

Committee on National Security Systems Instruction
(CNSSI) No. 1253

SECURITY CONTROL OVERLAYS
FOR
INDUSTRIAL CONTROL SYSTEMS

Version 1

July 2013



This version of the Overlay is meant to be used as a companion to the DHS
Cybersecurity Self Evaluation Tool (CSET).

Industrial Control Systems Overlay

1. Identification

This overlay is entitled the Industrial Control Systems Overlay as it identifies unclassified security control specifications required to address critical and supporting infrastructure control systems risks to national security systems. An Industrial Control System (ICS)¹ is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADAs) used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes. The purpose of this overlay is to establish the security controls necessary for ICSs, define the ICS Enclave authorization boundary, and illustrate various types of sensors, actuators and devices typically found on an ICS. This is version 1.0 dated July 8, 2013.

The following documents were used to create this overlay:

- National Institute of Science and Technology (NIST) Special Publication (SP) 800-34 Rev. 1, *contingency planning Guide for Federal Information Systems*, May 2010
- NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, May 1, 2010
- NIST SP 800-82, *Guide to Industrial Control Systems' Security*, June 2011
- NISTR 7628, *Guidelines for Smart Grid Cyber Security*, September 2010
- NIST SP 1108R2, *Framework and Roadmap for Smart Grid Interoperability Standards*, Release 2.0, February 2012
- Executive Order Improving Critical Infrastructure Cybersecurity, February 12, 2013
- Executive Order Critical Infrastructure Security and Resiliency, February 12, 2013
- Executive Order 13514, *Federal Leadership in Environmental, Energy and Economic Performance*, October 2009
- Council on Environmental Quality (CEQ), Adjunct to Executive Order 13514, *Implementing Instructions – Sustainable Locations for Federal Facilities*, September 15, 2011
- Executive Office of the President of the United States, *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future*, June 2011
- Committee on National Security Systems Instruction (CNSSI) No. 1253, Version 2, March 15, 2012
- ANSI/ISA 99.00.01-2007, *Security for Industrial Automation and Control Systems*
- DoD Unified Facility Criteria 3-470-01, *LonWorks Utility Monitoring and Control System (UMCS)*, May 2012
- DoD Unified Facility Criteria 4-010-01, *Minimum Antiterrorism Standards for Buildings*, February 2012
- DoD Unified Facility Criteria 4-022-01, *Security Engineering Manual*, March 2005
- DoD Unified Facility Guide Specification 25-10-10, *Utility Monitoring and Control System (UMCS) Front End and Integration*, November 2012

¹ DoDI 8500 series categorizes ICS as Platform Information Technology (PIT).

- Energy Sector Control Systems Working Group, *Roadmap to Secure Energy Delivery Systems*, January 2011
- FEMA 426, *Reference Manual to Mitigate Buildings Against Terrorist Attack*, December 2003
- International Code Council, *International Building Code*
- National Defense Authorization Act of 2010, Section 2841. *Adoption of Unified Energy Monitoring and Utility Control System Specification for Military Construction and Military Family Housing Activities*
- Critical Infrastructure Information Act of 2002
- Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection, 2003
- Department of Homeland Security National Infrastructure Protection Plan, 2009
- National Fire Protection Association (NFPA) 1, *National Fire Code*, Current Edition (2012)
- NFPA 70, *National Electric Code*, Current Edition (2011)
- NFPA 110, *Standard for Emergency and Standby Power Systems* (2010)
- National Science and Technology Council (NSTC) Committee on Technology, *Submetering of Building Energy and Water Usage*, October 2011

The overlay should be evaluated for revision when government or industry issue new guidance that may impact designation of ICS related security controls.

2. Characteristics and Assumptions

ICSs are physical equipment-oriented technologies and systems that deal with the actual running of plants and equipment. They include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout the nation's infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICSs range from non-critical systems, such as Building Automation Systems (BASs) or Building Control Systems (BCS) to critical systems such as the electrical power grid, Emergency Management Information Systems (EMISs), Safety Interlock System (SIS), Intelligent Transportation Systems (ITS) and Electronic Security Systems (ESSs). This overlay applies to both non-critical and critical ICSs, as the non-critical ICSs can be an entry point into the critical systems (note: Some BAS and BCS may be critical depending upon mission mapping).

Within the controls systems industry, ICSs are often referred to as Operational Technology (OT) systems. Historically, the majority of OT systems have been proprietary, analog, vendor supported, and have not been internet protocol (IP) enabled. Systems' key components, such as Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Physical Access Control Systems (PACs), Intrusion Detection Systems (IDSs), closed circuit television (CCTV), fire alarm systems, and utility meters are now becoming digital and IP enabled. OT systems use Human Machine Interfaces (HMIs) to monitor the processes, versus Graphical User Interfaces (GUIs) for IT systems, and most current ICSs and subsystems are now a combination of OT and Information Technology (IT).

Figure 1 is a typical electrical SCADA-type system which shows the HMI at the operators console, the transmission system infrastructure, and the RTU in the field. At the substation and building level, the meters are monitored in a local Energy Operations Center (EOC) or Regional Operations Center (ROC), which use real time analytics software to manage the energy loads and building control systems down to the sensor or actuator device level.

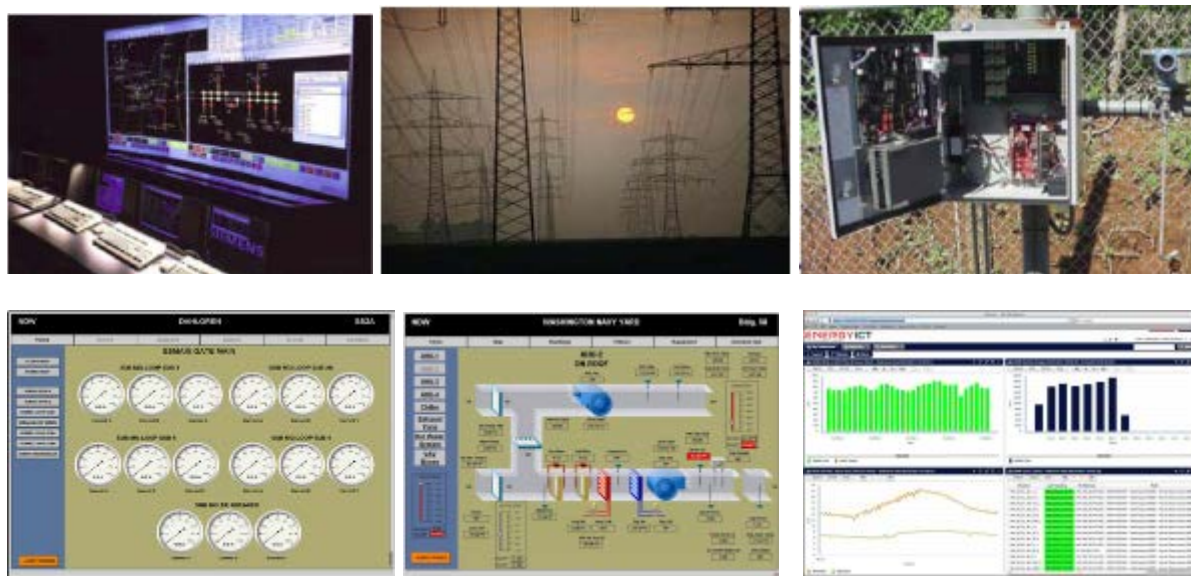


Figure 1 – ICS Human Machine Interface, System, Advance Meter Infrastructure (AMI), Building Control Network (BCN), Remote Terminal Unit²

A comparison of IT versus OT systems is provided in the table below:

Table 1 – IT vs. OT Systems Comparison

	Information Technology	Operational Technology
<u>Purpose</u>	Process transactions, provide information	Control or monitor physical processes and equipment
<u>Architecture</u>	Enterprise wide infrastructure and applications (generic)	Event-driven, real-time, embedded hardware and software (customized)
<u>Interfaces</u>	GUI, Web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices
<u>Ownership</u>	CIO and computer grads, finance and admin. depts.	Engineers, technicians, operators and managers

² The pictures and devices shown in this Overlay are for illustrative purposes only and are intended to show typical field devices that are the core elements of OT. This Overlay document does not endorse any specific vendor or product.

<u>Connectivity</u>	Corporate network, IP-based	Control networks, hard wired twisted pair and IP-based
<u>Role</u>	Supports people	Controls machines

An emerging concept in technology refers to the hybrid OT and IT ICSs as cyber-physical systems (CPSs). As defined by the National Science Foundation, cyber-physical systems:

“[are] engineered systems that are built from and depend upon the synergy of computational and physical components. Emerging CPSs will be coordinated, distributed, and connected, and must be robust and responsive. The CPS of tomorrow will need to far exceed the systems of today in capability, adaptability, resiliency, safety, security, and usability. Examples of the many CPS application areas include the smart electric grid, smart transportation, smart buildings, smart medical technologies, next-generation air traffic management, and advanced manufacturing.”

As these new technologies are developed and implemented, this Overlay will be updated to reflect advances in related terminology and capabilities. This Overlay presently focuses on the current generation technologies already in the field, and the known technologies likely to remain in inventory for at least the next ten years.

ICSs differ significantly from traditional administrative, mission support and scientific data processing information systems, and use specialized software, hardware and protocols. ICSs are often integrated with mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities. The “front end” portions of these ICSs resemble traditional information systems in that they use the same commercially available hardware and software components. While the majority of an ICS system still does not resemble a traditional information system (IS), the integration of the ICS’s “front end” with an IS introduces some of the same vulnerabilities that exist in current networked information systems.

ICSs can have long life spans (in excess of 20 years) and be comprised of technologies that in accordance with Moore’s law suffer rapid obsolescence. This introduces two significant issues: first, depending upon the relative age and isolation of the system, there may not be a patch or upgrade path for components of the system, and second, attempting to patch the component or employing modern scanning methods might disrupt the system and/or cause failure. ICSs have experienced complete system shutdown when an intrusion detection system (IDS) or host-based scanning system (HBSS) scan is performed on an otherwise operational ICS. For an ICS, updates should be delayed until after a thorough analysis of deployment impact has been completed. This has the potential to stretch out security update timeliness and require flexibility in security control compliance measurement and enforcement.

While many security controls from the NIST SP 800-53 baselines can be applied to an ICS, how and where they are implemented varies, primarily because of technical and operational constraints. Interconnections between ICSs and organizational networks and business systems expose ICSs to exploits and vulnerabilities, and any attempts to address these exploits and vulnerabilities must consider the constraints and requirements of the ICS.

In this Overlay, the terms IT and OT are used to define the Layers Architecture and delineate the boundary between the ICS Enclave and the CNNS IS. Figure 2 provides a schematic architecture

and definition of layers for ICSs that follow the American National Standards Institute (ANSI)/International Society of Automation (ISA) process, but include additional components/layers not shown in the ISA architecture.

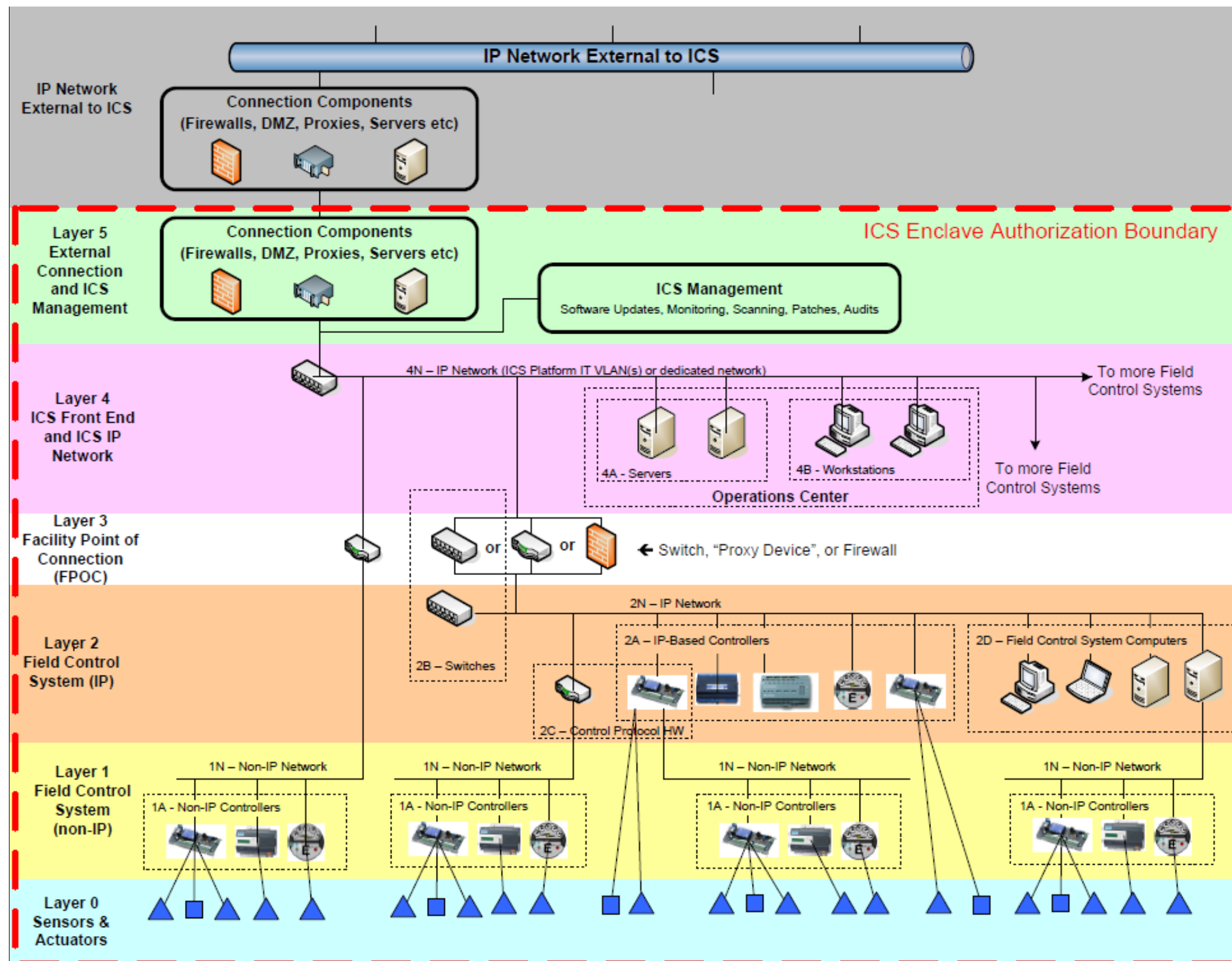


Figure 2 – ICS Layers

The ICS Architecture is described in five Layers (and multiple sub-layers), where each layer represents a collection of components that can be logically grouped together by function and Information Assurance approach. There are several critical considerations to the Layered Architecture:

- 1) Not every implementation of an ICS will make use of every layer;
- 2) The same device may reside in different layers, depending on its configuration. For example, some BACnet controllers may support different networks based on a dual in-line packet (DIP) switch, and thus the same device could physically be installed on a piece of equipment, but reside in either Layer 1 or Layer 2.
- 3) In some cases, a single device may simultaneously fit into two principal layers. For example, a device may act as both a Layer 2 controller and a Layer 3 FPOC.
- 4) In many cases, a device will fit multiple sub-layers within the same principal layer, usually within Layer 2. For example, a Layer 2A BACnet controller will often act as a Layer 2C router to a Layer 1 network beneath it.
- 5) A single device may belong in different layers, depending on the specific architecture. For example, the Layer 2A/2C controller in the example above may, in a small system, be the only IP device, in which case it is *also* the Layer 3 FPOC. In a larger system, there would be multiple IP devices and the upstream IP device (switch or router) would be the Layer 3 FPOC.

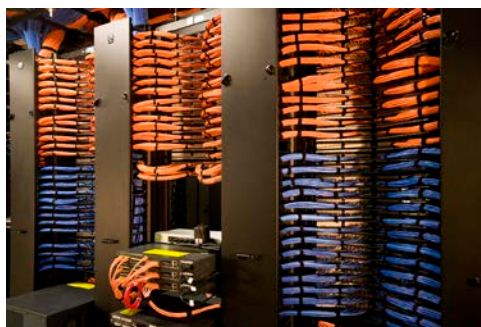
The ICS layer architecture is used to define the accreditation boundary for OT systems and is a logical representation of the OT network. The actual physical system can span many miles; for example, locks and dams, pipelines, electric transmission and distribution systems can all have many non-contiguous components, and there are a number of protocols commonly used by ICSs to allow the devices within the layers to communicate both horizontally and vertically. Some of these protocols are:

- LonWorks
- BACnet
- Modbus
- DNP 3

Illustrations of the components and devices that utilize these protocols are:



5: A Layer 5 Demarcation Point (DEMARC) or Point of Presence (POP) where the external IS meets the internal OT interface.

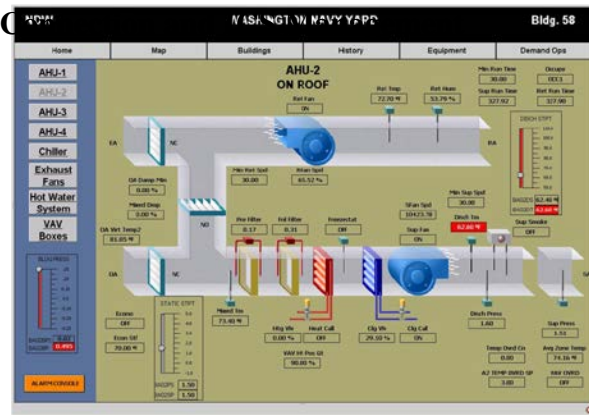


5: Layer 5 OT racks and servers located in a Facility Operations Center (FOC)/Security Operations Center (SOC)/Energy Operations Center (EOC).



Figure 3 - Layer 5: "External"

4-A: A Layer 4 OT rack and servers located in an EOC or FOC.



4-B: Workstation or wall display of HMI for the ICS.

Figure 4 - Layer 4: ICS Front End and IP Network




3-FS: A Layer 3 FPOC gateway (application layer proxy). The Layer 4 network is Modbus over IP over 10/100 Mbps Ethernet. The Layer 1 network is proprietary over proprietary 2-wire media. Note this is the same device as in 2C-FS.




3-LIP: A Layer 3 FPOC router between 3 LonTalk networks: Layer 1 Lon over TP/FT-10, Layer 1 Lon over TP/FT-10, and Layer 4 Lon over IP over Ethernet.


Figure 5 – Layer 3: Facility Points of Connection (FPOCs)



2A-CC: Very basic Layer 2A controller capable of monitoring six analog inputs and reporting their values to the network and setting two outputs. Network is BACnet over IP over 10/100 Mbps.




2A-JACE: Programmable Layer 2A controller. No analog inputs or outputs. Primary networking is proprietary over IP over 10/100 Mbps Ethernet. For a small field control system, this might be the Layer 3 FPOC.




2C-FS: A Layer 2C gateway (application layer proxy). The Layer 2 network is Modbus over IP over 10/100 Mbps Ethernet. The Layer 1 network is proprietary over proprietary 2-wire media.

Figure 6 – Layer 2: IP portion of the Field Control System



1A-VAV: Variable Air Volume (VAV) box controller with multiple analog inputs and outputs. Also incorporates dedicated actuator and pressure sensor (normally Layer 0 devices). Network is LonTalk over TP/FT-10 media at 78 Kbps.



1A-LGR: Programmable controller with no analog inputs or outputs. Primary network is BACnet over Ethernet (not IP) media at 10/100 Mbps. Also supports BACnet over MS/TP media and proprietary protocol over RS-485 media. Can also be in Layer 2.



1N-Lswitch: LonTalk router between 2 TP/FT-10 (media) network segments. Also has RS-232 console port for configuration (generally not used).

Figure 7 – Layer 1: Non-IP portion of the Field Control System

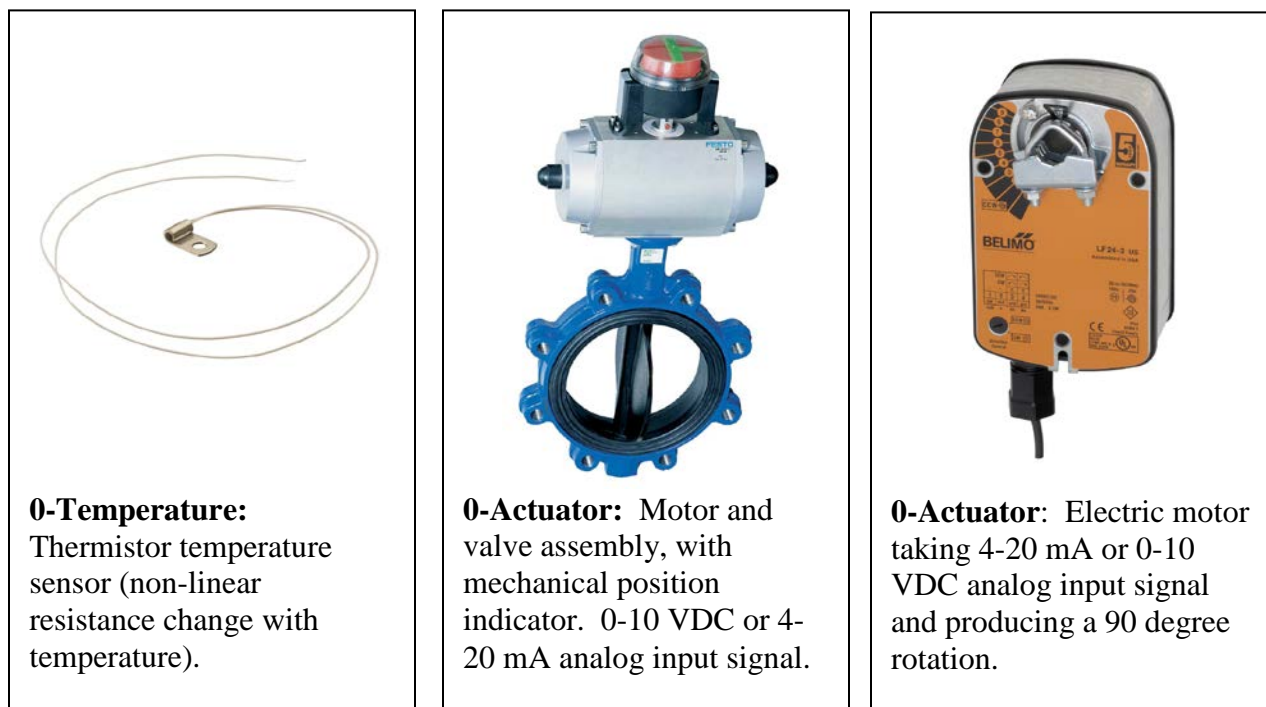


Figure 8 – Layer 0: Sensors and Actuators

Table 2 – ICS Architecture

Layer	Functional Description	Implemented Via	Installed By	Example Components	Security Control Considerations
<div>5</div> <div>"External" Connection and ICS Management</div> <div>(External Connection Between ICS and IP Network External to Enclave)</div> <div>ICS Management</div>	<p>In many Architectures, this layer provides the enclave boundary defense between the ICS (at Layers 4 and below) and IP networks external to the ICS. (In other architectures, this boundary defense occurs in the external network). In many cases, there is a component within the ICS which would reside in Layer 5.</p> <p>This layer may be absent for a variety of reasons. For example, there may not be an external connection, or the connection may be handled in the external network.</p> <p>Generally speaking from the perspective of ICS functionality, this connection should be severely restricted, if not eliminated entirely. The ICS can function in a completely isolated configuration. Additional functionality allowed through external connections includes:</p> <ul style="list-style-type: none">• Sending alarm notification using outbound access to a SMTP email server.• Upload of historical data and meter data to an enterprise server using outbound HTTP/HTTPS access for uploading. <p>Often it is desirable to allow inbound HTTP from web clients (essentially Layer 4B clients, but on the external network) to the Layer 4A server, but this is not required.</p>	<ul style="list-style-type: none">• Firewalls• DMZ/Perimeter Networking• Proxy Servers• Domain Controller, etc.	<ul style="list-style-type: none">• IT and communications staff and contractors.	<ul style="list-style-type: none">• Wide Area Networks (WANs)• Metropolitan Area Networks (MANs)• Local Area Networks (LANs)• Campus Area Networks (CANs)• Virtual Private Networks (VPNs)• Point of Presence• Demarcation Point or Main Point of Presence (MPoP)	<p>This Layer should implement a "deny all /permit exception" policy to protect the ICS from the external network and the external network from the ICS.</p>

Table 2 – ICS Architecture

Layer	Functional Description	Implemented Via	Installed By	Example Components	Security Control Considerations
<div>4</div> <div>ICS Front End and IP Network</div> <div>4N – ICS IP Network – ICS Network</div> <div>4A – Monitoring and Control (M&C) Server (Including Any Web Server, Data Historian, Etc.)</div> <div>4B – Operator’s Work Station (OWS)</div>	<p>(Layer 4A and 4B) The multi-facility operator interface for the system. This is typically a web-based client-server system with the clients at Layer 4B and the server(s) at Layer 4A.</p> <p>Some functions of the ICS are:</p> <ul style="list-style-type: none">• Providing graphical screens for monitoring and control of the system• Allowing operators to schedule systems, set up historical trends, and respond to alarm conditions• Provide for and support global control and optimization strategies that are impractical to implement within the control systems• Provide connections to external systems such as maintenance scheduling programs and proactive diagnostics <p>The Layer 4N network is the network that connects multiple facility networks into a common base-wide network.</p>	<p>The Layer 4N network may either be a physically dedicated network or a dedicated virtual local area network (VLAN) utilizing the standard base-wide IP network as a transport layer.</p>	<ul style="list-style-type: none">• The network (Layer 4N) is typically government furnished.• The computers, especially the clients in Layer 4B, are often government furnished.• The software application is typically provided, installed and configured by the controls vendor. <p><i>Note that later connections between the ICS and additional field control systems projects may be made by a variety of mechanisms.</i></p>	<ul style="list-style-type: none">• OT server racks• GUI and HMI displays• Fire alarm panels• Land Mobile Radio (LMR) and Radio base stations <p><i>The OT racks, hardware and software will likely be located in an EOC, Campus Wide Operations Center (CWOC), FOC, SOC, or ROC.</i></p>	<p>Layer 4 is where the ICSs most closely resemble a “standard” information system, and most security controls can be applied at this layer. It’s critical to remember that an ICS is NOT a standard IS, however, and that controls must be applied in such a way so as to not hamper the availability of the system. For example, some ICSs require software updates from the manufacturer prior to the implementation of a Java patch, and controls relating to the application of patches must not be implemented in a manner that requires automatic or immediate patching without ensuring that this won’t cause the system to go offline.</p>

Table 2 – ICS Architecture

Layer	Functional Description	Implemented Via	Installed By	Example Components	Security Control Considerations
3 Facility Points of Connection (FPOCs)	<p>For each field control system, the FPOC is the specific single demarcation point in the OT system between that field control system and the front end system. It may be a gateway that translates data from one protocol to another. It generally has security controls in that it restricts access (by user, protocol, or specific commands) between layers above and layers below. From a control architecture perspective, it often looks and functions identically to a Layer 2C device. For a non-IP network (Layer 1), the FPOC is the device that connects the non-IP network to IP. For an IP network (Layer 2), the FPOC is the device located at the single connection point between the IP network in Layer 2 and the ICS IP network; this is typically the upstream IP networking hardware switch or router.</p>	<p>Wide variety of devices depending on the specific architecture and protocols used:</p> <ul style="list-style-type: none">• Ethernet switch or IP router (any place there is a Layer 2 IP network)• Local operation network (Lon) (field control network) to Lon/IP router• Dedicated hardware gateway between proprietary field network and BACnet/IP• Application proxy providing enclave boundary defense between non-critical Lon/IP ICS network and a critical Lon field control network• Layer 2D stand-alone front end for a local field control system	<ul style="list-style-type: none">• Installation network staff• Controls contractor• System integrator when the field control system is connected to (integrated with) the front end system.	<ul style="list-style-type: none">• Standard IT Ethernet switch• Echelon iLON 600 router• ALC LGR BACnet controller (IP to MS/TP router)	<p>This device is critical from a security controls perspective as it is where the dedicated local field control network connects to the local network. Normally, securing this device protects the local network from the local field systems (which often have a difficult time meeting security controls). Occasionally, where there is a critical field control system, this device can protect the more critical field control system from the less-secure local system (i.e., where there are 99 non-critical systems and 1 critical one, isolate the 1 from the 99 rather than try and secure the 99).</p> <p>This device should, in effect, have a "deny all/permit by exception" policy applied. In many cases, this is inherent in the design of the network – a Layer 1 (non-IP) network inherently "denies" all protocols other than its specific control protocol. In other cases, this device may be a gateway ("application layer proxy") that does not permit any networking traffic through it, and only supports a very limited set of control functionality to pass. These devices tend to be "dumb" devices and may not support many of the security controls, however, the critical "deny all / permit by exception" approach should be designed into the device. Where this layer is an upstream IT device, it should be set up with the most restrictive access control list (ACL) possible.</p>
	<p>In many cases, there is a <i>single</i> Layer 2A controller in the system (generally with a Layer 1 network beneath it). In these cases, we may consider the controller the FPOC, or we may consider the upstream IP networking hardware (switch or router) to be the FPOC. Similarly, a device normally at Layer 2C could be the Layer 3 FPOC. Finally, we may have a Layer 2D computer which is the only IP device in the stand alone system; this may be considered the FPOC.</p>				
	<p><i>Note that a large system may have hundreds of these FPOC devices, one at each connection of a field control system to the local network.</i></p>				

Table 2 – ICS Architecture

Layer	Functional Description	Implemented Via	Installed By	Example Components	Security Control Considerations
<div>2</div> <div>IP Portion of the Field Control System</div> <div>2N – IP Field Control Network (FCN)</div> <div>2A – IP Based Networked Controllers</div> <div>2B – FCN Ethernet Hardware</div> <div>2C – IP to Non-IP Control Protocol Routers or Control Protocol Gateways</div> <div>2D – Field Control System Local Computers (Front-Ends, Engineering Tools)</div>	<p>(Layer 2A) This Layer (along with Layer 1) is where the control logic resides and where it gets converted to and from electrical signals and can have the first IP connections. This is the portion of the OT system where:</p> <ul style="list-style-type: none">• Analog electrical signals (from sensors) get converted to digital signals via A-D converters (although not all controllers will have hardware inputs).• Digital information is converted to analog electrical signals (to actuators) via D-A converters (although not all controllers will have hardware outputs).• Digital information is transmitted and received over a network.• Digital information is processed according to a user-defined sequence to generate new digital information.• These devices may incorporate integral Layer 0 sensors and actuators. For example, the VAV box controller shown incorporates an electric actuator. <p><i>Note that while there is exchange of data over the network, good design practice dictates that most of the data processing occurs using local sensor data and local actuator outputs; the system is designed to minimize dependence on networked data.</i></p> <p>Layer 2C may also contain control protocol routers and/or control protocol gateways between Layers 1 and 2. These devices are generally physically part of a Layer 2A controller. In addition, from a security controls perspective, they appear much the same as a Layer 2A controller.</p> <p>(Layer 2D) In some cases, for either legacy or stand-alone systems (not necessarily isolated, but stand alone in that they do not rely on another system, such as an ICS), the front end operator interface may be physically local to that system. In this case, the operator interface is considered to be part of Layer 2 since it does not ride over the ICS IP network.</p>	<p>(Layer 2A) Firmware-based dedicated digital processors, typically equipped with multiple analog inputs and outputs and corresponding A-D and D-A converters. These devices are constrained by cost to have the minimal functionality for the application and are very constrained in RAM, processing power, and network I/O. In addition, these devices come in a vast variety of architectures, processors, vendors, and firmware. Aside from the fact that they use IP and are generally more powerful than Layer 1A devices, they are otherwise identical to Layer 1A devices. Many of these devices are available as either Layer 1A or 2A devices, where the hardware is identical except for the transceiver; some can even be field-configured for one or the other.</p> <p>The Layer 2N network is generally Ethernet and the Layer 2B network hardware is standard IT network hardware, though generally with reduced functionality. For example, there may not be any requirement for remotely managed switches. Similarly, there is seldom a need for an IP router, since field control systems generally reside within a single (private) IP subnet.</p> <p>The Layer 2 network (2N and 2B) uses IP, generally over Ethernet, such as BACnet/IP or Lon/IP.</p> <p>While Layer 2D components functionally act similarly to computers at Layer 4, the fact that they are local (and dedicated) to a specific control system means that from a security controls perspective, they are better addressed as Layer 2 components. Layer 2D computers will often have another network logically beneath them, most often a non-IP network (and thus they will also function as Layer 2C devices).</p>	<ul style="list-style-type: none">• Controls contractor during installation or renovation of underlying mechanical or electrical system• Generally during new building construction or major renovation	<ul style="list-style-type: none">• Layer 2A:<ul style="list-style-type: none">◦ Major air handling unit (AHU) controller◦ Supervisory Controller◦ Electric meter (IP)• Layer 2B:<ul style="list-style-type: none">◦ "Dumb" Ethernet switch• Layer 2C:<ul style="list-style-type: none">◦ BACnet MS/TP to BACnet/IP router◦ Gateway between non-standard, non-IP protocol and a standard control protocol over IP• Layer 2D:<ul style="list-style-type: none">◦ Control system at a central plant where the nature and criticality of the system requires a local operator interface	<p>Since it contains a variety of components from controllers (Layer 2A) to computers (Layer 2D), there is a variety of security control considerations for this layer. Many of the controllers will have the same limitations as the controllers in Layer 1, where most security controls cannot/or will not apply to them. Some controllers will have significantly more capability, however, and additional controls will be applicable. In either case, the controllers should disable any network connections or services not required for operation of the OT system.</p> <p>In some systems, particularly legacy systems, the computers at Layer 2D may be running an older operating systems and may not support some of the security controls. In this case, the controls which can be applied without negatively affecting the availability of the system should be applied, and mitigating controls and measures should be taken when otherwise needed. Generally this will consist of further isolating the legacy systems.</p>

Table 2 – ICS Architecture

Layer	Functional Description	Implemented Via	Installed By	Example Components	Security Control Considerations
<div>1</div> <div>Non-IP Portion of the Field Control System</div> <div>1N – Network (Non-IP)</div> <div>1A – Networked Controllers (Non-IP)</div>	<p>(Layer 1A) This is where the control logic resides and gets converted to/from analog electrical signals, as well as the portion of the OT system where:</p> <ul style="list-style-type: none">• Analog electrical signals (from sensors) get converted to digital signals via analog-to-digital (A-D) converters*• Digital information is converted to analog electrical signals (to actuators) via digital-to-analog (D-A) converters *• Digital information is transmitted and received over a network• Digital information is processed according to a user-defined sequence to generate new digital information• Devices may incorporate integral Layer 0 sensors and actuators. For example, a VAV box controller incorporates an electric actuator <p><i>*Note that not all controllers will have hardware inputs.</i></p> <p><i>Note that while there is exchange of data over the network, good design practice dictates that most of the data processing occurs using local sensor data and local actuator outputs; the system is designed to minimize dependence on networked data.</i></p> <p>(Layer 1N) The Layer 1 network (media and hardware) does not use IP. It uses a variety of media at Layers 1 and 2 (some standard, some not) and it uses Layer 3 protocols other than IP. Some examples are:</p> <ul style="list-style-type: none">• BACnet over MS/TP, or BACnet over ARCnet• LonTalk over TP/FT-10 or LonTalk over TP/XF-1250• Modbus over RS-485 <p>For this reason, it is generally very specific to the control application and cannot be used for "standard" IT protocols and applications.</p>	<p>(Layer 1A) Firmware based dedicated digital processors, typically equipped with multiple analog inputs and outputs and corresponding A-D and D-A converters. These devices are constrained by cost to have the minimal functionality for the application and are very limited in random access memory (RAM), processing power, and network input/output (I/O). In addition, these devices come in a vast variety of architectures, processors, vendors, and firmware.</p> <p>(Layer 1N) The network media and hardware is similarly dedicated to that specific control protocol. There are Layer 2 and Layer 3 network devices made by a variety of vendors.</p>	<ul style="list-style-type: none">• Controls contractor during installation or renovation of underlying mechanical or electrical system• Generally during new building construction or major renovation	<ul style="list-style-type: none">• VAV box controllers• Networked (non-IP) electric meter• Intelligent (networked) thermostat• LonWorks TP/XF-1250 (media) to TP/FT-10 (media) Layer 3 router	<p>Since devices (controllers) in this tier tend to be simpler devices, and often have few security controls that can be applied, particularly after the system has been designed and installed. Some basic controls/measures that can be applied at this tier include:</p> <ul style="list-style-type: none">• Disabling (or at a minimum prohibiting) secondary network connections (connections other than to the Layer 1 network)• The use of passwords on devices such as displays (to the capability supported by the device – many of which do not permit 14 character passwords, for example)• The application of physical security measures – which will be dictated and implemented by the underlying equipment

Table 2 – ICS Architecture

Layer	Functional Description	Implemented Via	Installed By	Example Components	Security Control Considerations
<div>0</div> <div>Sensors and Actuators</div> <div>“Dumb” Non-Networked Sensors and Actuators</div>	<p>The interface between the OT system and the underlying controlled process/equipment where electrical signals in the control system get converted to/from physical values and actions in the underlying controlled system.</p>	<p>Devices which:</p> <ul style="list-style-type: none">• Convert physical properties (e.g., temperature, pressure, etc.) to an analog electrical signal*• Take an analog electrical signal* and produce a physical action (e.g., open/close a valve or damper, etc.) <p><i>* Note that these electrical signals are purely analog – there are no digital signals at this tier and hence no networking. Also note that there are "smart" sensors, which include a sensor (or actuator) with a controller. These devices are considered to be Layer 1A or Layer 2A devices.</i></p>	<ul style="list-style-type: none">• Controls contractor during installation or renovation of underlying mechanical or electrical system• Generally during new building construction or major renovation	<ul style="list-style-type: none">• Temperature sensor (thermistor, Resistant Temperature Detectors (RTD))• Mechanical actuator (for damper or valve)• Thermostat• Pressure sensor• Pulse-output meter	<p>In general, management and operational controls such as Physical Security, Access Control, and Security Controls may still apply to this tier. These devices are physically attached to the mechanical/electrical system and physical security is dictated and implemented based on the physical access to the equipment. Utility vaults, Mechanical, Electrical, Plumbing rooms, Pump Stations, etc., should be secure and only authorized personnel should have access. These devices, while they do not have network communication and no “intelligence” in the components at this layer, can cause physical damage, for example a valve left in the “ON” position.</p>

2.1 Operational Criticality

For ICS systems, it is particularly important to recognize that *availability* is often much more significant than *confidentiality* or *integrity*. While the emphasis may be on confidentiality or integrity for the vast majority of current systems, it's not inviolable – as recent cyberattacks such as Stuxnet have shown.

Additionally, ICSs generally span a range rather than have a distinct cutoff for operational criticality. For example, an electric utility SCADA system may be a primary system that supports a Critical Infrastructure Data Center system, with secondary generator back up. If primary power is lost, the system will have degraded capability and the restoration of the primary electric source is essential for long-term operations. High Impact National Security Systems (NSS) such as operational, life and public safety functions typically cannot experience loss of power, water, or network connectivity for more than a few minutes.

A Low Impact ICS addresses the “80%” non-critical systems (i.e., typical office, administrative, housing, warehouse, buildings or vehicle charging/storage control systems, etc.) that can remain nonoperational or degrade for a relatively long period of time without substantially affecting organizational missions. Many of the Moderate and High Impact ICSs are listed as Critical Infrastructure and Key Resources (CIKR). Figure 9 illustrates the conceptual types of ICS and operational criticality.

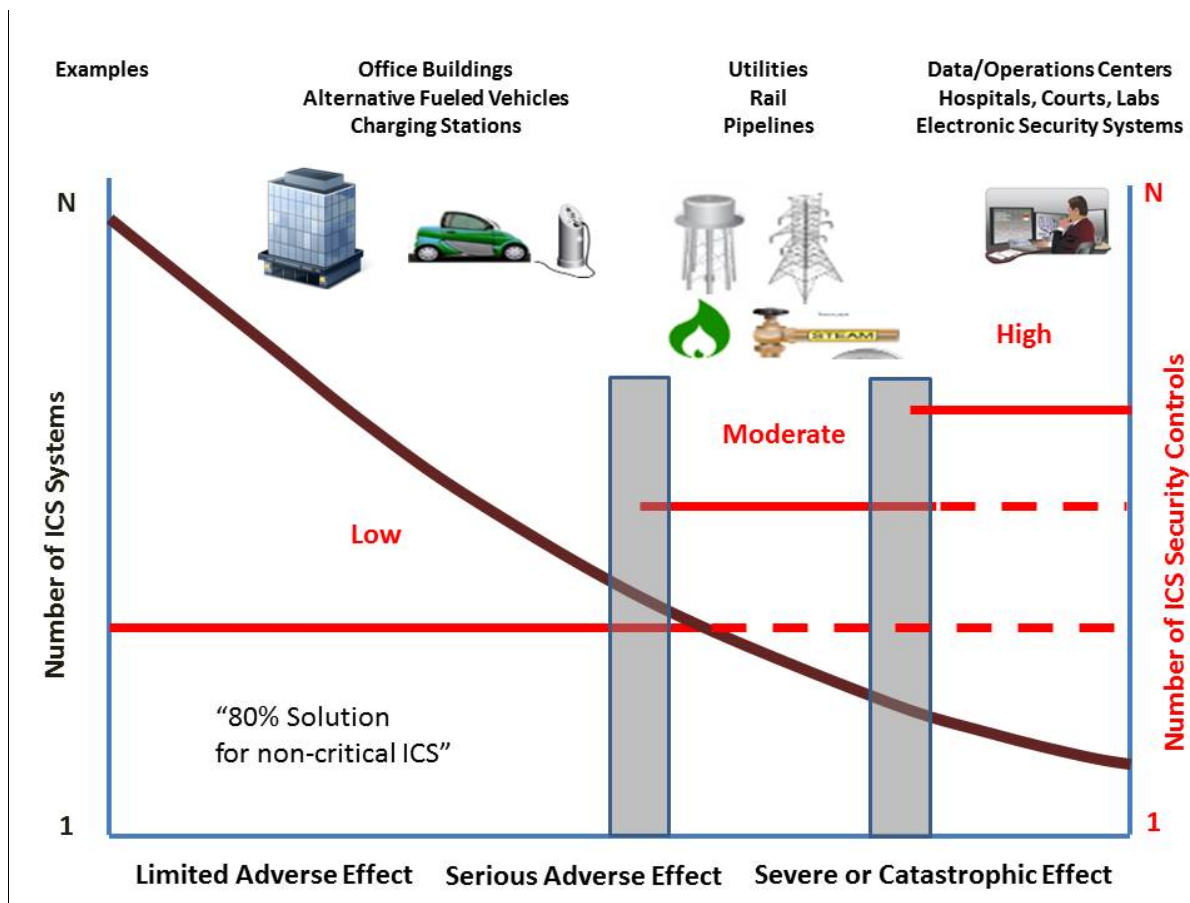


Figure 9 – ICS Operational Criticality

For this Overlay, the ICS system’s authorization boundary is defined as the ICS Enclave. An ICS Enclave can have multiple Sub-Enclaves; for example, a building may be the ICS Enclave as well as the BAS, EMS, PAS etc. systems. A campus may be designated as the ICS Enclave and the utility SCADA, Buildings, Rail, Exterior Lighting and Messaging systems, etc. would be the ICS Sub-Enclaves.

3. Applicability

CNSS agencies are required to maintain a contingency plan and define the recovery and reconstitution times for mission critical assets. Building and life safety codes also define minimum runtimes for emergency and standby power systems. For this initial overlay version 1, “Availability” is used as the primary applicability and justification rational.

The first step in determining applicability is to create an accurate map of all networked and isolated ICS assets and associated communication connections. The security category for an ICS is determined using the instructions in CNSSI No. 1253, Categorization Section 2.1. Many individual ICS systems may fall well below the Low, Low, Low (LLL) baseline, but as an aggregation within an ICS Enclave or Sub-Enclaves, they may each meet the threshold requiring the use of the overlay.

Establishing ICS applicability criteria for integrity (I) and confidentiality (C) is extremely challenging and very few current ICS systems have the same level of I and C capabilities as IT systems. Many ICSs cannot support even basic scanning or automated patch management. Developing robust I and C applicability criteria is a current research area and will be addressed in future overlays.

In addition to the security categorization, if the answer is “yes” to the following question, then apply the ICS overlay. This overlay only requires assessment and compliance at the control family level. CNSS agencies can elect to use NIST SP 800-53 Rev 3 Appendix I, ICS security controls for additional ICS-specific supplemental guidance and enhancements.

1. Is the system an industrial control system, based on the definition in NIST SP 800-82, *Guide to Industrial Control Systems Security*?

4. Summarized Overlay Control Specifications

The table below contains a summary of the security control specifications as they apply in this overlay. The symbols used in the table are as follows:

- A plus sign (“+”) indicates the control should be selected.
- Two dashes (“--”) indicates the control should not be selected.
- The letter “E” indicates there is a control extension³.
- The letter “G” indicates there is supplemental guidance, including specific tailoring guidance if applicable, for the control.
- The letter “V” indicates this overlay defines a value for an organizational-defined parameter for the control.

³ Control extensions will be submitted to NIST for consideration when updating the 800-53 catalog.

- The letter “R” indicates there is at least one regulatory/statutory reference that requires or prohibits the control selection or that the control helps to meet the regulatory/statutory requirements.

Table 3 – ICS Systems Overlay Security Controls

INDUSTRIAL CONTROL SYSTEMS					
CONTROL	SELECTED	CONTROL	SELECTED	CONTROL	SELECTED
AC-1	+	IA-3	+	SA-2	+
AC-2	+	IA-4	+	SA-3	+
AC-3	+	IA-5	+	SA-4	+
AC-5	+	IA-6	+	SA-5	+
AC-6	+	IA-7	+	SA-6	+
AC-7	+	IA-8	+	SA-7	+
AC-8	+	IR-1	+	SA-8	+
AC-10	+	IR-2	+	SA-9	+
AC-11	+	IR-4	+	SA-11	+
AC-14	+	IR-5	+	SC-1	+
AC-17	+	IR-6	+	SC-2	+
AC-18	+	IR-7	+	SC-3	+
AC-19	+	IR-8	+	SC-5	+
AC-20	+	MA-1	+	SC-6	+
AC-22	+	MA-2	+	SC-7	+
AT-1	+	MA-4	+	SC-8	+
AT-2	+	MA-5	+	SC-9	+
AT-3	+	MA-6	+	SC-10	+
AT-4	+	MP-1	+	SC-12	+
AU-1	+	MP-2	+	SC-13	+
AU-2	+	MP-5	+	SC-14	+
AU-3	+	MP-6	+	SC-15	+
AU-4	+	PE-1	+	SC-18	+
AU-5	+	PE-2	+	SC-19	+
AU-6	+	PE-3	+	SC-20	+
AU-7	+	PE-4	+	SC-21	+
AU-8	+	PE-6	+	SC-22	+
AU-9	+	PE-7	+	SC-23	+
AU-11	+	PE-8	+	SC-28	+
AU-12	+	PE-11	+	SC-33	+
CA-1	+	PE-12	+	SI-1	+
CA-2	+	PE-13	+	SI-2	+
CA-3	+	PE-14	+	SI-3	+
CA-5	+	PE-15	+	SI-4	+
CA-6	+	PE-16	+	SI-5	+
CA-7	+	PE-17	+	SI-6	+

INDUSTRIAL CONTROL SYSTEMS					
CONTROL	SELECTED	CONTROL	SELECTED	CONTROL	SELECTED
CM-1	+	PL-1	+	SI-7	+
CM-2	+	PL-2	+	SI-8	+
CM-3	+	PL-4	+	SI-9	+
CM-4	+	PL-5	+	SI-12	+
CM-5	+	PS-1	+	SI-13	+
CM-6	+	PS-2	+	PM-1	+
CM-7	+	PS-3	+	PM-2	+
CM-8	+	PS-4	+	PM-3	+
CP-1	+	PS-5	+	PM-4	+
CP-2	+	PS-6	+	PM-5	+
CP-3	+	PS-7	+	PM-6	+
CP-4	+	PS-8	+	PM-7	+
CP-8	+	RA-1	+	PM-9	+
CP-9	+	RA-2	+	PM-10	+
CP-10	+	RA-3	+	PM-11	+
IA-1	+	RA-5	+		
IA-2	+	SA-1	+		

5. Detailed Overlay Control Specifications

This section is a comprehensive view of the security controls as they apply to this overlay, and the guidance provided in this section elaborates on the guidance given in NIST SP 800-53. For controls that should either be selected or not selected, a justification is given based on the defined overlay characteristics. In addition to justification, a security control may have other specifications that include control extensions, supplemental guidance (including specific tailoring guidance), parameter values, and regulatory/statutory references. On occasion, a security control may only have supplemental guidance as its applicability is not absolute. This section is summarized in Table 3.

The security controls and control enhancements are likely candidates for tailoring, with the applicability of scoping guidance indicated for each control/enhancement. The citation of a control without enhancements (e.g., AC-17) refers only to the base control without any enhancements.

Organizations are required to conduct a risk assessment, taking into account the tailoring and supplementation performed in arriving at the agreed-upon set of security controls for the ICS, as well as the risk to the organization's operations and assets, individuals, other organizations, and the Nation being incurred by operation of the ICS with the intended controls. Based on an evaluation of the risk, the organization will further tailor the control set obtained using this overlay by adding or removing controls in accordance with the CNSSI 1253 process. The addition or removal of controls during tailoring requires justification.

CNSSI 1253, *Appendix I: Industrial Control Systems Security Controls, Enhancements, And Supplemental Guidance*, states, "adoption of National Institute of Standards and Technology

Special Publication 800-53, Revision 3, Appendix I, is not mandatory and is solely at the discretion of national security community departments and agencies, at this time, pending further applicability by the national security community.”

NIST SP 800-53 Rev 3, *Appendix I*, provides ICS Supplemental Guidance and is not repeated in this overlay. ICS supplemental guidance provides organizations with additional information on the application of the security controls and control enhancements to ICSs and the environments in which these specialized systems operate. The supplemental guidance also provides information as to why a particular security control or control enhancement may not be applicable in some ICS environments and why it may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls). Refer to Figure 3 – ICS Layers diagram, and Table 3 for the Layer definitions.

Table 4 – ICSs Layers Definitions

Layer	Description
	IP Network External to ICS
5	"External" Connection and ICS Management
	"External" Connection (between ICS and IP Network External to ICS)
	Platform IT System Management
4	ICS Front End and IP Network
4N	ICS IP network – ICS Network
4A	M&C Server (including any web server, data historian, etc.)
4B	OWS
3	FPOCs
2	IP Portion of the Field Control System
2N	IP FCN
2A	IP based networked controllers
2B	Field control network Ethernet hardware
2C	IP to non-IP control protocol routers or control protocol gateways
2D	Field control system local computers (front-ends, engineering tools)
1	Non-IP portion of the Field Control System
1N	Network (non-IP)
1A	Networked controllers (non-IP)
0	"DUMB" non-networked sensors and actuators

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Justification to Select: ICSs must have an access control policy that is updated annually, distinct and separate, from the IS systems. ICS access by vendors and maintenance staff can occur over a very large facility footprint or geographic area and into unobserved spaces such as mechanical/electrical rooms, ceilings, floors, field substations, switch and valve vaults, and pump stations. The ICS IP enabled nodes, field panel/controller, and HMI access should be restricted to authorized operators and maintenance personnel.

Applicability to ICS Layers: 2, 3, and 4.

AC-2 ACCOUNT MANAGEMENT

Justification to Select: ICSs must have account management that is updated annually, distinct and separate, from the IS systems. An ICS account is a separate account login from the IS workstation login. Many ICS components such as field devices cannot support automated account management and will require the use of non-automated methods.

Applicability to ICS Layers: 2, 3, and 4.

AC-3 ACCESS ENFORCEMENT

Justification to Select: ICS components are numerous and dispersed across a large geographic or facility footprint. With the increased connectivity of ICSs to other organizational systems and networks, access control enforcement is required to ensure that only authorized personnel have access to the ICS components and network.

Applicability to ICS Layers: 2, 3, and 4.

AC-5 SEPARATION OF DUTIES

Justification to Select: ICS are designed to ensure multiple operators can access the system to monitor and maintain the process/function. A single individual may have multiple privileges. Separation of duties is required to ensure no single operator can make the ICS exceed the design and operational parameters. Many ICS cannot support the separation of duties by virtue of physical location, ongoing operations and maintenance, and/or performance/availability requirements, and will require compensating controls.

Applicability to ICS Layers: All.

AC-6 LEAST PRIVILEGE

Justification to Select: ICSs require specific expertise to ensure the correct management, configuration, control and operation of the ICS. Implementing least privilege controls helps to ensure that the appropriate and authorized personnel have access to the systems.

Applicability to ICS Layers: 2, 3, and 4.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Justification to Select: Many ICSs must remain continuously on and operators must remain logged on to the system at all times. Response to unsuccessful login attempts will be implemented at both the operating system and the application levels. The Layer 2D level Field System computers may not be continually manned.

Applicability to ICS Layers: 2, 3, and 4.

AC-8 SYSTEM USE NOTIFICATION

Justification to Select: Many ICSs must remain continuously on and system use notification may not be supported, particularly at the Layer 2 level. For most ICS process or SCADA systems, system use notification is typically inherent within the HMI at the operator console. Field panels/controllers and standalone systems generally have some form of banner or system vendor name displayed for operator/maintenance login.

Applicability to ICS Layers: 2, 3, and 4.

AC-10 CONCURRENT SESSION CONTROL

Justification to Select: ICS can have multiple operators with concurrent session control and login. Concurrent sessions should be limited at the HMI to the operators and at the field level to technicians performing normal diagnostics and repair.

Applicability to ICS Layers: 2, 3 and 4.

AC-11 SESSION LOCK

Justification to Select: The ICS employs session lock to prevent access to specified workstations/nodes which may be critical to controlling ICS sensors.

Applicability to ICS Layers: All.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR UTHENTICATION

Justification to Select: In general, most applications that an operator or administrator would use require a type of authentication for access; however certain ICS non-IP sensor and actuator devices can require specific user actions that can be performed on the ICS system without identification or authentication.

Applicability to ICS Layers: 2, 3, and 4.

AC-17 REMOTE ACCESS

Justification to Select: Remote Access control policy and procedures are necessary to ensure that appropriate access to ICSs and information is maintained. There should be only one controlled path into an ICS with no backdoors or modems.

Applicability to ICS Layers: 2, 3, and 4.

AC-18 WIRELESS ACCESS

Justification to Select: ICSs can exist in all types of environments and geographic locations, some of which may not have a direct network connection available, and may only be supported by wireless connections.

Applicability to ICS Layers: 2, 3, and 4.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Justification to Select: ICSs can exist in all types of environments and geographic locations which may require mobile devices to configure and control ICS controllers, sensors and actuators. Many ICSs use Radio-frequency identification (RFID) and bar code scanners as part of the Operations and Maintenance (O&M) and preventive maintenance programs, and technicians may use a variety of portable scanners, diagnostic tools, and test devices.

Applicability to ICS Layers: 2, 3, and 4.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Justification to Select: ICSs have the potential to be interconnected with many different systems. It is important to document the terms, conditions, Memorandum Of Agreements (MOA), Service Level Agreements (SLA), etc. between the ICS and Service Providers to ensure appropriate access and information sharing.

Applicability to ICS Layers: 4 and 5.

AC-22 PUBLICLY ACCESSIBLE CONTENT

Justification to Select: In general, ICSs have no publically available information. However, many ICSs have embedded firmware default passwords and the operations manuals are publically available. Specific ICS installation design, configuration and operation should be restricted.

Applicability to ICS Layers: All.

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of security awareness, training policy and procedures as ISs. ICSs have become interconnected and a point of entry into the organization's network, and they also have unique and distinct vulnerabilities, mitigation, response, and recovery procedures that are different from an IS.

Applicability to ICS Layers: All.

AT-2 SECURITY AWARENESS

Justification to Select: ICSs require the same level of security awareness as an IS. ICSs have become interconnected and a point of entry into the organization's network, and also have unique and distinct vulnerabilities, mitigation, response, and recovery procedures that are different from an IS. Due to a large number of devices, geographic/facility footprint, and remote locations, all operators and technicians need to be aware of potential compromise of the ICS.

Applicability to ICS Layers: All.

AT-3 SECURITY TRAINING

Justification to Select: ICSs require the same level of security training as an IS. ICSs have become interconnected and a point of entry into the organization's network, and also have unique and distinct vulnerabilities, mitigation, response, and recovery procedures that are different from an IS. Due to large number of devices, geographic/facility footprint, and remote locations, all operators and technicians need ICS specific security training to be aware of potential compromise of the ICS.

Applicability to ICS Layers: All.

AT-4 SECURITY TRAINING RECORDS

Justification to Select: ICSs require the same level of security training as an IS. ICSs have become interconnected and a point of entry into the organization's network, and also have unique and distinct vulnerabilities, mitigation, response, and recovery procedures that are different from an IS. Due to large number of devices, geographic/facility footprint, and remote locations, all operators and technicians need ICS specific security training documented in the training record.

Applicability to ICS Layers: All.

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of audit and accountability policy and procedures as an IS. ICSs have become interconnected and a point of entry into the organization's network, and also have unique and distinct vulnerabilities, mitigation, response, and recovery procedures that are different from an IS. This control is required for the effective implementation of the ICS's selected security controls and control enhancements.

Applicability to ICS Layers: All.

AU-2 AUDITABLE EVENTS

Justification to Select: ICSs require analysis and documentation of auditable events similar to an IS, but will have unique logs and parameters. Maintaining the availability and integrity of the ICS is a primary consideration.

Applicability to ICS Layers: 2, 3, and 4.

AU-3 CONTENT OF AUDIT RECORDS

Justification to Select: ICSs require analysis and documentation of auditable events similar to an IS, but will have unique logs and parameters. The audit records of an ICS should enable validation so that the system is operating within parameter and, if compromised, supports the forensic analysis to restore services back to baseline.

Applicability to ICS Layers: 2, 3, and 4.

AU-4 AUDIT STORAGE CAPACITY

Justification to Select: ICSs require analysis and documentation of auditable events similar to an IS, but will have unique logs and parameters, and can generate an immense amount of data. ICSs typically require unique data compression and operational state analytics compared to an IS, with data typically maintained on the Historian.

Applicability to ICS Layers: All.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Justification to Select: ICSs require a response to an audit processing failure similar to an IS that captures software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

Applicability to ICS Layers: All.

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Justification to Select: ICSs require an audit review, analysis and report for indications of inappropriate or unusual activity similar to an IS, but will have unique reporting and response requirements. The Historian may not capture all inappropriate or unusual activity, and other scanning and intrusion detection systems will be required to ensure lower layer device and component integrity.

Applicability to ICS Layers: 2, 3, and 4.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Justification to Select: ICSs require an audit reduction and report for indications of inappropriate or unusual activity similar to an IS, but will have unique reporting and response requirements. The Historian may not capture all inappropriate or unusual activity, and other scanning and intrusion detection systems will be required to ensure lower layer device and component integrity.

Applicability to ICS Layers: 2, 3, and 4.

AU-8 TIME STAMPS

Justification to Select: ICSs require time stamps similar to an IS, but will use the ICS generated time.

Applicability to ICS Layers: 2, 3, and 4.

AU-9 PROTECTION OF AUDIT INFORMATION

Justification to Select: ICSs require the protection of audit information and audit tools from unauthorized access, modification, and deletion similar to an IS, but will be unique, and will typically be a combination of the Historian and other audit logs.

Applicability to ICS Layers: 2, 3, and 4.

AU-11 AUDIT RECORD RETENTION

Justification to Select: ICSs require audit record retention support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements similar to an IS, but will have unique retention times.

Applicability to ICS Layers: All.

AU-12 AUDIT GENERATION

Justification to Select: ICSs perform audit generation similar to an IS, but are separate and distinct. The ICS compiles audit records from all system and network components into a system-wide (logical or physical) audit trail that is time-correlated to the accreditation boundary, but will typically be a combination of the Historian and other audit logs.

Applicability to ICS Layers: All.

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

Justification to Select: ICSs require the same level of security assessment and authorization policy and procedures as IS. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

CA-2 SECURITY ASSESSMENTS

Justification to Select: ICSs require the same level of security assessment and authorization policy and procedures as an IS. ICSs have become interconnected and a point of entry into the organization's network, and also have unique and distinct vulnerabilities, mitigation, response, and recovery procedures that are different from an IS.

Applicability to ICS Layers: All.

CA-3 INFORMATION SYSTEM CONNECTIONS

Justification to Select: ICSs require system connections to other information systems outside of the authorization boundary and have unique Interconnection Security Agreements. ICSs have become interconnected and a point of entry into the organization's network, and also have unique and distinct vulnerabilities, mitigation, response, and recovery procedures that are different from an IS.

Applicability to ICS Layers: 4 and 5.

CA-5 PLAN OF ACTION AND MILESTONES

Justification to Select: ICSs require a Plan of Action and Milestones (POAM) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls, and to reduce or eliminate known vulnerabilities in the system. ICSs also have unique and distinct vulnerabilities, mitigation, response, and recovery procedures that are different from an IS.

Applicability to ICS Layers: All.

CA-6 SECURITY AUTHORIZATION

Justification to Select: ICSs require a security authorization distinct and separate from the IS. Authorization of an ICS system requires special skills and qualifications and an understanding of the unique operational and configuration of an ICS.

Applicability to ICS Layers: All.

CA-7 CONTINUOUS MONITORING

Justification to Select: ICSs are required to have a continuous monitoring program that allows the organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes.

Applicability to ICS Layers: All.

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of configuration management policy and procedures as an IS. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

CM-2 BASELINE CONFIGURATION

Justification to Select: The ICS's organization is required to develop, document, and maintain a current baseline configuration of the ICS, under configuration control, and maintain backup copies of the ICS. The baseline is essential for the restoration of the ICS should it fail or be compromised.

Applicability to ICS Layers: 2, 3, 4, and 5.

CM-3 CONFIGURATION CHANGE CONTROL

Justification to Select: The ICS is required to have configuration change control, which includes changes to components of the ICS, changes to the configuration settings for ICS products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. The ICS configuration is distinct and separate from the IS, and includes the ICS protocol and authorized ports and services.

Applicability to ICS Layers: 2, 3, 4, and 5.

CM-4 SECURITY IMPACT ANALYSIS

Justification to Select: ICSs operate as unique systems, with the underlying IS providing the basic OS and the ICS managed through the HMI, or they may be a standalone system managed by the FPOC panel/controller and running only the ICS protocol. New ICS software or updates should be analyzed in a separate test environment before installation in the operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Applicability to ICS Layers: 4 and 5.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Justification to Select: Only qualified and authorized individuals will have access to the ICS for purposes of initiating changes, including upgrades and modifications, separate and distinct from the IS changes. Many ICSs do not support the automated update of patches, service packs, device drivers, and the applications may not have a signed certificate.

Applicability to ICS Layers: 2, 3, 4, and 5.

CM-6 CONFIGURATION SETTINGS

Justification to Select: To change the configuration settings that affect the security posture and/or functionality of the ICS, only qualified and authorized individuals will have access to the ICS hardware, software, or firmware components.

Applicability to ICS Layers: 2, 3, 4, and 5.

CM-7 LEAST FUNCTIONALITY

Justification to Select: ICS protocols use unique ports and services compared to an IS. The ICS will be configured to provide only essential capabilities, and specifically prohibits or restricts the use of functions, ports, protocols, and/or services that affect the security posture and/or functionality of the ICS. Only qualified and authorized individuals will have access to the ICS hardware, software, or firmware components.

Applicability to ICS Layers: 2, 3, 4, and 5.

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Justification to Select: An ICS can have hundreds to millions of components and devices that are managed and controlled through the HMI or field control panel. The ICS inventory should include manufacturer, device type, model, serial number, physical location, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses.

Applicability to ICS Layers: 2, 3, and 4.

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Justification to Select: All federal organizations are required to have a contingency plan. The mission critical ICS, key operations, maintenance personnel, and priority of service should be clearly articulated in the plan. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

CP-2 CONTINGENCY PLAN

Justification to Select: All federal organizations are required to have a contingency plan. The mission critical ICS, key operations and maintenance personnel, and priority of service should be clearly articulated in the plan.

Applicability to ICS Layers: All.

CP-3 CONTINGENCY TRAINING

Justification to Select: All federal organizations are required to have a contingency plan and must train on the implementation of the plan. The mission critical ICS, key operations and maintenance personnel, and priority of service should be clearly articulated in the plan. Due to large number of devices, geographic/facility footprint, and remote locations, all operators and technicians need ICS specific contingency training documented in the training record.

Applicability to ICS Layers: All.

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Justification to Select: All federal organizations are required to have a contingency plan and must test and exercise the implementation of the plan. The mission critical ICS, key operations, maintenance personnel, and priority of service should be clearly articulated in the plan. Due to large number of devices, geographic/facility footprint, and remote locations, all operators and technicians need ICS specific contingency testing and exercises to maintain proficiency on the recovery and restoration of ICS functionality.

Applicability to ICS Layers: All.

CP-8 TELECOMMUNICATIONS SERVICES

Justification to Select: ICSs require a primary and alternate telecommunication service for communication between the operator's HMI, field control panels/controllers, and the field level devices. ICS telecommunication services include both the internal and external facility connections, and may be provided by a commercial carrier or a government owned dedicated service.

Applicability to ICS Layers: All.

CP-9 INFORMATION SYSTEM BACKUP

Justification to Select: ICS backups are essential to restore the ICS in case of failure. The ICS backup is separate and distinct from the IS backup.

Applicability to ICS Layers: 2, 3, and 4.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Justification to Select: ICS system recovery and reconstitution may be accomplished in conjunction with the IS system recovery and reconstitution, or as a standalone activity. A major network or system wide failure may take both the IS and ICS offline. An ICS may fail independently of the underlying network or IS OS.

Applicability to ICS Layers: All.

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Justification to Select: ICSs must have an identification and authentication policy that is updated annually and is distinct and separate from the IS systems. The policy must address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Justification to Select: Only authorized users that are properly authenticated on the ICS will be able to monitor and change the system configuration, define the operational parameters, and manage ICS functions. Operations and maintenance personnel must have proper identification and authorization for field controller, device and sensor repair or replacement.

Applicability to ICS Layers: 2, 3, and 4.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Justification to Select: Only authorized users that are properly authenticated on the ICS will be able to monitor and change the system configuration, define the operational parameters, and manage ICS functions. Operations and maintenance personnel must have proper identification and authorization for field controller, device and sensor repair or replacement. Many of the ICS devices and sensors are analog, do not support authentication, and require physical security compensating controls.

Applicability to ICS Layers: All.

IA-4 IDENTIFIER MANAGEMENT

Justification to Select: ICSs requires identifier management of the ICS Machine Address Code (MAC) and IP addresses, similar to an IS. The ICS MAC and IP addresses should be cross-correlated with the scanning and intrusion detection system to ensure that essential services are not inadvertently turned off.

Applicability to ICS Layers: Users connecting at Layers 2, 3, and 4.

IA-5 AUTHENTICATOR MANAGEMENT

Justification to Select: ICS authentication management is distinct and separate from the IS. An authenticator management system may be an ICS (e.g. biometrics, Physical Access Control CAC/PIV card reader, etc.).

Applicability to ICS Layers: Users connecting at Layers 2, 3, and 4.

IA-6 AUTHENTICATOR FEEDBACK

Justification to Select: ICS authenticator feedback is distinct and separate from the IS. The ICS must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Applicability to ICS Layers: All.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Justification to Select: ICS cryptographic module authentication is distinct and separate from the IS. Many legacy ICSs cannot support encryption at the device level and/or the protocols may have limited capability to support encryption. Encryption should be used at the layer that the IP router/switch/firewall can support.

Applicability to ICS Layers: 2, 3, and 4.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Justification to Select: ICSs require the same level of identification and authorization as an IS. Only authorized users that are properly authenticated on the ICS will be able to monitor and change the system configuration, define the operational parameters, and manage ICS functions. Operations and maintenance personnel must have proper identification and authorization for field controller, device and sensor repair or replacement. In general, non-organizational users are not allowed access to the ICS.

Applicability to ICS Layers: 2, 3, and 4.

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of incident response policy and procedures as an IS. The mission critical ICS, key operations, maintenance personnel, and priority of service should be clearly articulated in the contingency plan and incident response. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

IR-2 INCIDENT RESPONSE TRAINING

Justification to Select: All federal organizations are required to have a contingency plan and incident response training. The mission critical ICS, key operations, maintenance personnel, and priority of service should be clearly articulated in the plan. Due to large number of devices, geographic/facility footprint, and remote locations, all operators and technicians need ICS specific incident response training documented in the training record.

Applicability to ICS Layers: All.

IR-4 INCIDENT HANDLING

Justification to Select: Incident handling for the ICS is distinct and separate from the IS. ICS incidents may be caused by equipment failure, operator error, or malicious malware/cyberattack. Forensic analysis of ICS incidents is an emerging field.

Applicability to ICS Layers: All.

IR-5 INCIDENT MONITORING

Justification to Select: ICS incident monitoring is performed in conjunction with the IS incident monitoring. The ICS HMI or field control typically performs the operational management of the alarms and alerts associated with out of parameter performance, but ICS malware may spoof the integrity of the system. The IS-based scanning and intrusion detection system should account for ICS incidents.

Applicability to ICS Layers: All.

IR-6 INCIDENT REPORTING

Justification to Select: Federal policy (unless specifically exempted from such requirements) requires all ICS incidents to be reported to the ICS-Computer Emergency Readiness Team (CERT). ICS incidents are increasing at an exponential rate and mission critical ICS are high probability targets.

Applicability to ICS Layers: All.

IR-7 INCIDENT RESPONSE ASSISTANCE

Justification to Select: ICS incident response assistance within an organization is typically limited to a small number of personnel with subject matter expertise and knowledge of both the ICS and IS. External assistance is available from the ICS-CERT, but needs to be identified as a resource in the incident response plan.

Applicability to ICS Layers: All.

IR-8 INCIDENT RESPONSE PLAN

Justification to Select: All federal organizations are required to have an incident response plan. The mission critical ICS, key operations, maintenance personnel, and priority of service should be clearly articulated in the contingency plan and incident response plan. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of system maintenance policy and procedures as an IS. The mission critical ICS, key operations, maintenance personnel, and priority of service should be clearly articulated in the system maintenance policy and procedures. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

MA-2 CONTROLLED MAINTENANCE

Justification to Select: All ICSs require ongoing maintenance. Only authorized personnel will have access to and perform Operations & Maintenance (O&M) on the ICS components. Maintenance will be recorded in the ICS or organizational Computerized Maintenance Management System (CMMS).

Applicability to ICS Layers: All.

MA-4 NON-LOCAL MAINTENANCE

Justification to Select: All ICSs require ongoing maintenance. Only authorized personnel will have access to and perform non-local O&M on the ICS components. Maintenance will be recorded in the ICS or organizational CMMS.

Applicability to ICS Layers: All.

MA-5 MAINTENANCE PERSONNEL

Justification to Select: All ICSs require ongoing maintenance. Only authorized personnel should have access to and perform O&M on the ICS components. Maintenance should be recorded in the ICS or organizational CMMS.

Applicability to ICS Layers: All.

MA-6 TIMELY MAINTENANCE

Justification to Select: All ICSs require ongoing maintenance. Only authorized personnel should have access to and perform non-local O&M on the ICS components. Maintenance should be recorded in the ICS or organizational CMMS.

Applicability to ICS Layers: All.

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of media protection policy and procedures as an IS. ICS system design and operations, and the operational data can are generally not available to non-ICS authorized personnel. Specific facility consumption or performance data can provide adversaries with operations tempo or mission capability. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

MP-2 MEDIA ACCESS

Justification to Select: ICSs have multiple media access points and require the same level of media access protection as an IS. Many ICSs have embedded default passwords and require additional network segregation or physical access protection.

Applicability to ICS Layers: All.

MP-5 MEDIA TRANSPORT

Justification to Select: ICSs require the same level of media transport protection as an IS. ICS software and firmware updates may be performed by technicians using CDs, thumb drives, laptops, and other field diagnostic tools. ICS backups may be on removable media or via online backup.

Applicability to ICS Layers: All.

MP-6 MEDIA SANITIZATION

Justification to Select: ICSs require the same level of media sanitization protection as an IS. ICS software and firmware updates may be performed by technicians using CDs, thumb drives, laptops, and other field diagnostic tools. ICS backups may be on removable media or via online backup. All copies of ICS media will be sanitized prior to disposal, release out of organizational control, or release for reuse.

Applicability to ICS Layers: All.

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of physical and environmental protection policy and procedures as an IS. Physical and environmental protection ensures that the ICS components are accessible only to authorized personnel and are in a space or location that meets temperature, humidity, and other design and operations parameters. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Justification to Select: Physical access to an ICS should be carefully controlled and monitored. Only authorized personnel should have access to the ICS components.

Applicability to ICS Layers: All.

PE-3 PHYSICAL ACCESS CONTROL

Justification to Select: The ICS has multiple layers of defense and physical access control and only authorized users should have access to the ICS components. During an emergency-related event, access to ICS facilities and assets are limited to authorized first responders and maintenance personnel only. Primary nodes, distribution closets, and mechanical/electrical rooms should be locked and require key or electronic access control and incorporate intrusion detection sensors.

Applicability to ICS Layers: All.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Justification to Select: The ICS has multiple layers of defense and physical access control and only authorized users have access to the ICS distribution and transmission lines. Primary nodes, distribution closets, and mechanical/electrical rooms should be locked and require key or electronic access control and incorporate intrusion detection sensors.

Applicability to ICS Layers: 2, 3, 4, and 5.

PE-6 MONITORING PHYSICAL ACCESS

Justification to Select: The ICS has multiple layers of defense and physical access control is monitored. Primary nodes, distribution closets, and mechanical/electrical rooms should be locked and require key or electronic access control and incorporate intrusion detection sensors.

Applicability to ICS Layers: All.

PE-7 VISITOR CONTROL

Justification to Select: The ICS has multiple layers of defense and visitors are escorted or kept under electronic surveillance. Primary nodes, distribution closets, and mechanical/electrical rooms should be locked and require key or electronic access control and incorporate intrusion detection sensors.

Applicability to ICS Layers: All.

PE-8 ACCESS RECORDS

Justification to Select: ICSs require the same level of visitor and authorized personnel access record keeping as an IS. Due to large number of devices, geographic/facility footprint, and remote locations, all operators and technicians access should be cross validated between the ICS and physical security system.

Applicability to ICS Layers: All.

PE-11 EMERGENCY POWER

Justification to Select: Emergency power production, generators, transmission and distribution systems are a type of ICS, or components that are required to meet extremely

high performance specifications. The systems are governed by international, national, state and local building codes, must be tested on a continual basis, and must be repaired and placed back into operation within a short period of time. Traditionally, emergency power has been provided by generators for short to mid-term power (typically for fire and life safety systems, some IT load, and evacuation transport) and Uninterruptable Power Supply (UPS) battery packs in distribution closets and within work areas to allow some level of business continuity and for the orderly shutdown of non-essential IT and facility systems. Traditional emergency power systems typically are offline until a loss of power occurs and are typically on a separate network and control systems specific to the facility they support. New methods of energy generation and storage (e.g., solar voltaic, geothermal, flywheel, microgrid, distributed energy) that have a real-time demand and storage connection to local utilities or are cross connected to multiple facilities should be carefully analyzed to ensure that the power can meet the load and signal quality without disruption of mission essential functions.

Applicability to ICS Layers: All.

PE-12 EMERGENCY LIGHTING

Justification to Select: Emergency lighting systems are a type of ICS that are required to meet extremely high performance specifications. The systems are governed by international, national, state and local building codes, must be tested on a continual basis, and must be repaired and placed back into operations within a short period of time. Any occupied facility must have emergency lighting. Emergency lighting is typically on a UPS at the device level, on a dedicated emergency power circuit and designed to automatically turn on when loss of primary power occurs, with little outside network control connectivity. New generation emergency lighting is becoming more networked and integrated with physical access control, fire control, and other facility systems. Careful consideration should be given to ensure the emergency lighting systems fail over to the proper “on” mode.

Applicability to ICS Layers: All.

PE-13 FIRE PROTECTION

Justification to Select: Fire protection and life safety systems are a type of ICS that are required to meet extremely high performance specifications. The systems are governed by international, national, state and local building codes, must be tested on a continual basis, and must be repaired and placed back into operation within a short period of time. Any occupied facility must have fire protection. With the recent code changes to allow mass notification communication using VoIP, and the changes in technology converging the traditional stand-alone copper and twisted pair alarms and speakers, careful consideration should be given to ensure that the distribution closets and fire control panel/center switches, routers, hubs, and fire protection and life safety systems’ points of connection are on backup power and at the proper temperature and humidity. Discharge of fire protection water sprinklers can cause significant damage to other IS components. Smoke purge, exhaust fans and egress systems components are often interconnected to other ICSs such as the Physical Access Control and Building Automation systems.

Applicability to ICS Layers: All.

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Justification to Select: Temperature and humidity controls are typically components of other ICSs such as the HVAC, process, or lighting systems, or can be a standalone and unique ICS system. ICSs can operate in extreme environments and both interior and exterior locations. For a specific ICS, the temperature and humidity design and operational parameters dictate the performance specifications. As ICSs and ISs become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers and switches that support fire protection and life safety systems must be maintained at the proper temperature and humidity.

Applicability to ICS Layers: 2, 3, 4, and 5.

PE-15 WATER DAMAGE PROTECTION

Justification to Select: Water damage protection and use of shutoff and isolation valves is both a procedural action and a specific type of ICS. ICSs that are used in the manufacturing, hydropower, transportation/navigation, water and wastewater industries rely on the movement of water, and are specifically designed to manage the quantity/flow and pressure of water. As ICSs and ISs become interconnected and the network provides connectivity across the hybrid domain, caution should be taken that the power circuits, distribution closets, routers and switches that support fire protection and life safety systems are not disabled by water (e.g. a fire that activates the sprinkler system does not spray onto the fire control servers, router, switches and short out the alarms, egress systems, emergency lighting, and suppression systems).

Applicability to ICS Layers: 2, 3, 4, and 5.

PE-16 DELIVERY AND REMOVAL

Justification to Select: All ICSs require ongoing maintenance. Only authorized personnel should have access to and perform O&M on the ICS components. ICS hardware, sensors and devices are typically maintained by contractor support and not always under the direct control of the ICS operators. Components removed should be documented in the ICS and/or the CMMS.

Applicability to ICS Layers: 2, 3, 4, and 5.

PE-17 ALTERNATE WORK SITE

Justification to Select: ICSs require the same level of system backup, recovery, and ability to operate from an alternate site as an IS. Many ICSs can be operated in standalone mode at the FPOC as an interim measure. An ICS with an operations center/console and HMI should have a designated alternate recovery site in the contingency plan.

Applicability to ICS Layers: All.

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of security planning policy and procedures as IS. Electronic Security Systems are a specific type of ICS and provide the fundamental surveillance and monitoring capability dictated by the organizations security plan. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

PL-2 SYSTEM SECURITY PLAN

Justification to Select: ICSs require the same level of a system security plan as an IS. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network. Each unique ICS should be identified, but multiple ICSs may be incorporated into a single system security plan (e.g. a building BAS, EMS, PAC, vertical transport, fire and life safety, EMIS, etc. are unique ICSs that are required for the occupancy and use of the building and would be treated as an interconnected security system plan).

Applicability to ICS Layers: All.

PL-4 RULES OF BEHAVIOR

Justification to Select: ICSs require the same level of rules of behavior as an IS. An ICS is configured, operated, and maintained differently than an IS and the rules that describe their responsibilities and expected behavior with regard to ICS operations and ICS generated data must be clearly articulated and understood by the operators and the IT. In general, an ICS must always be “on” and the rules emphasize availability as a primary objective.

Applicability to ICS Layers: All.

PL-5 PRIVACY IMPACT ASSESSMENT

Justification to Select: ICSs require the same level of a privacy impact assessment as an IS. An ICS can have the authorized users names, and other personnel data such as credentials, phone and e-mail, and use a CAC or PIV card for authentication onto the underlying IS.

Applicability to ICS Layers: All.

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of personnel security policy and procedures as an IS. Only authorized users that are properly authenticated on the ICS will be able to monitor and change the system configuration, define the operational parameters, and manage ICS functions. Operations and maintenance personnel must have proper identification and authorization for field controller, device and sensor repair or replacement. In general, non-organizational users are not allowed access to the ICS. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

PS-2 POSITION CATEGORIZATION

Justification to Select: ICSs require the same level of position categorization as an IS. Only authorized users that are properly authenticated on the ICS will be able to monitor and change the system configuration, define the operational parameters, and manage ICS functions. Operations and maintenance personnel must have proper identification and authorization for field controller, device and sensor repair or replacement. In general, non-organizational users are not allowed access to the ICS. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network.

Applicability to ICS Layers: All.

PS-3 PERSONNEL SCREENING

Justification to Select: ICSs require the same level of personnel screening as an IS. Only authorized users that are properly authenticated on the ICS will be able to monitor and change the system configuration, define the operational parameters, and manage ICS functions. Operations and maintenance personnel must have proper identification and authorization for field controller, device and sensor repair or replacement. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network.

Applicability to ICS Layers: All.

PS-4 PERSONNEL TERMINATION

Justification to Select: ICSs require the same procedures for personnel termination as an IS. Upon termination of individual employment, ICS access will be terminated, and all ICS-related property and data returned. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network.

Applicability to ICS Layers: All.

PS-5 PERSONNEL TRANSFER

Justification to Select: ICSs require the same procedures for personnel transfer as an IS. Logical and physical access authorizations to ICS/facilities will be updated when personnel are reassigned or transferred to other positions within the organization.

Applicability to ICS Layers: All.

PS-6 ACCESS AGREEMENTS

Justification to Select: ICSs require the same level of access agreements as an IS. ICS will typically have multiple SLA's, MOA's, License and Use agreements and may be incorporated into vendor contracts that define order of notifications, repair and recovery time, and priority of restoration of service.

Applicability to ICS Layers: All.

PS-7 THIRD-PARTY PERSONNEL SECURITY

Justification to Select: ICSs require the same level of third-party personnel security as an IS. Many ICSs operate under the watch of contract guard services and an ICS vendor may have multiple component suppliers and subcontractors. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network.

Applicability to ICS Layers: All.

PS-8 PERSONNEL SANCTIONS

Justification to Select: ICSs require the same level of personnel sanctions as an IS. Personnel failing to comply with established ICS and information security policies and procedures must be denied access to the ICS.

Applicability to ICS Layers: All.

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of risk assessment policy and procedures as an IS. All federal agencies are required to conduct a risk assessment of CIKR. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

RA-2 SECURITY CATEGORIZATION

Justification to Select: ICSs require the same level of security categorization as an IS. CNSSI 1253 defines the security categorization for critical infrastructure. The DHS National Infrastructure Protection Plan defines the sector specific critical infrastructure.

Applicability to ICS Layers: All.

RA-3 RISK ASSESSMENT

Justification to Select: ICSs require risk assessments to be performed, similar to an IS, but using the risk assessment standards developed by the DHS Sector Leads. All federal agencies are required to conduct a risk assessment of CIKR. In general, the DHS ICS-CERT Tool is used to conduct risk and vulnerability assessments of ICS.

Applicability to ICS Layers: All.

RA-5 VULNERABILITY SCANNING

Justification to Select: ICSs require the same level of vulnerability scanning as an IS. ICS can now be physically destroyed or incapacitated by malware/cyberattack. The ICS operators and IT must coordinate closely to ensure scanning does not interrupt key ICS process and commands.

Applicability to ICS Layers: 2, 3, 4, and 5.

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Justification to Select: ICSs require the same level of system and services acquisition policy and procedures as an IS. The Executive Order (EO) -- *Improving Critical Infrastructure Cybersecurity*, requires the development of a Cybersecurity Framework, that “shall provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.” The EO also requires DoD and GSA to, “make recommendations on the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration”. A net expected outcome of the new standard will be the requirement for federal government procurement of security certified ICS products and vendor services, similar to those already in effect for traditional IT products and services. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

SA-2 ALLOCATION OF RESOURCES

Justification to Select: ICSs require the same allocation of resources as an IS. The convergence of IT and OT onto multi-use IP enabled platforms is enabling significant changes to the traditional design and operation of ICS. Standalone twisted pair copper cable and multiple conduits are being replaced by IT department provided switches,

routers and firewalls. However, the ICS technology refresh cycle can be dramatically different than the IT refresh cycle, and assigning the inventory, budgeting, and repair/replacement must be closely coordinated within the organization and with the ICS vendor.

Applicability to ICS Layers: All.

SA-3 LIFE CYCLE SUPPORT

Justification to Select: ICSs require the same life cycle support as an IS. The convergence of IT and OT onto multi-use IP enabled platforms is enabling significant changes to the traditional design and operation of the ICS. Standalone twisted pair copper cable and multiple conduits are being replaced by IT department provided switches, routers and firewalls. However, the ICS technology refresh cycle can be dramatically different than the IT refresh cycle, and assigning the inventory, budgeting, and repair/replacement must be closely coordinated within the organization and with the ICS vendor.

Applicability to ICS Layers: All.

SA-4 ACQUISITIONS

Justification to Select: ICSs have the same acquisition requirements as an IS. Currently, there is a limited ability to require ICS vendors and contractors to provide information describing the design and implementation details of the security controls to be employed within the ICS, ICS components, or ICS services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls. For many ICS component, there is no feasible means to test the production environment in a test and development environment. A net expected outcome of the new EO standard will be the requirement for federal government procurement of security certified ICS products and vendor services, similar to those already in effect for traditional IT products and services.

Applicability to ICS Layers: All.

SA-5 INFORMATION SYSTEM DOCUMENTATION

Justification to Select: ICSs have the same information system documentation requirements as an IS. Currently, ICS system administrator level documentation describes the configuration, installation, and operation of the ICS; effective use and maintenance of security features/functions; and known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions. However, ICS vulnerability patch management has historically taken a significant amount of time to deploy due to the operational constraints and technology of legacy systems and has been done manually. The ICS-CERT maintains ICS alerts, vulnerabilities, and patches. Network separation, use of virtualization, and firewall deep packet inspection are evolving technologies that can be applied as IT solutions on top of the OT components.

Applicability to ICS Layers: 2, 3, 4 and 5.

SA-6 SOFTWARE USAGE RESTRICTIONS

Justification to Select: ICSs have the same software usage restrictions requirements as an IS. ICS hardware and software may be bought as a package and/or as separate actions. ICSs can run on several different protocols, depending on the type or function of the ICS.

Applicability to ICS Layers: All.

SA-7 USER INSTALLED SOFTWARE

Justification to Select: ICSs have the same user installed software usage restrictions requirements as an IS. For most ICSs, the vendors have explicit rules governing the installation of software by users, and limited to ICS version updates and patches. With IP enabled ICS, unintentional software connections can have dire effects on the ICS performance (e.g. a printer software driver autosearching for IP addresses can block ICS commands executing at the device level). All ICS software should be tested in a non-operational environment before users add new software or applications to the ICS.

Applicability to ICS Layers: All.

SA-8 SECURITY ENGINEERING PRINCIPLES

Justification to Select: ICSs have the same security engineering requirements as an IS. ICS vendors are beginning to adopt the best practices of secure coding, supply chain verification and validation, and establishing separate test and development environments. A net expected outcome of the new EO standard will be the requirement for federal government procurement of security certified ICS products and vendor services, similar to those already in effect for traditional IT products and services.

Applicability to ICS Layers: 2, 3, 4, and 5.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Justification to Select: ICSs have the same external information system services requirements as an IS. Most ICS have the capability for remote access for operations and maintenance through a direct or wireless connection. The ICS should have a DMZ and firewall segregating the ICS network from the business systems.

Applicability to ICS Layers: 4 and 5.

SA-11 DEVELOPER SECURITY TESTING

Justification to Select: ICSs have the same developer security testing requirements as an IS. Many legacy ICSs have not undergone security testing. The DHS Cyber Security Evaluation Tool (CSET) tool should be used to conduct a baseline vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations. A net expected outcome of the new EO standard will be the requirement for federal government procurement of security certified ICS products and vendor services, similar to those already in effect for traditional IT products and services.

Applicability to ICS Layers: All.

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Justification to Select: ICSs require the same system and communications protection and policy as an IS. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

SC-2 APPLICATION PARTITIONING

Justification to Select: ICSs require the same application partitioning as an IS. Generally, an ICS will use different computers, different central processing units, different instances of the operating system, and different network addresses than an IS. Some ICSs can operate as a standalone system at the FPOC.

Applicability to ICS Layers: 2, 3, and 4.

SC-3 SECURITY FUNCTION ISOLATION

Justification to Select: ICSs require the same security function isolation as an IS. The ICS Enclave should clearly delineate the boundary that controls access to, and protects the integrity of, the ICS hardware, software, and firmware.

Applicability to ICS Layers: All.

SC-5 DENIAL OF SERVICE PROTECTION

Justification to Select: ICSs require the same denial service protection as an IS. ICSs are particularly susceptible to Denial Of Service (DOS) attacks by virtue of the relatively simplicity of the devices and sensors, small packet sizes, and latency of the system. Generally, the firewall at the DMARC or POP will isolate external DOS from the internal ICS packets required for normal ICS operations and communication down to the devices, sensors and actuators.

Applicability to ICS Layers: 4 and 5.

SC-6 RESOURCE PRIORITY

Justification to Select: ICSs require limits the use of resources by priority, similar to an IS. ICS operational safety is a primary function. Lower-priority process should not delay or interfere with higher-priority processes.

Applicability to ICS Layers: All.

SC-7 BOUNDARY PROTECTION

Justification to Select: ICSs require the same boundary protection as an IS. The ICS Enclave should clearly delineate the boundary that controls access to, and protects the integrity of, the ICS hardware, software, and firmware. Generally, the firewall at the DMARC or POP will isolate external systems from the internal ICS packets required for normal operations and communication down to the devices, sensors and actuators. Some ICS can operate as a standalone system at the FPOC.

Applicability to ICS Layers: 2, 4, and 5.

SC-8 TRANSMISSION INTEGRITY

Justification to Select: ICSs require the same transmission integrity as an IS. Cryptographic mechanisms can be used to recognize changes to ICS information during transmission, but latency induced from the use of cryptography may adversely impact the operational performance of the ICS. ICS malware can cause physical damage and/or impact on operations by spoofing the integrity of the ICS HMI.

Applicability to ICS Layers: All.

SC-9 TRANSMISSION CONFIDENTIALITY

Justification to Select: ICSs require the same transmission confidentiality as an IS. Cryptographic mechanisms can be used to recognize changes to ICS information during transmission, but latency induced from the use of cryptography may adversely impact the operational performance of the ICS. ICS malware can cause physical damage and/or impact on operations by spoofing the integrity of the ICS HMI. ICS information passed between the layers may still retain confidentiality, but the data reflects an incorrect system state.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-10 NETWORK DISCONNECT

Justification to Select: ICSs require the same network disconnection and termination of a communications session as an IS. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Justification to Select: ICSs require the same cryptographic key establishment and management as an IS. Latency induced from the use of cryptography may adversely impact the operational performance of the ICS. The use of cryptographic key management in ICS is intended to support internal nonpublic use.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-13 USE OF CRYPTOGRAPHY

Justification to Select: ICSs require the same use of cryptography as an IS. ICS data transmitted between the devices, controllers and HMI should separate and on a different network from the IS. Many of the ICS devices and protocols support only limited cryptography and may operate as standalone systems at the FPOC and below. Data above Layer 3 should have cryptography modules protection for unclassified information.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-14 PUBLIC ACCESS PROTECTIONS

Justification to Select: ICSs require the same level of public access protection as an IS. In general, public access to the ICS is not permitted; however, many of the components of an ICS may be in remote or geographically dispersed locations. Many substations, pumping stations, RTU's, exterior lighting, etc. may have public exposure.

Applicability to ICS Layers: All.

SC-15 COLLABORATIVE COMPUTING DEVICES

Justification to Select: ICSs require the same level of collaborative computing device protection as an IS. In general, older legacy ICSs do not support the use collaborative computing devices. Newer ICSs are being designed to operate as a network of things and ICS interconnectivity is essential for Smart Buildings, Smart Grid, Smart Cars, etc.

Applicability to ICS Layers: All.

SC-18 MOBILE CODE

Justification to Select: ICSs require the same level of mobile code protection as an IS. In general, older legacy ICSs have limited capability to support the use of mobile code. Newer ICSs are being designed to operate as a network of things, and ICS interconnectivity and use of mobile code is essential for Smart Buildings, Smart Grid, Smart Cars, etc.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-19 VOICE OVER INTERNET PROTOCOL

Justification to Select: ICSs require the same level of VoIP protection as an IS. Many ICS's command and control, emergency management, LMR, and fire and life safety systems use VoIP as a primary protocol.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Justification to Select: ICSs require the same level of secure name and address resolution service as an IS. ICSs may be accessed by remote clients, and authentication and integrity verification assurances for the host/service name should be established to the lowest IP layer. Many ICS protocols below the FPOC will not support name/address resolution.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-21 SECURE NAME / ADDRESS RESOLUTION (RECURSIVE OR CACHING RESOLVER)

Justification to Select: ICSs require the same level of secure name and address resolution service as an IS. ICSs may be accessed by remote clients, and authentication and integrity verification assurances for the host/service name should be established to the lowest IP layer. Many ICS protocols below the FPOC will not support name/address resolution.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Justification to Select: ICSs require the same level of secure name and address resolution service as an IS. ICSs may be accessed by remote clients, and internal/external role separation for the host/service name should be established to the lowest IP layer. Many ICS protocols below the FPOC will not support name/address resolution.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-23 SESSION AUTHENTICITY

Justification to Select: ICSs require the same level of session authenticity service as an IS. ICSs may be accessed by remote clients and are susceptible to man-in-the-middle attacks by virtue of default passwords embedded in firmware.

Applicability to ICS Layers: 2, 3, 4, and 5.

SC-28 PROTECTION OF INFORMATION AT REST

Justification to Select: ICSs require the same level of protection of information at rest as an IS. The ICS information at rest includes the Historian and/or field panels and controllers. ICS malware can spoof the system state and provide false integrity.

Applicability to ICS Layers: All.

SC-33 TRANSMISSION PREPARATION INTEGRITY

Justification to Select: ICSs require the same level of transmission preparation integrity as an IS. The ICS data aggregation, packaging, and transformation in preparation for transmission includes the Historian and/or field panels and controllers. ICS malware can spoof the system state and provide false integrity.

Applicability to ICS Layers: All.

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Justification to Select: ICSs require the same system and information integrity policy and procedures as an IS. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network. This control is required for the effective implementation of the ICS selected security controls and control enhancements.

Applicability to ICS Layers: All.

SI-2 FLAW REMEDIATION

Justification to Select: ICSs require the same flaw remediation and configuration management processes as an IS. ICSs operate as unique systems, with the underlying IS providing the basic OS and the ICS managed through the HMI, or they may be standalone systems managed by the FPOC panel/controller and running only the ICS protocol. Software updates are generally done manually.

Applicability to ICS Layers: All.

SI-3 MALICIOUS CODE PROTECTION

Justification to Select: ICSs require the same level of malicious code protection as an IS. ICSs operate as unique systems, with the underlying IS providing the basic OS and the ICS managed through the HMI, or they may be standalone systems managed by the FPOC panel/controller and running only the ICS protocol. ICS malware can cause physical damage or spoof the integrity of the system.

Applicability to ICS Layers: 2, 3, 4, and 5.

SI-4 INFORMATION SYSTEM MONITORING

Justification to Select: ICSs require the same level of information system monitoring as an IS. ICSs operate as unique systems, with the underlying IS providing the basic OS and the ICS managed through the HMI, or they may be standalone systems managed by the FPOC panel/controller and running only the ICS protocol. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network.

Applicability to ICS Layers: Layer 5 or at connection side of external network, may apply to Layers 2, 3, and 4.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Justification to Select: ICSs require the same level of situational awareness and compliance with security alerts, advisories, and directives as an IS. ICSs operate as unique systems, with the underlying IS providing the basic OS and the ICS managed through the HMI, or they may be standalone systems managed by the FPOC panel/controller and running only the ICS protocol. The ICS alerts are provided by the ICS-CERT.

Applicability to ICS Layers: All.

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Justification to Select: ICSs require the same level of security functionality verification as an IS. ICSs operate as unique systems, with the underlying IS providing the basic OS and the ICS managed through the HMI, or they may be standalone systems managed by the FPOC panel/controller and running only the ICS protocol. The ICS will have a security function separate and distinct from the IS.

Applicability to ICS Layers: All.

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Justification to Select: ICSs require the same level of software and information integrity as an IS. ICSs operate as unique systems, with the underlying IS providing the basic OS and the ICS managed through the HMI, or they may be standalone systems managed by the FPOC panel/controller and running only the ICS protocol. ICS malware can cause physical damage and/or impact on operations by spoofing the integrity of the ICS HMI or field panel/controller.

Applicability to ICS Layers: All.

SI-8 SPAM PROTECTION

Justification to Select: ICSs require the same level of spam protection as an IS. ICSs operate as unique systems, with the underlying IS providing the basic OS and the ICS managed through the HMI, or they may be standalone systems managed by the FPOC panel/controller and running only the ICS protocol. Spam on the IS can impact the ICS communications and exceed system latency causing the system to go into safe mode or go offline.

Applicability to ICS Layers: 2, 3, 4, and 5.

SI-9 INFORMATION INPUT RESTRICTIONS

Justification to Select: ICSs require the same level of information input restrictions as an IS. Only authorized ICS operators and maintenance personnel will have access to the ICS components.

Applicability to ICS Layers: 2, 3, and 4.

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Justification to Select: ICSs require the same level of information output handling and retention as an IS. ICS operate as unique systems with the underlying IS providing the basic OS and the ICS managed through the HMI, or may be a standalone system managed by the Facility Point of Connection panel/controller and running only the ICS protocol. The full life cycle of ICS information could provide consumption, mission tempo, and mission capability to an adversary.

Applicability to ICS Layers: All.

SI-13 PREDICTABLE FAILURE PREVENTION

Justification to Select: ICSs require the same level of predictable failure prevention as an IS. ICSs require ongoing preventive maintenance, and many ICSs have predictive maintenance to ensure the risk of failure is minimized the greatest extent possible.

Applicability to ICS Layers: All.

PM-1 INFORMATION SECURITY PROGRAM PLAN

Justification to Select: All federal agencies are required to develop and maintain an information security program plan. The plan will include the organizational ICSs.

Applicability to ICS Layers: All.

PM-2 SENIOR INFORMATION SECURITY OFFICER

Justification to Select: All federal agencies are required to appoint a senior information security officer (SISO). The SISO must also appoint Authorizing Officials with the skills and capabilities to evaluate and advise on the vulnerabilities and risk mitigations of ICS systems.

Applicability to ICS Layers: All.

PM-3 INFORMATION SECURITY RESOURCES

Justification to Select: IT and ICS must be properly resourced and accounted for in the inventory. IT systems are typically inventoried and budgeted for with the Exhibit 300. ICSs are typically inventoried and budgeted for with capital project or operations and maintenance funds. ICSs can be personal property or real property installed equipment.

Applicability to ICS Layers: All.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Justification to Select: All federal agencies are required to develop and maintain a plan of action and milestones process for the security program. The plan will include the organizational ICSs.

Applicability to ICS Layers: All.

PM-5 INFORMATION SYSTEM INVENTORY

Justification to Select: All federal agencies are required to develop and maintain an inventory of the IT and ICSs. The facility/engineering community will maintain the inventory for the ICS enclave listed in the organization master inventory. Other inventory systems such as CMMS or Builder may be used for ICSs and subsystems detailed inventory. The facility/engineering community must coordinate capital projects and operation and maintenance work orders with the CIO, and identify OT assets that will need technology refresh.

Applicability to ICS Layers: All.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Justification to Select: ICSs require the same level of information security measures of performance as an IS. ICSs have different measures of performance, and require specialized skills to identify vulnerabilities and malware and conduct forensic analysis of active systems.

Applicability to ICS Layers: All.

PM-7 ENTERPRISE ARCHITECTURE

Justification to Select: All federal agencies are required to develop and maintain IS and ICS systems compliant with the Federal Enterprise Architecture. A standalone ICS may not meet enterprise level security objectives, but should be consistent with the information security architecture at the system-of-systems level defined for the organization.

Applicability to ICS Layers: All.

PM-9 RISK MANAGEMENT STRATEGY

Justification to Select: All federal agencies are required to develop and maintain a risk management strategy for IS and ICS systems. ICS risk management decisions and mitigations can vary dramatically from traditional IT risk management.

Applicability to ICS Layers: All.

PM-10 SECURITY AUTHORIZATION PROCESS

Justification to Select: All federal agencies are required to develop and maintain a security authorization process. The SISO must also appoint Authorizing Officials with the skills and capabilities to evaluate and advise on the vulnerabilities and risk mitigations of ICSs.

Applicability to ICS Layers: All.

PM-11 MISSION/BUSINESS PROCESS DEFINITION

Justification to Select: All ICSs provide a foundational level of physical interaction with the environment to provide some type of service to the organizations mission/business processes, whether basic utilities, HVAC, or advanced manufacturing processes. The level of adverse impact that could result if a compromise of ICS information occurs can range from minor annoyance to loss of life and catastrophic property damage.

Applicability to ICS Layers: All.

6. Tailoring Considerations

When tailoring a security control set that includes the ICS Overlay, care should be taken that regulatory/statutory security controls are not tailored out of the control set. In general, the ICS may be part of a regulated entity (electrical production/distribution, water, wastewater, etc.) that must meet national, state, or local permitting or discharge requirements; or part of a building that must comply with national, state or local building code (fire and life safety, building automation system, etc.).

This section provides general considerations when tailoring the set of security controls for ICSs, followed by more specific considerations relevant to each family of security controls. The set of security controls resulting from application of overlays may need some modification to address mission-specific technologies, designs, threats, and concept of operations. Such modifications are permitted with the authorizing official's approval on a case-by-case basis.

The nature of ICS creates situations in which security controls cannot be implemented as intended. In these cases, the organization should employ appropriate compensating controls in accordance with general tailoring guidance given in NIST SP 800-53, CNSSI No. 1253, and other applicable guidance. In general, implementation of security controls should not adversely impact the operational performance of the ICS.

Federal employees (to include the AO and IA functions) and contractors that work on High Performance Green Buildings subject to the Federal Buildings Personnel Training Act must also maintain their core competencies, see www.fmi.gov for specific information.

ICS operations and maintenance must be done in compliance with building, electrical, mechanical, and fire codes.

Organization-wide information security program management controls are deployed throughout the organization supporting the information security program. They are not associated with security control baselines and are independent of any system impact level.

A complete inventory of all field level devices, sensors and actuators should be in an automated management system (e.g. Computerized Maintenance Management system (CMMS), Computer-aided Facility Management System (CAFM), Building Information Model (BIM), Geospatial Information System (GIS), Construction-Operations Building information exchange data (COBie, Building Automation Management information exchange (BAMie), As-Built drawings, Sustainment Management Systems (SMS) Builder, Paver, Roofer, etc.). The ICS IP enabled devices should be cross-validated to the Host Based Scanning System or Intrusion Detection System to detect anomalous network traffic and secure ports typically reserved for ICS field protocols (Modbus, LonTalk, BACnet, DNP 3, etc.).

Audit and Accountability Family

In general, audit information and audit tools are not present on legacy ICS, but on a separate information system (e.g., the historian in the DMZ). In situations where the ICS cannot support or protect audit information and audit tools on the ICS, the organization employs compensating controls (e.g., providing audit information and audit tool protection on a separate information system) in accordance with the general tailoring guidance.

The preferred method for time stamping uses Network Timing Protocol (NTP) to synchronize servers and workstations. The ICS should have all of the internal clocks standardized to a specific time zone (GMT, ZULU, UTC, etc.) and all clocks must agree with each other, though they may not necessarily have the exact time.

Contingency Planning Family

ICS systems often contain a physical component at a fixed location. Such components may not be relocated logically. Some replacement components may not be readily available. Continuance of essential missions and business functions with little or no loss of operational continuity may not be possible. In situations where the organization cannot provide necessary essential services, support, or automated mechanisms during contingency operations, the organization provides nonautomated mechanisms or predetermined procedures as compensating controls in accordance with the general tailoring guidance.

Because ICS are the foundational elements (power, water, HVAC, lighting, etc.) for all missions, the Continuity of Operations Plan (COOP) must be closely coordinated with the Critical Infrastructure Protection Plan and critical ICS systems identified and prioritized for restoration of services.

Identification and Authentication Family

The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

Incident Response Family

The automated mechanisms used to support the tracking of security incident are typically not part of, or connected to, the ICS. Security incidents and monitoring should be coordinated with the DHS ICS-CERT and USCYBERCOM ICS functional leads.

Reportable ICS incidents include water, wastewater, and air discharge permits; hazardous materials storage and transportation; electrical and utility NERC and FERC standards; building, electrical, mechanical, and fire codes.

Maintenance Family

The automated mechanisms used to schedule, conduct, and document maintenance and repairs are not necessarily part of, or connected to, the ICS.

Media Protection Family

As-Built drawings, Building Information Models (BIM), and Construction-Operations Building information exchange (COBie, if used) and other critical infrastructure data should be marked and treated as For Official Use Only (FOUO) at a minimum. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

Planning Family

OPSEC procedures should be used to mitigate exposure of critical information.

Risk Assessment Family

Categorization must be closely coordinated with the organization Critical Infrastructure Protection Plan, the DHS ICS-CERT, the USCYBERCOM Functional Lead, and the organizations OPSEC Functional Lead.

System and Services Acquisition Family

The ICS enclave should be entered into the organizational IT Portfolio Repository system; budgetary breakouts for sensor and actuator level components, Real Property Installed Equipment, and operations and maintenance must be closely coordinated by the IT and Engineering communities and reflected in the IT, Capital Project, and O&M budgets.

Systems and Communications Protection Family

The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational

performance of the ICS. While the legacy devices commonly found within ICS often lack direct support of cryptographic functions, compensating controls (e.g., encapsulations) may be used to meet the intent of the control.

System and Information Integrity Family

In general, ICSs do not output information other than audit and performance logs; the output is the continuous availability of the essential service being provided (i.e., power, water, HVAC, etc.). Reporting of performance and consumption data should be closely coordinated with the OPSEC Functional lead to ensure critical information is not divulged.

Program Management Family

The facility/engineering community should resource for the ICS Enclave listed in the organization master inventory. Other inventory systems such as Computerized Maintenance Management Systems or Builder may be used for ICS systems and subsystems detailed inventory. The facility/engineering community must coordinate capital projects and operation and maintenance work orders with the CIO and identify OT assets that will need technology refresh.

The risk management strategy must be closely coordinated with the organizations Critical Infrastructure Protection Program, and the OPSEC Functional lead.

10. Definitions

Alternative Fuel Vehicle (AFV)	An AFV is a vehicle that runs on a fuel other than "traditional" petroleum fuels (petrol or diesel); and also refers to any technology of powering an engine that does not involve solely petroleum (e.g. electric car, hybrid electric vehicles, solar powered).
Advanced Metering Infrastructure (AMI)	Advanced metering systems are comprised of state-of-the-art electronic/digital hardware and software, which combine interval data measurement with continuously available remote communications. These systems enable measurement of detailed, time-based information and frequent collection and transmittal of such information to various parties. AMI typically refers to the full measurement and collection system, which includes meters at the customer site, communication networks between the customer and a service provider, such as an electric, gas, or water utility, and data reception and management systems.
BACnet	The term BACnet is used in two ways: its first meaning is the BACnet Protocol Standard - the communication requirements as defined by ASHRAE-135, including all annexes and addenda. The second is as a reference to the overall technology related to the ASHRAE-135 protocol.
Building Automation System (BAS)	A BAS is a distributed control system, which is a computerized, intelligent network of electronic devices designed to monitor and control the mechanical electronics, and lighting systems in a building. BAS core functionality keeps the building climate within a specified range, provides lighting based on an occupancy schedule, and monitors system performance and device failures and provides email and/or text notifications to building engineering or maintenance staff. The BAS functionality reduces building energy and maintenance costs when compared to a non-controlled building. A building controlled by a BAS is often referred to as an intelligent building or a smart home.

Building Control System (BCS)	A control system for building electrical and mechanical systems, typically HVAC (including central plants) and lighting. A building control system is one type of a Field Control System.
Building Control Network (BCN)	The network used by the Building Control System. Typically the BCN is a BACnet ASHRAE-135 or LonWorks CEA-709.1-C network installed by the building control system contractor.
Cyber-physical systems (CPS)	CPSs are engineered systems that are built from and depend upon the synergy of computational and physical components. Emerging CPS will be coordinated, distributed, and connected, and must be robust and responsive. The CPS of tomorrow will need to far exceed the systems of today in capability, adaptability, resiliency, safety, security, and usability. Examples of the many CPS application areas include the smart electric grid, smart transportation, smart buildings, smart medical technologies, next-generation air traffic management, and advanced manufacturing.
Data Historian	A centralized database supporting data analysis using statistical process control techniques.
Critical Infrastructure Protection (CIP)	A program to evaluate, monitor, and risk rank mission critical infrastructure assets.
Critical Infrastructure and Key Resources (CIKR)	Term used in the DHS National Infrastructure Protection Plan and used by the Sectors to categorize the built environment.
Demarcation Point (DEMARC)	<p>In telephony, the demarcation point is the point at which the public switched telephone network ends and connects with the customer's on-premises wiring. It is the dividing line which determines who is responsible for installation and maintenance of wiring and equipment -- customer/subscriber, or telephone company/provider. The demarcation point varies between countries and has changed over time.</p> <p>The term MPOE (minimum or main point of entry) is synonymous, with the added implication that it occurs as soon as possible upon entering the customer premises. A network interface device often serves as the demarcation point.</p>

Direct Digital Control (DDC)	Control consisting of microprocessor-based controls with the control logic performed by software.
Electronic Security System (ESS)	Electronic Security Systems are operations systems that provide monitoring and alarming through the combination of hardware, software, firmware, and devices to enhance the efficiency and effectiveness of a physical security program. ESS use exterior and interior sensors and other terminal devices to provide asset protection through physical and operational security of a geographic area, building, or area within a building. ESS includes access control systems, perimeter monitoring systems, intrusion detection systems, video management and analytic systems, physical security information management systems, and land mobile radios. The various systems may be integrated at the Security Operations Center or may be stand-alone.
Emergency Management Information Systems (EMIS)	EMISs are used for continuity and interoperability between emergency management stakeholders and they support the emergency management process by providing an infrastructure that integrates emergency plans at all levels of government and non-government involvement, and by utilizing the management of all related resources (including human and other resources) for all four phases of emergencies. The system must meet requirements established by the National Incident Management System and typically includes an incident management tracking capability, a geospatial common operating picture, and the radio and telecommunications network for first responders. EMIS are often integrated with local government First Alert and the police/fire CAD 911 systems.
ICS Enclave	Collection of information systems connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.
ICS Enclave Boundary	Point at which an enclave's internal network service layer connects to an external network's service

Energy Service Interface (ESI)	<p>A network-centric device and gateway. It provides security, and often, coordination functions that enable secure interactions between network devices and the electric power company. It may permit applications such as remote load control, monitoring and control of distributed generation, display of customer usage, reading of non-energy meters, and integration with building management systems. It also provides auditing/logging functions that record transactions to and from networking devices.</p>
Exterior Lighting and Messaging Systems	<p>Exterior lighting systems and messaging systems use a variety of control systems, with a mix of legacy analog and newer digital capabilities. Lights can be controlled with sensors and remote services. There are several types of exterior lights:</p> <ul style="list-style-type: none"> • street lights are used to light roadways and walkways at night • LED and photovoltaic luminaires to provide energy-efficient alternative to traditional street light fixtures • Floodlights are used to illuminate outdoor playing fields or work zones during nighttime hours • beacon lights are positioned at the intersection of two roads to aid in navigation • security lights can be used along roadways in urban areas, or behind homes or commercial facilities • entry lights can be used outside to illuminate and signal the entrance to a property. These lights are installed for safety, security, and for decoration. <p>Message boards are used to control vehicle and pedestrian traffic, as scrolling information at property and building entrances, and at transit nodes to display arrival and departure times. Message boards can be LED, plasma, or light bulb displays.</p>
Facility Point of Connection (FPOC)	<p>The FPOC is the point of connection between the ICS network backbone (an IP network) and the field control network (either an IP network or a non-IP network). The hardware at this location which provides the connection is referred to as the FPOC Hardware. FPOC hardware takes the form of a control protocol</p>

	router, a control protocol gateway, or an IP device such as a switch or firewall. In general, the term "FPOC Location" means the place where this connection occurs, and "FPOC Hardware" means the device that provides the connection. Sometimes the term "FPOC" is used to mean either and its actual meaning (i.e. location or hardware) is determined by the context in which it is used.
Field Control Network (FCN)	The network used by a field control system.
Field Control System (FCS)	A building control system or Utility Control System (UCS).
Field Device	Control equipment (controller, sensor, actuator etc.) that is connected to/part of a field control system.
Fire Alarm and Life Safety Systems	A fire alarm system consists of components and circuits arranged to monitor and annunciate the status of fire alarm or supervisory signal initiating devices and to initiate the appropriate response to those signals. Fire systems include the sprinklers, sensors, panels, exhaust fans, signage, and emergency backup power required for building protection and occupant emergency egress. Life safety systems enhance or facilitate evacuation smoke control, compartmentalization, and/or isolation.
Human-Machine Interface (HMI)	The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to a PC with a color graphics display running dedicated HMI software.
Industrial Control System (ICS)	A system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems includes supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.
ICS Network	An IP network connecting multiple field control systems to the Monitoring and Control Software using one or more of: LonWorks (CEA-709.1-C and CEA-852-B), BACnet ASHRAE-135 Annex J), Modbus or OPC DA.

Intelligent Transportation Systems (ITS)	ITS are systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport. Intelligent transport technologies include wireless communications, computational technologies, floating car data/floating cellular data, sensing technologies, inductive loop detection, video vehicle detection, and Bluetooth detection. Intelligent transport applications include emergency vehicle notification systems, automatic road enforcement, variable speed limits, collision avoidance systems, and dynamic traffic light sequence.
Land Mobile Radios (LMR)	Land mobile radios are IP-based P25 equipment used by security, first responders and emergency managers to communicate over a secure channel for day to day operations and public safety events. LMR's and the P25 network interconnect transmission sites, management systems, dispatch console systems, logging recorders and data networks.
Java Application Control Engine (JACE)	JACE is a mechanism to connect individual building control systems via a real time common objects model.
LonTalk®	A networking protocol developed by Echelon Corporation and recognized by ANSI/CEA as ANSI/CEA-709.1-C. LonTalk implements layers 1-6 of the OSI reference model.
LonWorks®	A networking platform (created by Echelon Corporation) that provides solutions to numerous problems of designing, building, installing, and maintaining control networks.
Meter Data Management System (MDMS)	A system which automatically and reliably collects regular interval energy use data, processes the data to create meaningful information, and distributes to energy stakeholders who can take action to reduce energy use.
Modbus	A basic protocol for control network communications generally used in SCADA systems. The Modbus protocol definition is maintained by The Modbus Organization.

Monitoring and Control (M&C) Software	The ICS 'front end' software which performs supervisory functions such as alarm handling, scheduling and data logging and provides a user interface for monitoring the system and configuring these functions.
Net Zero Energy	Net Zero Energy produces as much energy on site as it uses, over the course of a year.
Net Zero Water	Net Zero Water limits the consumption of freshwater resources and returns water back to the same watershed so not to deplete the groundwater and surface water resources of that region in quantity and quality over the course of a year.
Net Zero Waste	Net Zero Waste reduces, reuses, and recovers waste streams, converting them to resource values with zero landfill over the course of a year.
OPC Data Access	This group of standards provides specifications for communicating real-time data from data acquisition devices to display and interface devices like Human-Machine Interfaces (HMI). The specifications focus on the continuous communication of data.
Operations and Maintenance (O&M)	O&M appropriations are used to finance “expenses” not related to military personnel or RDT&E. Types of expenses funded by O&M include DoD civilian salaries, supplies and materials, maintenance of equipment, certain equipment items, real property maintenance, rental of equipment and facilities, food, clothing, and fuel.
Operational Technologies (OT)	OT is physical-equipment-oriented technology and systems that deal with the actual running of plants and equipment, devices to ensure physical system integrity and to meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software.
Physical Access Control System (PACs)	PACS are required by HSPD-12 and the basic components of a PACs are the head-end server, panels, door controllers, readers, lock or strike mechanisms and the user identity cards.

Platform Information Technology (PIT)	PIT are IT or OT resources, both hardware and software, and include: weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems to include supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks).
Point of Presence (POP)	On the Internet, a point-of-presence (POP) is an access point from one place to the rest of the Internet. A POP necessarily has a unique Internet Protocol address. A POP may actually reside in rented space owned by the telecommunications carrier to which the ISP is connected. A POP usually includes routers, digital/analog call aggregators, servers, and frequently frame relays or ATM switches.
Programmable Logic Controller (PLC)	A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing.
Safety Interlock System (SIS)	A system that is composed of sensors, logic solvers, and final control elements whose purpose is to take the process to a safe state when predetermined conditions are violated. Other terms commonly used include emergency shutdown system (ESS), safety shutdown system (SSD), and safety interlock system (SIS).

Sources and Methods Information (SAMI)	DCID 6/5, Policy for Protection of Certain Non-SCI Sources and Methods Information (SAMI), 12 February 2001
Supervisory Control and Data Acquisition (SCADA)	A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.
TP/FT-10 (LonWorks)	A Free Topology Twisted Pair network (at 78 kbps) defined by CEA-709.3. This is the most common media type for a CEA-709.1-C control network.
TP/XF-1250 (LonWorks)	A high speed (1.25 Mbps) twisted pair, doubly-terminated bus network defined by the LonMark Interoperability Guidelines. This media is typically used only as a backbone media to connect multiple TP/FT-10 networks.