The Differences Between ICS/OT and IT Security

This SANS industrial control system (ICS) poster offers guidance on defining the differences between cybersecurity defense methodologies, security controls, safety, impacts, skillsets, and the security missions for ICS/OT (operations technology) compared to traditional information technology (IT) security.

INDUSTRIAL CONTROL SYSTEMS UNDERPIN MODERN SOCIETY

Control systems and critical infrastructure underpin a range of daily activities that are part of today's modern world. When we flip on a light switch at home or the office, pump gas into our cars at a gas station, or pour water from a tap, we are relying on industrial control and critical infrastructure systems. The complex, interconnected, and interdependent mix of both legacy and modern computer systems that are responsible for supporting the operation and security of everything from oil and gas production to manufacturing and public utilities management requires additional considerations for modern cyber defense beyond traditional IT security.

LEGACY ICS

Industrial control systems were not always as connected, highly automated, and complex as they are today. In the past, such systems were designed, built, tested, and deployed for a particular purpose, enabled the control system to operate in isolation, and ran on proprietary protocols. They were designed and operated in an isolated network away from other networks, including IT business networks and the Internet.

ICS MODERNIZATION

Over the years, advancements of modern network technology and equipment control systems have facilitated a shift from an isolated control environment to a more connected environment. This has brought several business benefits such as cost savings, and of course more external connections ultimately broke the isolated or "air-gapped" model, making ICS less isolated and exposed to additional cyber risk.

MODERN ICS

The enabling of more external connections has allowed for taking advantage of the benefits of remote monitoring and control of industrial processes, including using external support personnel to reduce travel costs and remotely access environments. Today, most control systems use modern TCP/IP network stacks, modern network technologies, and a blend of traditional IT and industrial protocols. However, in many cases legacy systems still exist as part of critical subsystems within control systems. In addition, despite its benefits, automation can bring new types of risks.

SAFETY CULTURE AND TRAINING

Safety training, drills, meetings, and stop-work safety protocols are commonplace in control system environments. Impacts such as malfunctioning equipment or a cyber-attack on the control system network can have safety ramifications for facility workers and the environment, as well as the potential to disrupt or destroy physical engineering assets. As such, many ICS organizations have a strong safety culture. Even access to process control sites typically requires safety training and personal protective equipment as well as safety training and certification, depending on the job role or even just to visit.

IMPACT

PURPOSE

CONTROLS

SYSTEMS

DATA TYPE

INTERFACES

IT SECURITY AND ICS SECURITY DEFINED

Industrial engineering control system assets are often inaccurately compared to traditional IT assets. IT and ICS systems have different missions, objectives, and impacts during an incident. They also have different devices, including but not limited to embedded operating systems and engineering devices speaking nontraditional industrial protocols. Adversaries targeting ICS must use different attack tactics and techniques for access, execution, collection, and persistence to degrade safety, manipulate control, and damage physical engineering assets or property.

IT and ICS systems differ in terms of:

IT SECURITY – MOVING AND SECURING DATA

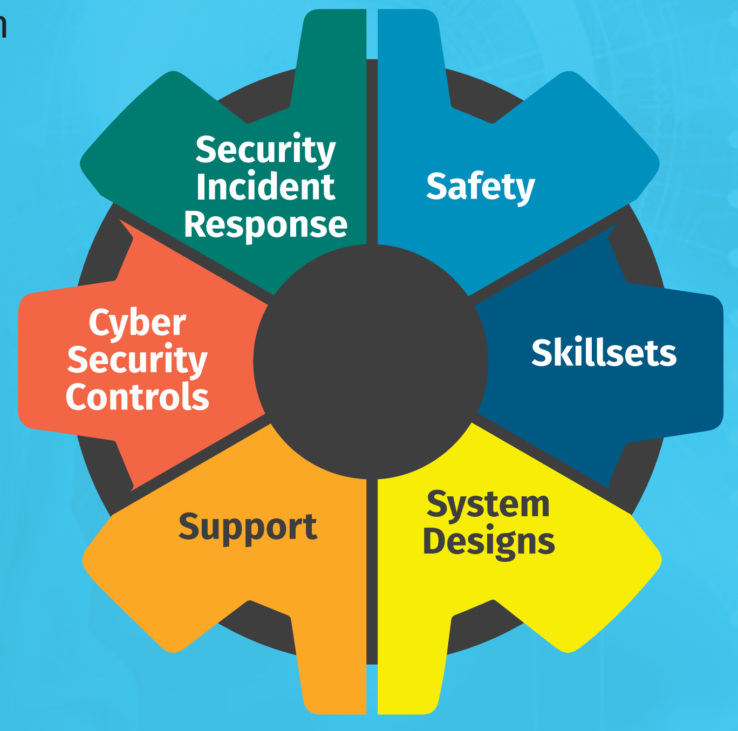
Traditional IT security focuses on digital data at rest or data in transit and the pillars of confidentiality, integrity and availability.

ICS/OT SECURITY – ENABLING AND SECURING PHYSICAL INPUT AND ACTIONS

OT/ICS systems manage, monitor, and control real-time engineering systems for physical input values and control output for physical actions in the real world. The main priority in OT/ICS is the safety and reliability of operations.

MAIN DIFFERENCES BETWEEN ICS/OT AND IT SECURITY

The main differences between IT and OT/ICS systems drive differing requirements across six areas:



UNIQUE CONSIDERATIONS FOR ICS SECURITY

Unique Systems—Nontraditional computer systems with industrial and proprietary protocols.

Reliance on External Vendor Support—Engineering systems with external engineering team support that may require special secure remote access and monitoring.

Legacy Systems—Devices that may not be suitable for patching or firmware updates, or that are only available for patching or firmware updates to internal operating systems at infrequent times.

Nontraditional Operating Systems—Purpose-built embedded and/or proprietary operating systems that are common in control environments where many traditional security defenses are not effective or applicable.

Safety of People—The main goal for control systems is not confidentiality, integrity and availability, but rather safety. Then integrity to trust operational commands, then availability.

Protection of Physical Assets—Control systems use physical components to change the physical world. Impacts such as a cyber-attack could result in physical damage, safety implications, environmental impacts, and the potential for loss of life.

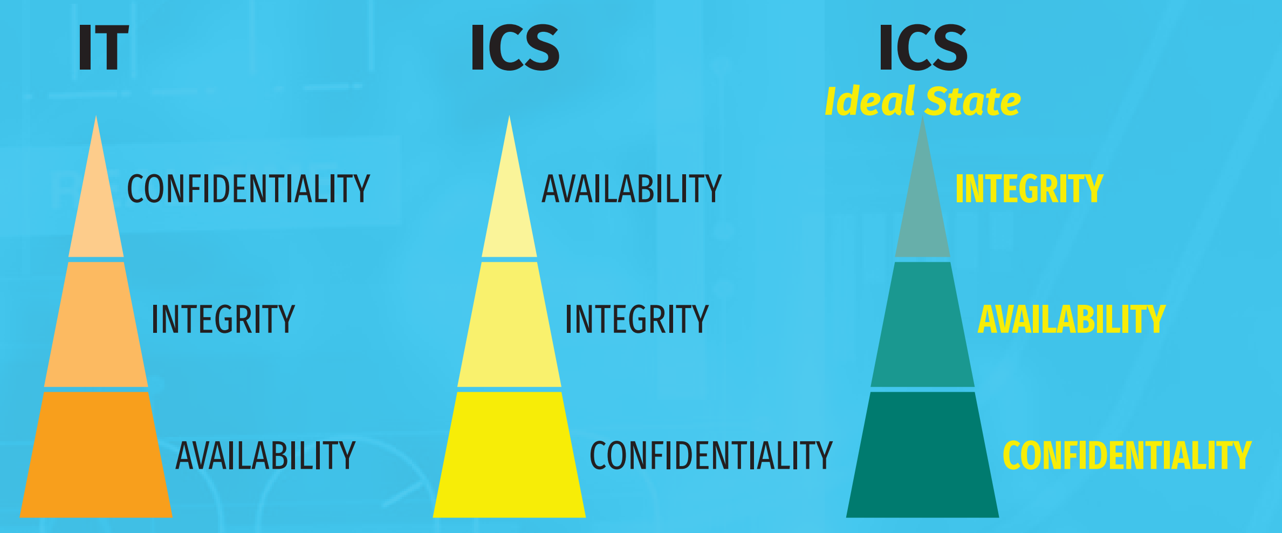
SECURITY TRIAD PRIORITIZATION

The priority in IT security tends to be data confidentiality, integrity, and availability. The objective in the ICS is a control system that has integrity, availability, and confidentiality that enables operating the process with confidence and supports safety as its primary goal. This involves:

- Safe operations
- Integrity of the engineering process and commands
- Availability of the operational processes and safety systems
- Confidentiality of sensitive ICS engineering information that may exist in the ICS network(s).

It is not that confidentiality is not important in ICS, it is just that it has far less importance in an industrial environment with so few users and with limited or no access to the Internet. As well, IT and ICS have different attack surfaces, and risk profiles.

External site-to-site encrypted channels are needed for geographically dispersed facilities. However, secure authentication of ICS commands inside control networks could be put in place after ICS-specific or adapted defenses are established, starting with network architecture, passive defenses, and a solid deployment of ICS network security monitoring conducted daily by trained ICS security defenders using ICS protocol aware tools. Enabling encryption inside an ICS network(s) requires a risk benefit analysis and heavy consideration for cyber defense capabilities and impacts to the real-time communication requirements and legacy devices.



CYBER ATTACKS IN INFORMATION TECHNOLOGY ENVIRONMENTS

Cyber incidents in traditional IT environments can lead to digital data corruption, sensitive information breaches, data destruction, and business application system downtime.

CYBER ATTACKS IN INDUSTRIAL ENVIRONMENTS

Cyber-attacks in ICS environments, or cyber-kinetic attacks, can lead to direct or indirect physical damage to engineering assets, introduce environmental impacts, and cause human injury or death.

IT INCIDENT IMPACT POTENTIAL	ICS INCIDENT IMPACT POTENTIAL
Business applications unavailable—local to business/organization	Critical infrastructure unavailable—possible wide region disruption or outages
Digital data corruption	Loss of control or manipulation of physical process
Digital data loss	Personnel safety, loss of life

SANS
INDUSTRIAL CONTROL SYSTEMS SECURITY

Comparison of Security Controls

There's a wealth of knowledge available to perform IT defense. However, a "copy and paste" of traditional security into an ICS could have problematic or even devastating impacts that results in unsafe conditions. The steps of IT incident response—Detection and Identification, Containment, Eradication, Recovery, and Lessons Learned—are still at play in an ICS. However, there are more steps, and each step needs to be adapted for the safety and reliability of operations that prioritize human life and the protection of physical assets. For example, false positives are not or very rarely acceptable in the ICS and can cause major unintended engineering process and safety impacts.

Security Control	Common IT Action	Common ICS/OT Action
Endpoint Protection	Signatures, heuristics-based—Quarantine files	Allowlisting—Alerting
Firewalls	Segment users and servers	Segment away from IT, Internet; segment ICS process zones
Network IDS/IPS	Intrusion Prevention System—Drop network traffic flagged as suspicious	Intrusion Detection System—alert only for suspicious traffic—must have ICS deep-packet inspection capabilities
Vulnerability Scanning	Regular internal, automated, and active scanning methods are common	Tested, passive methods used, run during maintenance window, use careful consideration—active scanning could disrupt legacy engineering assets
Patching	Monthly, streamlined process	Less frequent, legacy devices may not be patchable, less patch windows available
Security Awareness	Phishing, Internet usage, and data protections	IT security awareness with additional cybersecurity, physical security, engineering safety specific to OT/ICS
Event Detection	Windows event logs, traditional endpoint protection, URL inspection, email sandboxing, etc.	Windows event logs, engineering field devices change logs, ICS protocol baselining and anomaly detection, ICS network boundary access detection, remote access by vendors to critical components
Incident on Asset	Containment, patch, re-deploy	Fight through attack—maintain safety, conduct quick triage, contain where feasible, monitor operations, completely eradicate on next maintenance window

NETWORK INTRUSION DETECTION & PREVENTION

All network inspection devices deployed to make decisions on ICS traffic should be able to conduct deep packet analysis and interpret ICS protocols and commands. As with antivirus solutions on endpoints, false positives can occur in network inspection as well. Thus, an IDS Intrusion Detection System (IDS) for alerting on suspect network traffic on a control network is more suitable than an Intrusion Prevention System (IPS), as IPS solutions block or drop network traffic that could end up being legitimate control commands, thus wrongly disrupting the control system and risking safety.

VULNERABILITY SCANNING

Automated vulnerability scanning in IT is a common and usually unintrusive practice. Vulnerability scanning in an ICS network can have unpredictable and undesirable effects, especially with aged firmware versions or legacy devices simply not designed to handle abnormal traffic patterns or excessive network connections to them. Alternative less-invasive methods of vulnerability assessments can be performed by reviewing asset inventories, configuration files, and firmware versions against threat intelligence and vulnerability advisories. With careful planning and a phased approach, vulnerability assessment can be conducted effectively in ICS. For example, using a passive network traffic analysis is a safer method than injecting packets onto the ICS network to discovery vulnerabilities.

ENCRYPTION

Encrypting network traffic between remote sites over inherently insecure channels can protect both IT and ICS networks and is a general best practice. However, confidentiality inside an ICS is less of a requirement than it is inside business networks. Internal ICS network encryption can result in unintended challenges with little gain. Attention to endpoint processing power, network latency, and bandwidth consumption, especially in facilities with legacy equipment, will be needed. In addition, Network Security Monitoring defense capabilities may be severely limited if the control network is encrypted, effectively blinding defenders. The risk profile for IT is different than for ICS. The risk of users eavesdropping or sniffing sensitive personal data inside the ICS network is not the same as in a business network and demands a different protection approach.

ENDPOINT PROTECTION

Most modern endpoint protection solutions have signature-based, behavioral, or heuristics engines to assist with threat identification in IT environments. Signature-based endpoint protection tools may not be trivial to update in an isolated ICS network. Behavioral threat prevention tools can cause false positives and disrupt an industrial process and cause unsafe physical conditions. In contrast, allowlisting features for ICS endpoint protection can be effective when maintained throughout controlled changes or maintenance windows in the ICS. Allowlisting does not require signatures or constant updates, which makes security control maintenance easier in control environments, as such environments are more static, with far fewer users compared to IT environments.

FIREWALLS

The proper use of firewalls is critical in ICS for the same reasons as in IT. Firewalls can be used for containment in incident response, as chokepoints for data collection for Network Security Monitoring, and for segmenting network zones and properly controlling traffic via role-based access control lists. For example, they can be used to isolate different control networks from each other, the Internet, and corporate business networks. ICS firewalls should not allow any direct connections to or from the Internet. If remote access is needed for maintenance or support, this should be implemented with care and with multiple layers such as multi-factor authentication, extremely strict access control, additional monitoring/alerting, the use of jump hosts, and an ICS demilitarized zone.

PATCHING

Patching operating systems and software is an effective security practice that has been commonplace in business networks for decades. For ICS, there are special circumstances where patching may not be feasible or possible. This could be the case with legacy equipment or critical infrastructure systems during peak load of operations. This process continues to improve across multiple ICS sectors, so patching is becoming more of a positive and achievable part of preventative maintenance for facilities. However, patching must be evaluated much more than simply by employing Common Vulnerability System Scoring (CVSS). Remember, when evaluating advisories and vulnerability reports to prioritize patching, a Threat = Capability of the adversary + Intent of the adversary + Opportunity for the adversary to have an impact. When patching in ICS, always ask the question "Do the ICS operational needs and safety outweigh the risk of a potential identified vulnerability within the control system actually being accessed and successfully exploited?"

PROTOCOLS

Some traditional networking and IT protocols can be seen inside control system environments used for engineering processes, but they go well beyond common protocols and can include specific industrial protocols and several proprietary protocols as well.

Common IT Protocols

- SSH
- SMB
- SFTP
- HTTP
- HTTPS
- SMTP
- 802.11
- DHCP
- DNS

Common ICS/OT Protocols

- SSH
- Telnet
- FTP
- SMB
- HTTP
- HTTPS
- DHCP
- DNS
- OPC
- ICCP
- ModbusTCP
- DNP3
- IEC104
- IEC101
- HART
- PROFINET
- PROFIBUS
- EtherNet/IP
- VSAT
- BGAN
- BACnet
- and various industrial proprietary protocols

ICS AND IT SYSTEM LIFECYCLE DIFFERENCES

Information Technology	Industrial Control Systems
Operating Environment	
Indoor office settings, air-controlled data centers	Outdoor Extreme weather conditions, industrial facilities, complex remote sites
Technology & Support	
Commercial off-the-shelf software Specialized engineering software	Specialized engineering software
Commercial off-the-shelf hardware Specialized engineering hardware	Specialized engineering hardware
Traditional IT protocols	IT protocols + Industrial and proprietary protocols
Lifecycle	
Regular frequent patching	Less frequent patching, fewer maintenance windows
2–3 year upgrade cycles	5–10+ year upgrade cycles
Dynamic environments	Static environments
Design and Architecture	
Abundance of users, in/outbound internet connectivity, focus on user experience	Very few operators, little/no Internet connectivity, very restrictive, focus on process rather than user experience to prioritize safety
Network segmentation – users, servers	Network segmentation adhering to Purdue Levels 0–5, or ICS410 Network Architecture Reference Model
Common and well-known systems, more modern technology	Systems more unique and legacy components are common
Many users with individual and unpredictive network patterns	More static network, system-to-system more predictable network communications
Priority and Mission	
Data confidentiality, integrity, availability	Safety of people, protection from physical equipment damage, industrial command integrity, process control system availability of engineering processes
Cyber Attacks	
Adversary attack research and exploits kits well known and publicly available and scalable to general IT networks	Smaller adversary groups targeting ICS (currently, but increasing to target ICS)
	Adversaries generally need more time and skill to have significate impact
	ICS attacks need to be tailored more so, tools not as scalable or adaptable for other general ICS attacks

IT/OT CONVERGENCE

IT/OT convergence can be broken down into two threads of thought: technology, and resources/teams.

COVERGENCE OF TECHNOLOGY

Many operations technology environments have been leveraging traditional operating systems and networking infrastructure to automate and improve control system processes for decades. These traditional operating systems running OT and engineering software remain part of ICS supporting the control system mission, and thus should be properly managed and protected as ICS/OT assets.

COVERGENCE OF SECURITY RESOURCES

In recent years, leaders have been bringing IT security and ICS security teams with their unique security skillsets together or separating them out. Specifically, they are bringing in IT security team members to manage traditional security for the business networks, and ICS security team members to protect the control system networks at all levels of the control system for all OT/ICS assets, including nontraditional systems, protocols, and engineering systems in ICS environments.

ICS/OT SPECIFIC CYBERSECURITY DEFENSE REQUIREMENTS

Whether in a converged or specific ICS security team, it is imperative that OT/ICS defenders be trained with ICS-specific security knowledge, technologies, tools, and procedures. This means training them to understand the nuances between traditional IT and ICS security, the ICS mission, safety, the engineering process, and ICS protocols and active defense strategies that excel inside control environments, which are different from traditional IT security.

THE ICS SECURITY FUTURE

This poster has shown that there are different approaches to IT and ICS security—and that's okay! While some parts of traditional IT security can help guide the community, a direct "copy-paste" of such security is not recommended for ICS and will likely cause disruptions and or safety concerns in control system environments. The OT/ICS community can adapt IT security for OT/ICS where it makes sense, all the while adjusting and prioritizing safety, human life, the reliability of operations, and the protection of physical assets. Remember, **"ICS Defense Is Doable!"**

SANS ICS CURRICULUM

ICS310: ICS Cybersecurity Foundations™

ICS410: ICS/SCADA Security Essentials™
Global Industrial Cyber Security Professional (GICSP)

ICS418: ICS Security Essentials for Leaders™

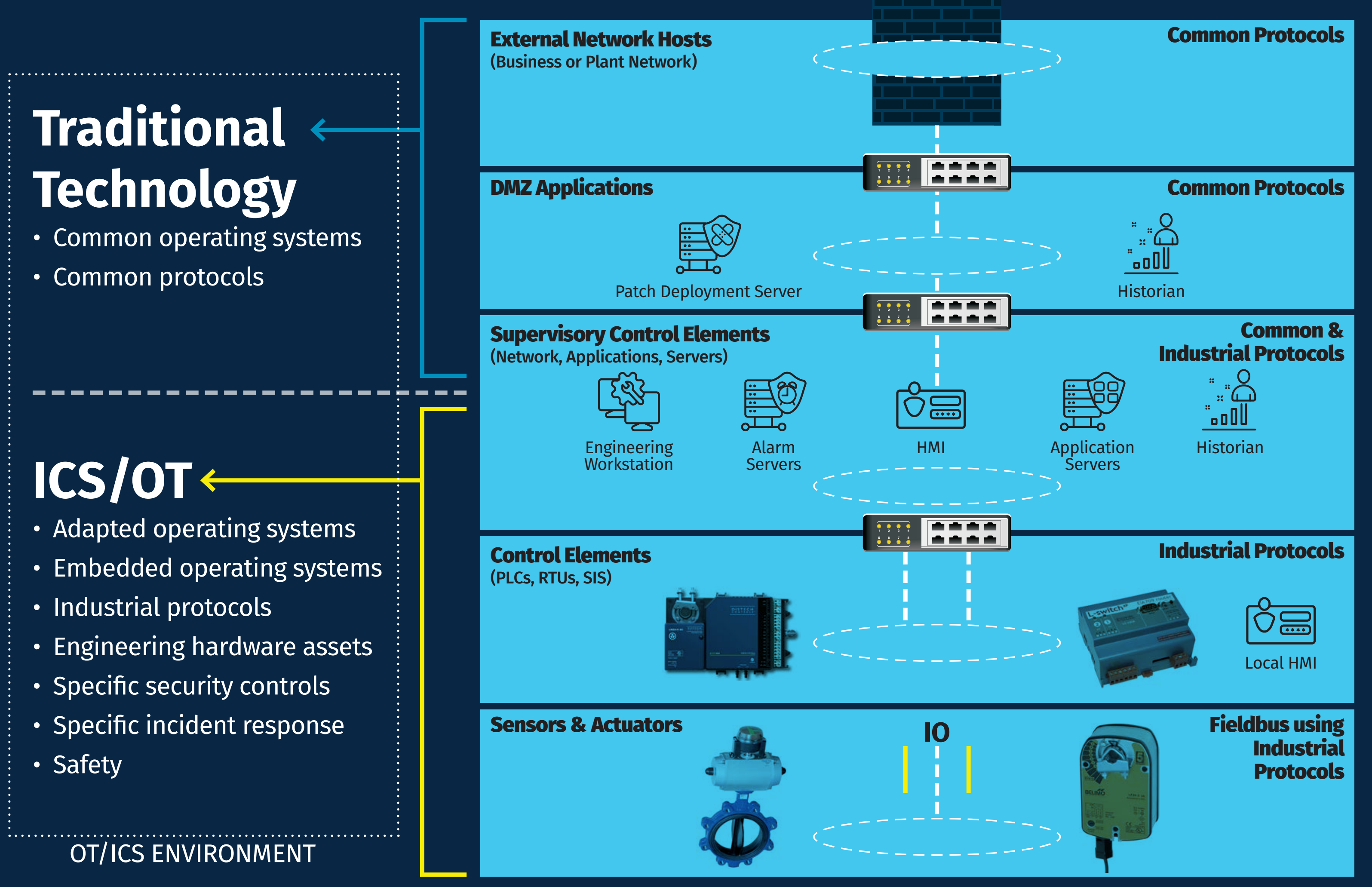
ICS456: Essentials for NERC Critical Infrastructure Protection™
GIAC Critical Infrastructure Protection (GCIP)

ICS515: ICS Visibility, Detection, and Response™
GIAC Response and Industrial Defense (GRID)

ICS612: ICS Cybersecurity In-Depth™

ICS613: ICS/OT Penetration Testing & Assessments™

SYSTEMS, PROTOCOLS AND ICS NETWORK MAP



Traditional Technology

- Common operating systems
- Common protocols

ICS/OT

- Adapted operating systems
- Embedded operating systems
- Industrial protocols
- Engineering hardware assets
- Specific security controls
- Specific incident response
- Safety

OT/ICS ENVIRONMENT

SANS ICS RESOURCES

- sans.org/ics
- ics-community.sans.org/signup
- @SANSICS
- Free and open-source tools for ICS are available at ControlThings.io

SANS INDUSTRIAL CONTROL SYSTEMS SECURITY

sans.org/ics

ICSPS_ICS-IT_0525
This poster was created by Dean C. Parsons.