptable asset loss and consequences;

[1] https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final

• Identifies, quantifies, and evaluates the costs/benefits of security functions and considerations to inform analysis of alternatives, engineering trade-offs, and risk treatment decisions;

• Performs system security analyses in support of decision making, risk management, and engineering trades;

• Demonstrates through evidence-based reasoning, that security claims for the system have been satisfied;

The Guideline continues with defining security requirements and tasks or activities that must be completed throughout a robust Systems Life Cycle Process (based on processes defined in ISO/IEC/IEEE 15288). Below is a high-level list of some of the Systems Security Engineering processes with their respective activities, tasks and subtask requirements that must be completed throughout a disciplined, multidisciplinary Systems Engineering Life Cycle Process.

- **Agreement Processes** – Acquisition and Supply
- **Organizational Project Enabling Processes** – Lifecycle Model Management, Infrastructure Management, Portfolio Management, HR Management, Quality Management, and Knowledge Management
- **Technical Management Processes** – Project Planning, Project Assessment and Control, Decision Management, Risk Management, Configuration Management, Information Management, Measurement, and Quality Assurance
- **Technical Processes** – Business or Mission Analysis, Stakeholder Needs and Requirements Definition, System Requirements Definition, Architecture Definition, Design Definition, Systems Analysis, Implementation, Integration, Verification, Transition, Validation, Operation, Maintenance, and Disposal

# Secure Systems Development – ISA/IEC 62443-4-1

You cannot truly do robust systems security engineering if you neglect integrating secure design practices, tools, procedures, techniques, requirements and principles into the product, application, programming and software development lifecycles of ICS OT assets and operations.

The international society of automation (ISA) 99 standards committee in working agreement with the international electrotechnical commission (IEC) have created a lifecycle series of international standards known as ISA/IEC 62443, specifically designed for ICS OT, including Industrial IoT, security. 62443 committee members include all of the key stakeholder groups mentioned earlier in this paper as well as government agency representatives from around the globe.

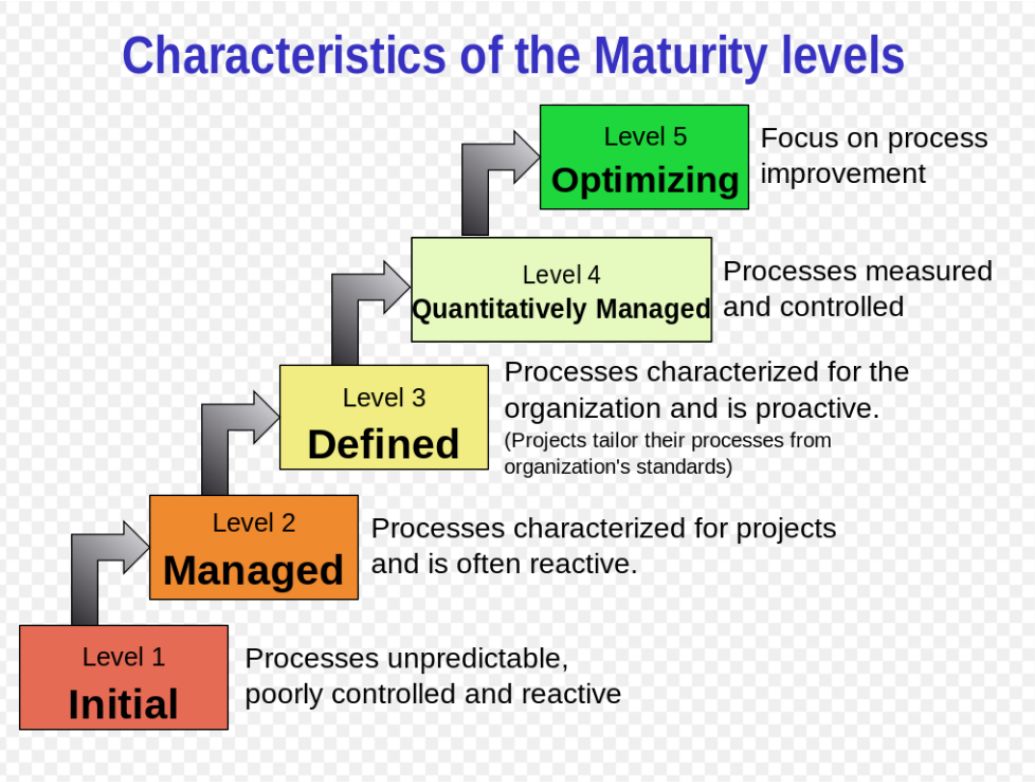
The 4-1 part of the standard was essentially created to define a set of 8 practices with subsets of requirements and mapping to systems development capability maturity models for vendors and OEMs to implement and maintain secure by design development lifecycles within their product supply chains. Although 4-1 was directed at the vendors and OEMs, it does not excuse asset owners and operators or integrators and solution providers from following the 4-1 in all systems and application development activities. In order to create a true systems security engineering ecosystem all key stakeholders must include 4-1 security practices within all development lifecycles including when writing PLC logic languages such as the IEC 61131-3 languages like Ladder Logic/Diagram (LD), Function Block Diagram (FBD), Sequential Function Chart (SFC), Instruction List (IL) and Structure Text (ST).

Secure Systems Development Practices defined in 4-1 are:

- Practice 1 – Security Management (SM)
- Practice 2- Specification of security requirements (SR)
- Practice 3 – Secure by design (SD)
- Practice 4 – Secure implementation (SI)
- Practice 5 – Security verification and validation testing (SVV)
- Practice 6 – Management of security related issues (DM)
- Practice 7 – Security update management (SUM)
- Practice 8 – Security guidelines (SG)

Each of these practices has a series of requirements and tasks that must be completed. Within the 4-1 a brief explanation of systems development maturity levels from the vendor and OEM perspective is below. The well-known systems development CMMI model was used to defined maturity levels.

**Capability Maturity Model Integration (CMMI) Levels**




[2]

[2] https://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration

**Table 1 – Maturity levels**

| Level | CMMI-DEV | ISA-62443-4-1 | ISA-62443-4-1 Description |
|---|---|---|---|
| 1 | Initial | Initial | Product suppliers typically perform product development in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency across projects and repeatability of processes may not be possible. |
| 2 | Managed | Managed | At this level, the product supplier has the capability to manage the development of a product according to written policies (including objectives). The product supplier also has evidence to show that personnel who will perform the process have the expertise, are trained and/or follow written procedures to perform it.<br>However, at this level, the organization does not have experience developing products to all of the written policies. This would be the case when the organization has updated its procedures to conform to this standard, but has not yet put all of the procedures into actual practice.<br>The development discipline reflected by maturity Level 2 helps to ensure that development practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.<br>NOTE At this level, the CMMI and ISA-62443-4-1 maturity models are fundamentally the same, with the exception that ISA-62443-4-1 recognizes that there may be a significant delay between defining/formalizing a process and executing (practicing) it. Therefore, the execution related aspects of the CMMI-DEV Level 2 are deferred to Level 3. |
| 3 | Defined | Defined (Practiced) | The performance of a Level 3 product supplier can be shown to be repeatable across the supplier's organization. The processes have been practiced, and evidence exists to demonstrate that this has occurred.<br>NOTE At this level, the CMMI and ISA-62443-4-1 maturity models are fundamentally the same, with the exception that the execution related aspects of the CMMI-DEV Level 2 are included here. Therefore, a process at Level 3 is a Level 2 process that the supplier has practiced for at least one product. |
| 4 | Quantitatively Managed | Improving | At this level, Part 4-1 combines CMMI-DEV Levels 4 and 5. Using suitable process metrics, product suppliers control the effectiveness and performance of the product and demonstrate continuous improvement in these areas. |
| 5 | Optimizing | | |

It goes without saying, systems security engineering would be incomplete if the secure development lifecycle was not included. In order for the chain of a secure, safe and resilient society to become and remain strong 4-1 must be leveraged not only by vendors and OEMs but these practices must be applied as part of a systems security engineering culture within integrators and solutions providers, asset owners and operators as well as among ICS OT cybersecurity professionals. How code is written and tested impacts the ICS OT systems, device and component abilities and attack surfaces. This is especially important and often over looked during the systems integration stages when integrating multiple types of systems. In the age of Smart Grid, Smart Cities, Smart Cars charging on the edge of the distribution grid and Smart hospitals with embedded devices implanted inside people it is very important that 4-1 is looked at from an integration of different types of domains, components, systems etcetera that have a broader impact to public safety.

# Systems Level Capabilities – ISA/IEC 62443-3-3

Within a robust Systems Security Engineering culture secure and mature systems or software development lifecycles are essential but not the only piece of the complete pie. It is crucial that the functional capabilities of any ICS OT, including Industrial IoT, systems include security mitigation features that counter vulnerabilities, threats and exploits. Some of the functional capabilities may even successfully remove attack surfaces and vulnerabilities all together if properly implemented as part of a mandatory and consistently mature systems security engineering culture.

Within the 62443 series of ICS OT security international standards the 3-3 was written to define a minimum set of foundational and systems requirements and necessary requirements enhancements for ICS OT systems. It is essential that systems are designed, tested, validated, integrated, implemented, operated and maintained with the appropriate levels of security functionality enabled. If systems are not designed and operated with such capabilities it will make having a systems security engineering culture nearly impossible. 3-3 should be applied by all key stakeholders but it was essentially written for those stakeholders responsible for designing, testing, implementing, configuring, integrating, operating and maintaining the ICS OT systems. Often times this could be integrators and solutions providers, asset owners and operators themselves, ICS OT cybersecurity professionals or even vendors and OEMs performing multiple roles during the warranty period.

Below is high level list of foundational requirements (FR) and system requirements (SR) for ICS OT system level security capabilities.

- FR 1 Identification and authentication control
    - SR 1.1 – Human user identification and authentication
    - SR 1.2 – Software process and device identification and authentication
    - SR 1.3 – Account management
    - SR 1.4 – Identifier management
    - SR 1.5 – Authenticator management
    - SR 1.6 – Wireless access management
    - SR 1.7 – Strength of password-based authentication
    - SR 1.8 – Public key infrastructure (PKI) certificates
    - SR 1.9 – Strength of public key authentication

  - SR 1.10 – Authenticator feedback
  - SR 1.11 – Unsuccessful login attempts
  - SR 1.12 – System use notification
  - SR 1.13 – Access via untrusted networks
- FR 2 Use control
  - SR 2.1 – Authorization enforcement
  - SR 2.2 – Wireless use control
  - SR 2.3 – Use control for portable and mobile devices
  - SR 2.4 – Mobile code
  - SR 2.5 – Session lock
  - SR 2.6 – Remote session termination
  - SR 2.7 – Concurrent session control
  - SR 2.8 – Auditable events
  - SR 2.9 – Audit storage capacity
  - SR 2.10 – Response to audit processing failures
  - SR 2.11 – Timestamps
  - SR 2.12 – Non-repudiation
- FR 3 System integrity
  - SR 3.1 – Communication integrity
  - SR 3.2 – Malicious code protection
  - SR 3.3 – Security functionality verification
  - SR 3.4 – Software and information integrity
  - SR 3.5 – Input validation

  - SR 3.6 – Deterministic output
  - SR 3.7 – Error handling
  - SR 3.8 – Session integrity
  - SR 3.9 – Protection of audit information
- FR 4 Data confidentiality
  - SR 4.1 – Information confidentiality
  - SR 4.2 – Information persistence
  - SR 4.3 – Use of cryptography
- FR 5 Restricted data flow
  - SR 5.1 – Network segmentation
  - SR 5.2 – Zone boundary protection
  - SR 5.3 – General purpose person-to-person communication restrictions
  - SR 5.4 – Application partitioning
- FR 6 Timely response to events
  - SR 6.1 – Audit log accessibility
  - SR 6.2 – Continuous monitoring
- FR 7 Resource availability
  - SR 7.1 – Denial of service protection
  - SR 7.2 – Resource management
  - SR 7.3 – Control system backup
  - SR 7.4 – Control system recovery and reconstitution
  - SR 7.5 – Emergency power
  - SR 7.6 – Network and security configuration settings

- SR 7.7 – Least functionality
- SR 7.8 – Control system component inventory

# Device & Component Level Capabilities -ISA/IEC 62443-4-2

Often when it comes to systems security engineering, software development lifecycle and system level implementation may be remembered, and security capabilities and practices may even be implemented. However, if the ICS OT devices and components including their hardware, firmware, conduit and communication features are forgotten this could leave a backdoor or achilles heel within any robust systems security engineering culture. The 4-2 was created with this in mind. Just as the 4-1 it may have been written speaking directly to vendors and OEMs, but it is important that the other key stakeholders define device and component level security requirements as mandatory and participate in the functionality verification, validation, acceptance testing, integration, design, modification, configuration, operation and maintenance phases of an ICS OT asset and operations lifecycle. Asset owners and operators, ICS OT cybersecurity professionals and integrators and solution providers must be fully capable and aware of understanding, configuring, validating and ensuring the device and component level security capabilities are implemented and maintained.

The 4-2 was written in such a way that component, software, embedded device, host and network device-based requirements would be mapped to the set of foundational requirements (FR), systems requirements (SR) and requirements enhancements (RE) structure found in other parts of the 62443 series of international ICS OT security standards. With respect to systems security engineering the most applicable related part would be the 3-3 discussed earlier.

Below is a list of 4-2 device and component level requirements that map into the core seven foundational requirements found in 3-3 system level requirements so that devices and components that become part of an overall system can support meeting those overall system requirements.

Please note for clarification in 4-2 requirements are broken down by device and component groups such as:

- CR – component requirements that are common to all types of components
- SAR – software application requirement
- EDR – embedded device requirement
- HDR – host device requirement
- NDR – network device requirement

- FR 1 Identification and authentication control

  - CR 1.1 – Human user identification and authentication
  - CR 1.2 – Software process and device identification and authentication
  - CR 1.3 – Account management
  - CR 1.4 – Identifier management
  - CR 1.5 – Authenticator management
  - NDR 1.6 – Wireless access management
  - CR 1.7 – Strength of password-based authentication
  - CR 1.8 – Public key infrastructure (PKI) certificates
  - CR 1.9 – Strength of public key authentication
  - CR 1.10 – Authenticator feedback
  - CR 1.11 – Unsuccessful login attempts
  - CR 1.12 – System use notification
  - NDR 1.13 – Access via untrusted networks
  - CR 1.14 – Strength of symmetric key based authentication
- FR 2 Use control
  - CR 2.1 – Authorization enforcement
  - CR 2.2 – Wireless use control
  - CR 2.3 – Use control for portable and mobile devices
  - SAR, EDR, HDR, NDR 2.4 – Mobile code
  - CR 2.5 – Session lock
  - CR 2.6 – Remote session termination
  - CR 2.7 – Concurrent session control
  - CR 2.8 – Auditable events

  - CR 2.9 – Audit storage capacity
  - CR 2.10 – Response to audit processing failures
  - CR 2.11 – Timestamps
  - CR 2.12 – Non-repudiation
  - EDR, HDR, NDR 2.13 – Use of physical diagnostic and test interfaces
- FR 3 System integrity
  - CR 3.1 – Communication integrity
  - SAR, EDR, HDR, NDR 3.2 – Malicious code protection
  - CR 3.3 – Security functionality verification
  - CR 3.4 – Software and information integrity
  - CR 3.5 – Input validation
  - CR 3.6 – Deterministic output
  - CR 3.7 – Error handling
  - CR 3.8 – Session integrity
  - CR 3.9 – Protection of audit information
  - EDR, HDR, NDR 3.10 – Support for Updates
  - EDR, HDR, NDR 3.11 – Physical tamper resistance and protection
  - EDR, HDR, NDR 3.12 – Provisioning product supplier roots of trust
  - EDR, HDR, NDR 3.13 – Provisioning asset owner roots of trust
  - EDR, HDR, NDR 3.14 – Integrity of boot process
- FR 4 Data confidentiality
  - CR 4.1 – Information confidentiality
  - CR 4.2 – Information persistence

    - CR 4.3 – Use of cryptography
- FR 5 Restricted data flow
    - CR 5.1 – Network segmentation
    - NDR 5.2 – Zone boundary protection
    - NDR 5.3 – General purpose person-to-person communication restrictions
- FR 6 Timely response to events
    - CR 6.1 – Audit log accessibility
    - CR 6.2 – Continuous monitoring
- FR 7 Resource availability
    - CR 7.1 – Denial of service protection
    - CR 7.2 – Resource management
    - CR 7.3 – Control system backup
    - CR 7.4 – Control system recovery and reconstitution
    - CR 7.5 – Emergency power
    - CR 7.6 – Network and security configuration settings
    - CR 7.7 – Least functionality
    - CR 7.8 – Control system component inventory

# Safety Systems Security Capabilities – ISA84/IEC 61511

The ISA84/IEC 61511 international standard for functional safety engineering which focuses on functional safety systems, specifically Safety Instrumented Systems (SIS) is being updated in working group 9 – cybersecurity for safety systems, in collaboration with ISA/IEC 62443 standards committee. The Safety Integrity Levels (SIL) of SIS and safety functions should always be evaluated for security functional capabilities within devices, components, systems, communications conduits, firmware and software etcetera. Those security functional capabilities in an ICS OT Systems Security Engineering context should always leverage the ISA/IEC 62443 parts 3-3, 4-1 and 4-2 security capabilities, requirements and practices for ICS OT systems, devices and components. It is imperative that non digital mechanical safeguards be considered as viable security countermeasures within safety systems and that any programmable, electronic, analog and digital components must always be evaluated from a cybersecurity systems security engineering perspective to avoid a false sense of safety. Failing to do so causes security attack surfaces that can directly threaten personnel, environmental and public safety to be ignored and invites weaknesses in the design of safety systems.

With the TRISIS/TRITON/HATMAN attack it is now well known in the general public domain that at least some threat actors have decided that intentionally targeting safety systems is fair game. Safety systems specifically exist in parallel to, integrated with or segregated from the primary ICS OT to contain or prevent consequences that cause loss of life, injury and or environmental damage in the event that the primary ICS OT fails or operates incorrectly under normal accidental use cases. It does not however to date account for intentional actions albeit accidental or malicious by insiders or others. Thus, Systems Security Engineering needs to be applied to all ICS OT including safety systems in order to keep assets, processes, operations, personnel, the environment and societies safe. In the voice of Dave Chappelle memes “Modern problems requires modern solutions”.

# Conclusion

In this new decade, the new roaring 20s of this 21st century, containing this fourth industrial age, a revival of systems security engineering should be seen as a societal imperative that is no longer optional. Systems security engineering is especially paramount for ICS OT use cases such as IIoT and IoT integration. It is unsafe and unwise for society to continue down the path of automate everything, converge everything and make everything smart without ensuring a social construct that embeds systems security engineering rigor into everything that we make, integrate and operate. The leaders of this new era will be those who have the fortitude to put societal safety, security and resilience above their financial and or political bottom line. How do we measure the cost to society moving forward if we continue to neglect systems security engineering as a culture? The next couple of decades will be the final judge as we build out the infrastructures of tomorrow today without thinking of the future. The wise will leverage NIST SP 800-160 in combination with ISA/IEC 62443 3-3, 4-1, 4-2 and ISA84/IEC 61511 to ensure that all ICS OT is built, verified, tested, validated, integrated, operated, maintained and disposed of from a systems security engineering rigor perspective as a cultural way of life across all domains and all levels of society.

# About the Author

Isiah Jones is a Senior ICS OT Cybersecurity Engineer and Cyber professional with 15 years of progressive experiences in various aspects of IT, security, assurance, and ICS OT. Working exclusively on ICS security since 2014. Isiah has performed ICS OT cybersecurity work in the Middle East, East Africa, Europe, Hawaii, and throughout the continental United States. Isiah has delivered cyber IT or ICS OT security services or support for the US Navy, US Marine Corps, Siemens, FERC, and many commercial asset owners, ICS OEMs, ICS integrators and operators across several sectors and asset type verticals globally.

Isiah has held national security clearances as high as TS/SCI and Q. He has had a network of affiliations that reach into the US intelligence community, Defense community, US Congress, FERC, Department of Energy, Depart of Homeland Security, Department of Commerce, National Labs, ICS OEM vendors, ICS integrators, and asset owners/operators. He is a former US Navy civil services Information Assurance Officer (IAO) and Systems Analyst as well as a former FERC civil services GS-15 subject matter expert on ICS OT cybersecurity for US national security critical energy infrastructures. He is also a former ICS OT cyber mission assurance and Information Systems Security Engineering (ISSE) consultant and contractor. He is an active volunteer contributor on multiple working groups within the ISA/IEC 62443 international standards committee, the ISA84 standards committee working group for cybersecurity for safety systems as well as multiple committees within American Water Works Association (AWWA). He brings well rounded experiences, access, insights, connections and visibility into critical infrastructure security issues across many asset types and sectors (water, wastewater, electric, oil, gas, LNG, building automation, airfields, maritime, hydro dams, manufacturing, life sciences, logistics & warehouse, ERP etcetera).