SANS, working with industry experts, is making a difference in the Industrial Control System (ICS) cybersecurity front. SANS has joined forces with industry leaders to, change the game, by equipping both security professionals and control system engineers with the security awareness, work specific knowledge, and hands-on technical skills they need to secure automation and control system technology. The SANS ICS team is working to provide ICS-focused curriculum and certifications, as well as community resources including posters, white papers, and security practice application guidance. SANS has engaged the dedicated practitioner community that assembles during our global and regional ICS summits, and leverages leaders from enterprises, governments, and vendors from around the globe to tackle our common challenges and share working solutions.

SANS ICS CURRICULUM

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

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

ICS515: ICS Active Defense & Incident Response
GIAC Response and Industrial Defense (GRID)

ICS612: ICS Cyber Security In-Depth

SANS ICS RESOURCES

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

Poster was created by Justin Searle with support of the SANS ICS faculty.

ICS410 SCADA Reference Model

Enforcement Boundaries
Enforcement boundaries include cybersecurity technologies to limit and monitor communications. Items typically found in this zone include firewalls, NIDS/NIPS, routers (with ACLs), data diodes, netflow collectors, and full-packet collectors. Technologies implemented will differ at the various enforcement zones (major and minor) within each ICS environment depending on identified risks and constraints.

Demilitarized Zone (DMZ)
A DMZ can be leveraged in any enforcement boundary. It provides a staging and inspection area to pass data between two different levels, where neither side has full control. The preferred model is for one side to push data to the DMZ, and the other side can pull that data when needed.

PURDUE LEVEL 5:
Enterprise Networks
Corporate-level services used to support enterprise scalability supporting individual business units and users. These systems are usually located in corporate data centers, and can include servers providing enterprise AD, internal email, CRM systems, HR systems, document management systems, backup solutions, and enterprise SOC.

PURDUE LEVEL 4:
Business Networks
IT networks for business users at local sites. This level includes business workstations, local file and print servers, local phone systems, enterprise AD replicas, connectivity to enterprise WAN, and possibly local Internet access. No system that can influence OT processes should be in this level. Direct Internet access should not extend below this level.

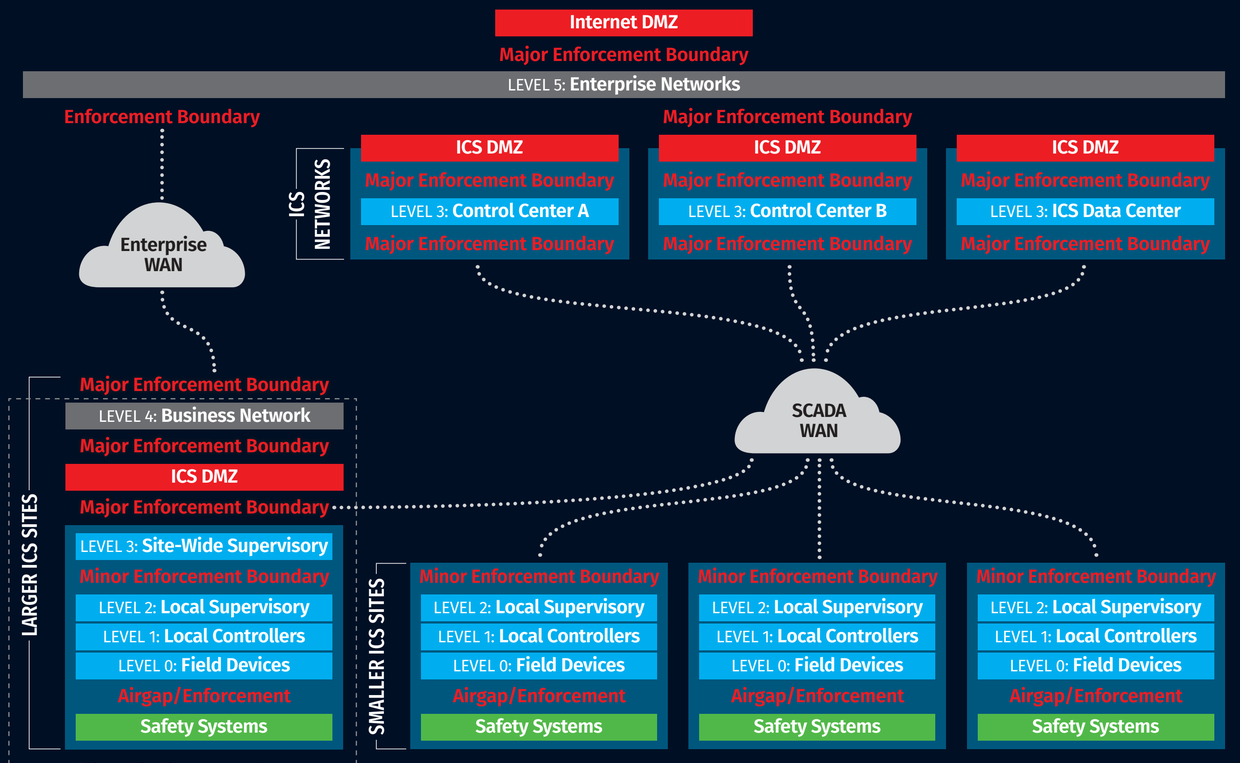
PURDUE LEVEL 3:
Site-Wide Supervisory
Monitoring, supervisory, and operational support for an entire site or region. This level can include master servers, HMIs, alarm servers, analytic systems, or historians if scoped for an entire site or region. Level 3 can (and should) be broken into multiple subnets, grouped by function/role to simplify ACLs. If Active Directory is needed, use a separate domain with no trust relationships. Use a subnet here for security servers like SIEM, patching, and endpoint security.

PURDUE LEVEL 2:
Local Supervisory
Monitoring and supervisory control for a single process, cell, line, or DCS solution. Isolate processes from one another, grouping by function, type, or risk. This level includes HMIs, alarm servers, process analytic systems, historians or control room if scoped for a single process and not the site/region. Systems in this level can leverage Active Directory in level 3 if needed.

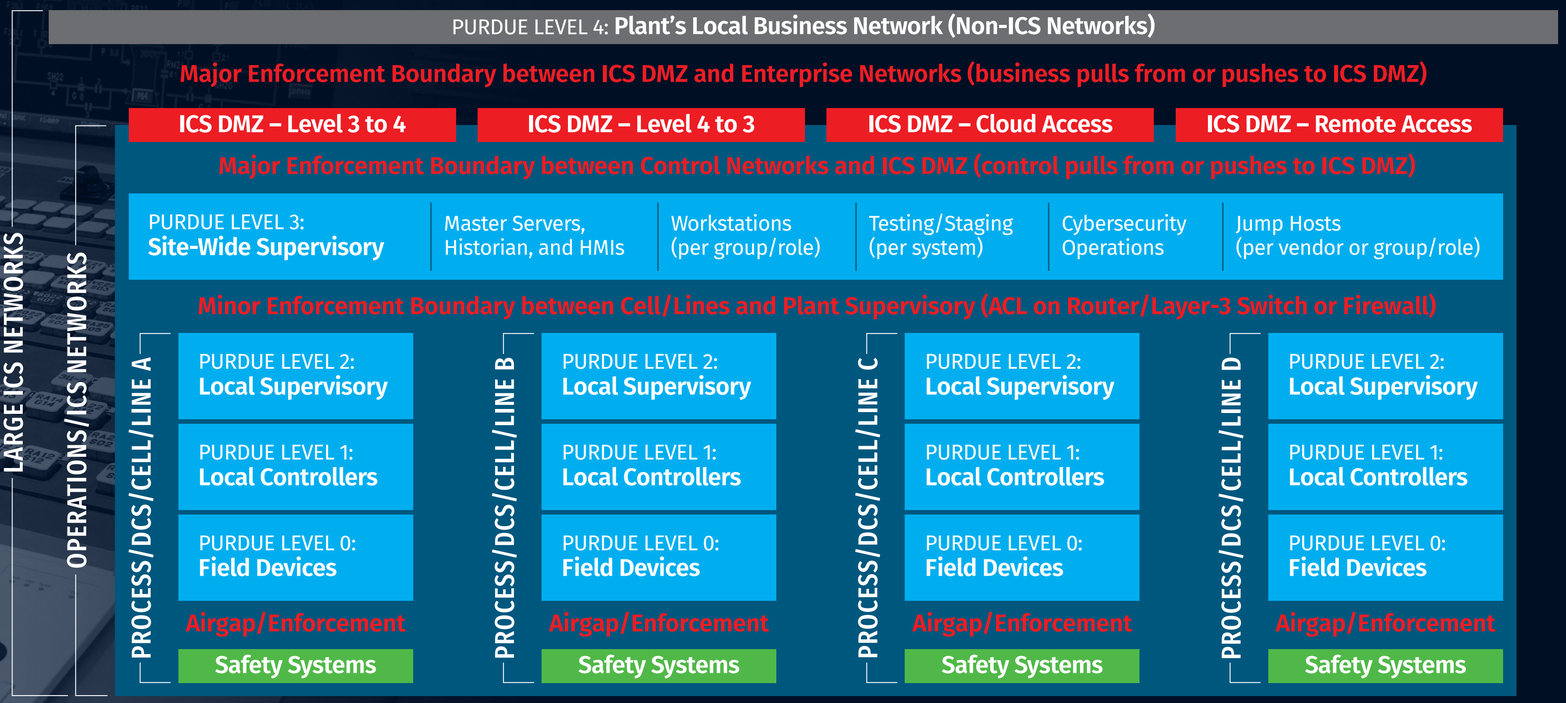
PURDUE LEVEL 1:
Local Controllers
Devices and systems to provide automated control of a process, cell, line, or DCS solution. Devices can include PLCs, control processors, programmable relays, RTUs, and process-specific microcontrollers. Modern ICS solutions often obscure the lines between level 0 and 1.

PURDUE LEVEL 0:
Field Devices
Sensors and actuators for the cell, line, process, or DCS solution. It could include basic sensors/actuators, smart sensors/actuators speaking fieldbus protocols, IEDs, IIoT devices, communications gateways, and other field instrumentation. It may not be necessary to distinguish between level 0 and 1.

Safety Systems
Systems that are engineered for a specific protective function, attempting to prevent worse-case scenarios. This level includes all items identified in Level 0 and 1 with a dedicated purpose for a safety control function such as acoustic monitoring, liquid chemistry monitoring, vibration monitoring, and emission monitoring. In most safety systems there exists a control function that serves to protect the operation and personnel.



ICS410 Large ICS Site Reference Model



SANS Industrial Control Systems

Security Resources

Control Systems Are a Target

ICS Cyber Threat Actors

- ICS sees a greater percentage of nation state activity
- Criminal groups can threaten process disruption or sell ICS intellectual property
- Malicious insiders are highly effective since many ICS environments use shared credentials and weak separation of duties
- Politically statement are stronger when hacktivists leverage critical infrastructure

Information Leakage

- Sensitive information is often placed on company websites and found by attackers through search-engine queries (google hacking)
- Org charts, business partners, vendors, ICS technologies, HR position postings, engineer bios, and many other company details are often used in the attacks to launch initial attacks involving social engineering
- Systems may be directly exposed to the Internet without proper controls, through accident or ignorance, making discovery and compromise trivial

Remote Access

- Most remote access methods, including VPNs, can be identified by Nmap, Shodan, and other tools
- Dial-up modems can be discovered with war-dialing, have few access controls, and are near impossible to prevent denial-of-service attacks
- Remote access methods are often implemented as a single step into the ICS environment, failing at providing a remote access model with layered defenses
- VPNs often allow applications and data on external machines to be used inside ICS networks, risking the propagation of malware

Connectivity Between Business and ICS

- Some ICS industries often fail to create enforcement boundaries between the business and ICS, often resulting in malware and IT staff interruptions in ICS processes
- Most attacks migrate from the Internet, through the business networks, and into the ICS networks
- ICS perimeters can be compromised through existing connectivity between business machines and ICS systems

You may not realize it, but your organization's Industrial Control System (ICS) environments are a target for cyber attackers. The ICS automation, process control, access control devices, system accounts, and asset information all have tremendous value to attackers. This poster demonstrates the many different ways attackers can gain access to an ICS environment and demonstrates the need for active security efforts and ICS engineer training that will enable informed engineering decisions and reinforce secure behaviors when interacting with an Industrial Control System. In many cases, these are not one-off attacks, but are planned with reconnaissance, persistent connectivity, stolen accounts, multiple backdoors, and adjustments to tactics as needed. These are campaigns that happen over the course of months, and require system owners/operators to be vigilant, recognizing when something is not right.

ICS Security Goal:
Ensure the safe, reliable, and secure operation of ICS environments from procurement to retirement

Abnormal activity or unexplained errors deserve a closer security look

ICS Networks

- It is very easy to maneuver undetected throughout a control environment, for both attacks and malware, until it is too late
- Most ICS protocols are susceptible to network-based man-in-the-middle and spoofing attacks. When defenses are available in the protocol, they are often not enabled
- SCADA and other WAN connectivity carrying ICS traffic between sites provide a greater attack surface for compromise
- Wireless connectivity between systems and devices is common in modern ICS, providing attackers greater opportunities to capture, block, and inject your traffic

Social Engineering

- Attackers have 20+ years worth of usable exploits since most ICS software and operating systems are infrequently patched and are used past vendor end of life dates
- Built-in host defenses and endpoint protection solutions are not common in ICS, limiting visibility of attacks and compromises
- Attackers leverage default usernames, weak passwords, and outdated authentication mechanisms
- Embedded devices like DCS controllers, PLCs, RTUs, IEDs and IIoT devices have few if any defenses

Supply Chain

- ICS infrastructures can be attacked through compromised vendors, contractors, or integrators
- ICS hardware and software can be directly breached prior to arriving in the production environment

Governance

- ICS environments are often exceptions to corporate security policies and requirements
- Cyber attacks often aren't considered in ICS incident response procedures. As a result, systems are attacked again as soon as they are brought back up
- ICS assets are often architected or assessed from a safety and reliability perspective but not always from a cybersecurity perspective

Physical Security

- ICS assets are often in remote geographies or are unmonitored and physical security protections are often insufficient. Attackers who can go to the site can steal or alter ICS device
- ICS assets containing sensitive information such as passwords, cryptographic artifacts, firmware, and intellectual property can be physically extracted from devices
- Physical changes or alterations to ICS devices are often difficult to detect

SANS The most trusted source for cybersecurity training, certifications, degrees, and research

ics.sans.org