WHITE PAPER

Critical Infrastructure Security Guide 1:

What network operators need to understand about the cyber security threat

Critical Infrastructure Security Guide 1:

What network operators need to understand about the cyber security threat

Industrial Control Systems (ICS) monitor and manage much of the critical infrastructure we depend upon - assets such as electric power grids, nuclear power plants, water and wastewater pipeline systems, oil and gas production facilities, rail systems and many more.

Advances in IP-based communications technology, automation, and computer networking have dramatically improved the scope and responsiveness of the modern ICS. Using specialized automation, computer networks, and high-speed communications, an ICS enables assets to be managed 24/7 in real-time reliably, quickly, and often over wide areas.

However, this progress has also opened the door to a new threat: the cyber-security attack. The same technological developments that drive modern ICS design with enhanced connectivity, can also enable hostile groups or individuals to gain access, steal data, take control of industrial equipment or an entire plant or even shut down operations altogether. Because these services are so critical, and interruptions have the potential to endanger lives and economies, it is vital to secure the communications systems that act as the nervous system of an ICS.

This paper will detail the importance of cyber security on our communications networks, and introduce some important concepts and ideas, as you begin to strengthen and secure your network.

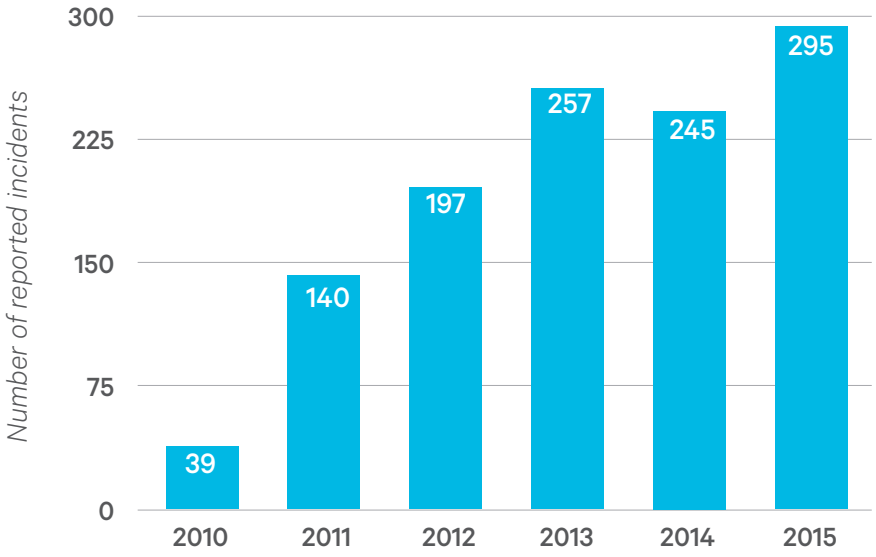
- **The nature of the threat**
- **What is an industrial control system?**
- **Some dangerous assumptions**
- **Identifying borders, frontiers and attack surfaces**
- **Types of cyber attack**
- **The next frontier: the Internet of Things**
- **Where to start**
- **Where to go for more information**

THE NATURE OF THE THREAT

The past decade has seen a steady rise in cyber-security attacks on industrial control systems throughout the world. For example:

- **2015** – A cyber attack on December 23 caused a power outage in western Ukraine impacting 225,000 customers. The attackers remotely tripped breakers after installing malware, thereby bringing down the power grid. They also clogged the utility's service center with spam calls to block genuine calls from affected customers. [1]
- **2013** - Iranian hackers infiltrated the operations center of the Bowman Avenue Dam, a small flood control dam in New York, by means of a broadband cellular modem that connected the dam to the Internet. While the dam controls were not accessed, the facility was targeted by a wider network scan for industrial control systems exposed to the Internet.
- **2010** – The Stuxnet computer worm penetrated an ICS at the Natanz Iranian nuclear facility via a portable USB drive. It infected the Siemens Simatic S7 programmable logic controllers that managed the centrifuges used for fuel enrichment, speeding them up until they self-destructed.
- **2005** – A report for the Idaho National Laboratory (a US Department of Energy National Laboratory) detailed 120 cyber security attacks on US control systems. [2]

An incident report recently issued by a US government agency tasked with tracking ICS security threats noted the trend from 2010-2015:



These figures summarize only reported incidents inside the USA - many other countries experience significantly more attacks. The United Kingdom, for example, reports daily attacks against its national electricity grid. Moreover, it is likely that most cyber attacks go unreported, so the upward trend in security incidents is actually steeper.

Given such disturbing statistics, we must look at why these systems are vulnerable to cyber attacks, and how they can be made less vulnerable. We need to understand what's inside an ICS, (regardless of the industry it operates in) and the nature of the attacks that are commonly launched against it.

WHAT IS AN INDUSTRIAL CONTROL SYSTEM?

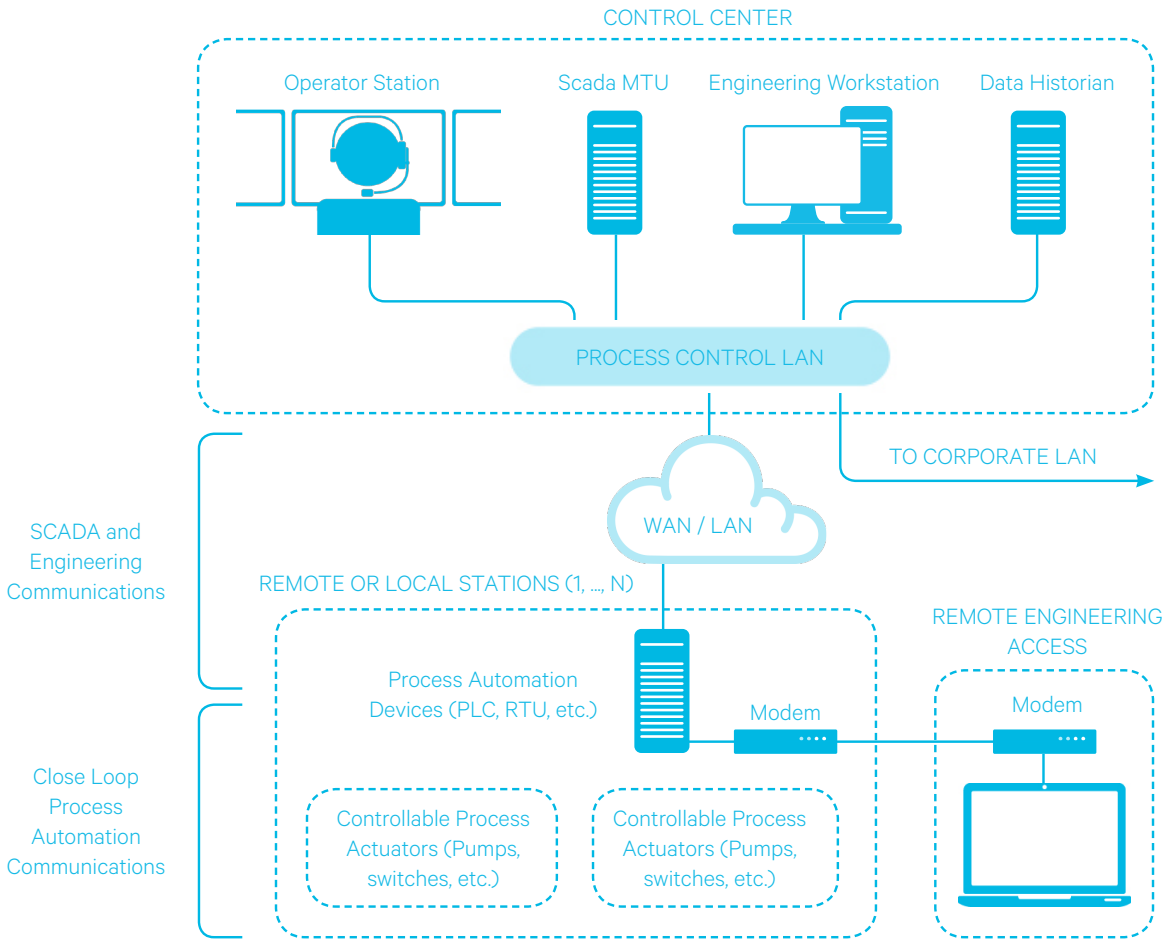
You might find an ICS (Industrial Control System) controlling a field of oil rigs, or refinery processing equipment, or an electricity distribution network, or a factory assembly line. In its most narrow sense, an ICS is either a supervisory control and data acquisition (SCADA), or distributed control system (DCS), or programmable logic controller (PLC) system that monitors and controls a set of industrial equipment.

The use or SCADA, DCS, or PLC is determined by:

- area of operation (SCADA and DCS can be very wide area, PLC is plant-level),
- bandwidth (SCADA and PLC are low-to-medium bandwidth, DCS is high bandwidth),
- reliability (SCADA may have variable reliability, DCS and PLC are highly reliable).

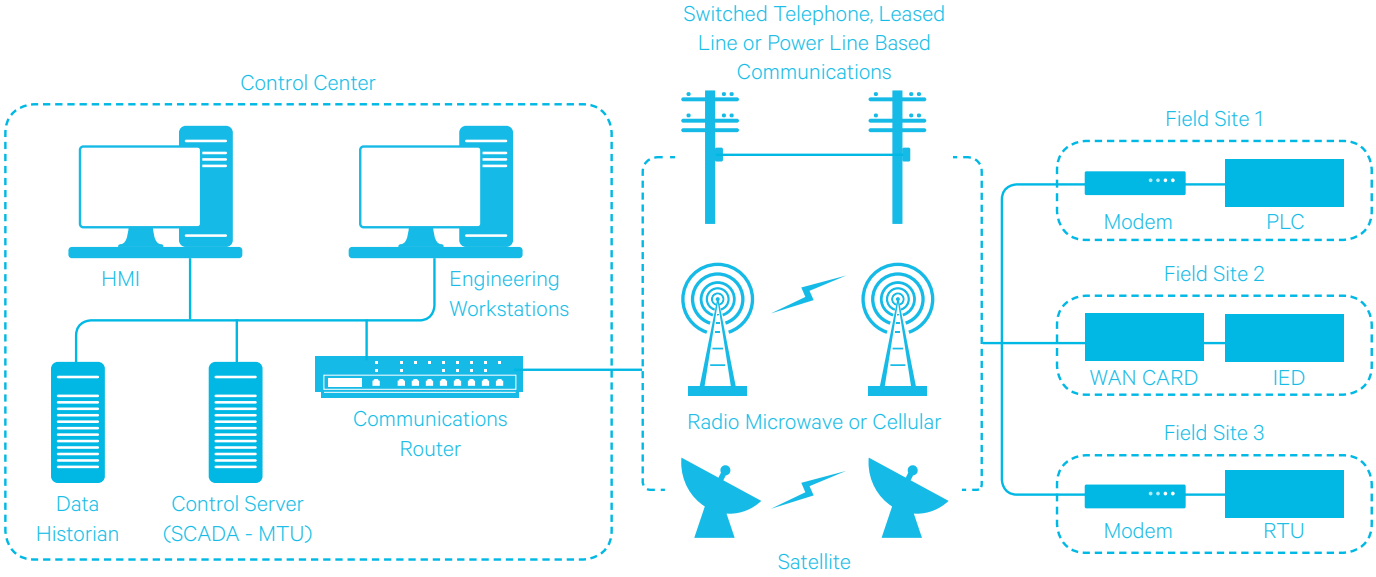
However, advances in equipment design, communications, computer and automation systems have increasingly blurred these distinctions to the point where a single, general-purpose device may replace all three types of ICS.

A generic ICS looks something like this:

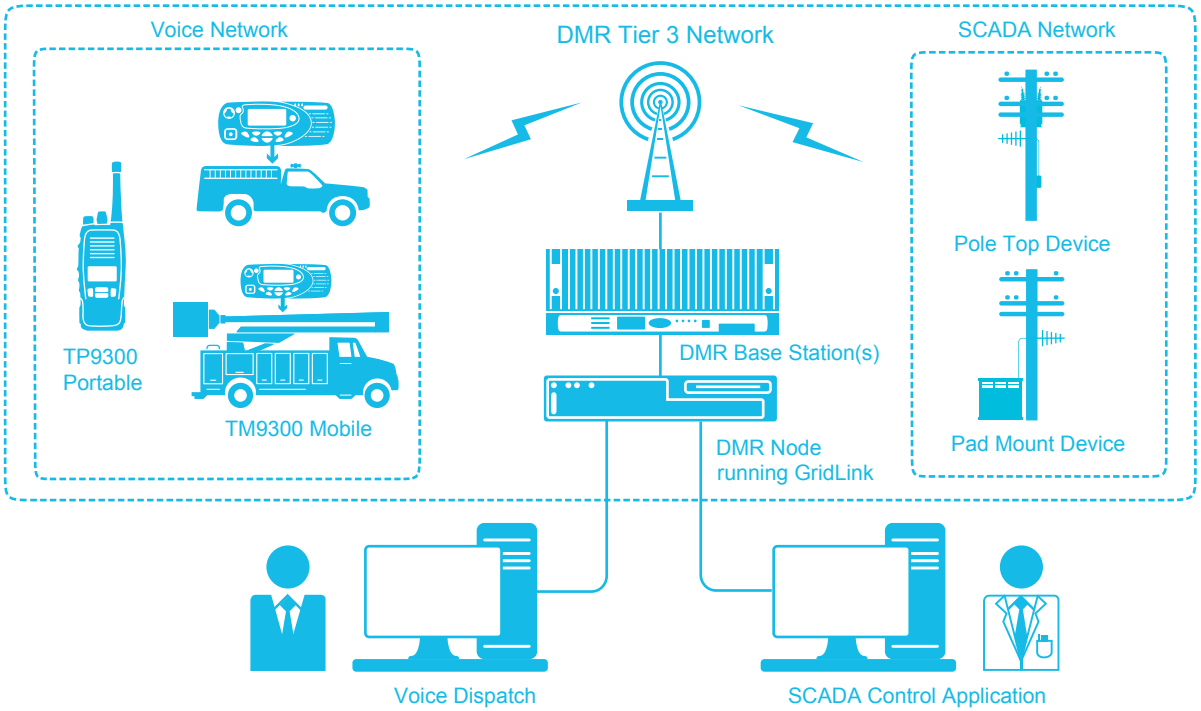


Data (meter readings, equipment status reports) are sent from a remote or local site to a control center where - by human or automatic intervention - supervisory commands can be sent back to the remote site. Controllers trigger actuators to change the operation of physical equipment at that site. Equipment can be remotely monitored and controlled, and its operation can be modified, turned on, or off.

A wide area SCADA or DCS system will generally include a communications network (fiber or copper line, radio/cellular/ microwave wireless, or satellite):



A specific example of this generic design is a Voice+SCADA system using Digital Mobile Radio (DMR) communications to connect a dispatch center, field maintenance crews, and an operator using the Human-Machine Interface (HMI) of the SCADA system.



A modern ICS typically embraces multiple field systems (multiple SCADA/DCS/PLC systems) interconnecting over multiple communications networks (radio, cellular, fiber, satellite etc.) to a centralized control center - and possibly regional control centers. If there is a connection to the corporate network, it is usually via the control center.

A wireless network connects these elements, and, utilizing purpose-built applications, sends their combined and integrated data to servers for storage, retrieval, processing and analysis. Within an ICS the number of smart, IP-connected, embedded elements trading data and control messages can run into the thousands.

What makes an ICS vulnerable?

For years, security experts have been sounding alarms about the susceptibility of SCADA systems to attacks. Here are five compelling reasons:

Mandated network performance

Many of the devices or facilities managed by an ICS are supposed to run without interruption around the clock. There are even strong economic or regulatory penalties to discourage operational downtime. As a result, any maintenance tasks or upgrade installations which might interrupt operation become a major issue. Retrofitting security, applying regular firmware patches and updates, or replacing legacy equipment frequently fall into the 'too hard' category.

Legacy equipment

Another source of vulnerability lies in the legacy content of an existing ICS. The most IP-ready field equipment or web-based control center applications may still be connected to a SCADA or DCS system that may be 15 to 30 years old. Created in the pre-history of security, they were never designed with security in mind. Isolated, site-specific systems, they employ simple, insecure, non-encrypted communications protocols over serial lines.

Early industrial control systems were designed for reliability rather than security, since there was no Internet to complicate the picture. Trusted components (sensors, controllers, workstations) were easy to connect, and data and commands used manufacturers' transparent serial protocols across medium bandwidth links that were not always dependable. Components had no built-in security or communications protocols, interfaces were unprotected, and all users were assumed to be authorized. And the monolithic network architecture ensured that there were no security checks to impede transmissions. So, while such integration undoubtedly bring performance and operational benefits, it also opens the door to unforeseen hacks.

"... a large, expert and active hacking community directs their efforts to exposing and often exploiting flaws in operating systems and architectures..."

Reliability vs security

With the development of computer networking, which enabled COTS switches and routers to create and interconnect multiple subnetworks, ICS operators took advantage of the better performance, increased reliability, and reduced costs of COTS networking to improve their networks.

Unfortunately, security innovation was largely left behind: the components were still insecure, communications protocols were still mainly clear text, and authentication of users and applications was still weak. Some attempt was made to separate control networks from corporate networks using firewalls, but the design goals were still more concerned with reliability and cost reduction than with security. This might be described as 'insecure-by-design'.

Deliberate hacking and intrusion

To make matters even worse, a large, expert and active hacking community directs their efforts to exposing and often exploiting flaws in operating systems and architectures. Hacks of popular operating systems commonly used in ICS and corporate workstations (such as Windows or Linux), or cell phone operating systems (such as Android) are constantly in the news. But even a proprietary operating system that executes on a SCADA/ICS controller is at risk. Most ICS devices allow remote access for maintenance, allowing an intruder to enter via a maintenance laptop.

Failure to maintain

Corporate policies and regulatory controls may 'freeze' an ICS when it is first commissioned and certified, making patching and updating vulnerable operating systems all but impossible.

It is difficult to retrofit security onto a design which is unprotected at so many levels. If you consider all the possible hardware, software, network, and physical vulnerabilities of a system (its 'attack surface'), it soon becomes clear that only a complete redesign from the ground up will secure the ICS from known threats. However, an operator who is aware of the problem and has completed a thorough attack surface analysis can begin to plan for change.

SOME DANGEROUS ASSUMPTIONS

Facing up to cyber attacks is not a fit-and-forget exercise. It is an ongoing, and constantly evolving challenge. To assume that a security retrofit is good enough, is a failure to grasp the complexity and dynamic nature of security. In particular, legacy equipment is responsible for some dangerous assumptions among ICS operators, which blind them to the vulnerability of their systems.

Dangerous Assumptions

1. **An ICS is safe if it is not connected to the Internet.**
2. **Attacks come from outside the ICS rather than inside.**
3. **Firewalls will protect an ICS from all attacks.**
4. **The proprietary communications protocols used by an ICS can help protect it.**
5. **Cyber attacks are generally targeted, so a low-profile ICS will not be targeted.**
6. **Security can be retrofitted to an ICS on an "as required" basis.**

The Stuxnet attack on the Iranian centrifuges (page 4) knocks over the first four assumptions, since the Iranian ICS was not connected to the Internet, and had military grade firewalls The attack vector was an infected USB drive plugged into a workstation within the ICS, which targeted the proprietary Siemens PLC.

And the Bowman Avenue Dam event (page 4) upsets the fifth assumption as the hackers apparently did not specifically target the facility. They picked it up in a wider network scan for unprotected Internet-connected ICS.

Assuming that security can be simply retrofitted to existing ICS (Assumption 6) is rather like fitting a spoiler to an old car - dangerous because it contains an element of truth that can mislead an ICS operator to think that they have done enough to protect their system. It is true that any extra security is better than none, but the security improvements that can be retrofitted are severely constrained by the limitations of legacy equipment and may not even meet current or future regulatory requirements. They will provide far less protection than security that has been designed into the ICS from the start.

The only assumption you can safely make is that your network is not safe. ICS operators can become their own biggest threat if their attitude to security is based on legacy assumptions. That is why assistance from experienced security professionals is critical, to combat the many different types of attack that can be launched against an ICS.

IDENTIFYING BORDERS, FRONTIERS AND ATTACK SURFACES

A key principle of security is to define a border or frontier associated with the assets you need to protect. Also referred to as the "electronic perimeter", it resembles a country trying to protect its border from unseen and potentially hostile forces. Each "crossing point" – where your system interacts with external systems or devices - must either be the focus of protection or, where possible, eliminated entirely.

Systems without connection to the outside are obviously much more secure, but entirely disconnected systems are generally not very useful. But even these are not entirely safe, as attacks can be subtle, or even launched from inside. A crossing point might be an entirely segregated server or network that is secure against direct external attack, but it can still be compromised through its power or air-conditioning systems.

An attack surface is the theoretical set of pathways where your system can be compromised, and is the sum of all points of vulnerability. Obvious threat points are the internet and connection to other external networks, but there are others. These include base operating systems, open-sourced or licensed software components and databases, technicians' laptops, cell phones, or USBs used during routine maintenance. The increased uptake of 'bring-your-own-device' (BYOD) policies in the workplace has greatly increased the attack surface.

Another vulnerability is where ICS and corporate traffic share a single communications network. Potential risks include:

- **Wider base of potential attacks**
  Since authorized users (and unauthorized users who maliciously gain access to the corporate network) can attack or monitor ICS systems, the attack base now includes ICS users plus anyone on the corporate network.
- **Denial of Service (DOS) attacks**
  This may be mounted from single or groups of corporate workstations without the knowledge of legitimate users who may have unwittingly loaded malicious code, which can even be remotely triggered. It can also occur at the interface from the node to the enterprise and disrupt consoles, on the wide area network and disrupt linking, even at the RF physical layer, with jammers.
- **Unauthorized monitoring of ICS traffic**
  Monitoring traffic does not cause immediate damage but it can provide system information to an attacker who is then more able to mount a better attack.
- **Man-in-the-middle attacks**
  By tapping into a communications link, hackers can hijack a session between authorized users or systems, enabling them to capture sensitive data which they can use to impersonate the communicating parties. Readings that are meant to go to monitoring stations can be deleted, diverted or modified, false commands can be send to operators, or data transmissions can be replayed causing network disruptions.

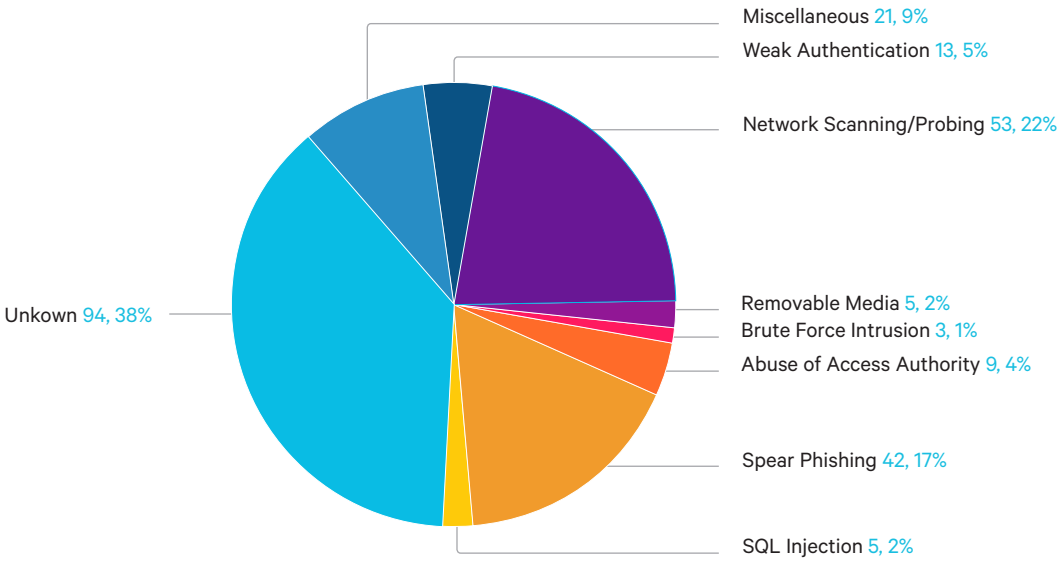
This is by no means an exhaustive list but underscores the reason ICS traffic should be isolated from corporate traffic and be tightly controlled. Regular testing of border crossing points helps to ensure security systems are performing as expected.

TYPES OF CYBER ATTACK

In one unsettling experiment, the security firm Kaspersky Lab set up a decoy on an ICS normally used to control national infrastructure. It attracted 1300 unauthorised access attempts in a single month. Four hundred attempts were successful, including 34 connections to integrated development environments (IDEs), seven downloads of programmable logic controller (PLC) firmware, and one case of reprogramming a PLC with the hacker's software.

In a security survey run by SANS security technology institute, 34% of operators responded that their systems had been infiltrated or infected in an attack at least twice in the last year. Of these, 15% said that more than a month passed before they discovered that they had been hacked, and 44% of those hacked reported that they were unable to isolate the source of the intrusion.[3]

In a 2014 year-end review,[4] US agency ICS-CERT summarized the types of attacks on US ICS systems encountered in the 245 incidents reported:



Analyzing the known types of attacks over several years, the United States Computer Emergency Readiness Team identified a substantial list of common ICS vulnerabilities including:

- Buffer overflow
- Cross-site Scripting (XSS) – where a hacker inserts and executes malicious script inside a legitimate website or web application that the victim uses
- Lack of proper access control and password policy
- Lack of data protection policy
  - » No maintenance of Operating System (OS)
  - » Outdated software utilization and poor patch management
- Lack of test facilities
  - » Dual Network Interface Card (NIC) - two network cards as security between ICS and corporate systems
  - » Lack of remote access security
- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) vulnerabilities
- Lack of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
- Clear (i.e. unencrypted) text utilization
- Poor log maintenance
- Lack of proper anti-virus or malware Protection software

Verizon's RISK security team described some of the specifics they found in a potentially serious attack in 2016 on a water treatment and supply company in which hackers penetrated a payments application and broke into a SCADA system that managed water treatment, maliciously changing water treatment chemical levels several times. In Verizon's analysis, bad network design enabled the hackers to access all of the company's equipment, find the payments application, and locate within it an .INI file containing an administrative password for a central router which allowed access the SCADA system.

Finding exposed SCADA systems is not particularly difficult. There is even a legitimate search engine SHODAN (now used mainly by cybersecurity and law enforcement professionals) that trawls the Internet for accessible SCADA systems and returns the IP addresses of the systems it locates.[5] Filters allow the searcher to focus on web cams, servers, routers, monitoring systems and so on. Hackers can develop illegitimate applications similar to SHODAN that allow them to hunt for unprotected systems without being detected.

THE NEXT FRONTIER: THE INTERNET OF THINGS

The next big evolution of industrial control systems is the Internet of Things (IoT) - physical devices communicating directly with each other, machine-to-machine, without human intervention. Smart elements such as sensors, measuring devices, and actuators embedded in control equipment can exchange data in real time, so they can be monitored, integrated, configured, optimized, and managed. In a fully automated system they can even manage themselves. Provided network bandwidth and big data applications are available to cope with the truly staggering amounts of data, the IoT vision promises huge gains in functionality, flexibility, and performance.

This vision is already upon us. A host of consumer products, such as web-connected TVs, WiFi-enabled smart LED light bulbs, home automation, and self-driving cars are in the marketplace now. All these are ultimately plugged into centralized systems which manage service provision, metering and billing. Industries such as Smart Grid utilities, Digital Oilfields, and fully automated manufacturing plants are all investing heavily in IoT systems, services and applications.

Unfortunately, the IoT is also a new frontier for cyber attacks. We have seen reports of cars remotely hijacked through their wireless interface, of Internet-connected TVs secretly collecting marketing information for manufacturers, casual hacking of home webcams, hacktivists launching attacks on power utilities. The IoT opens a new underworld in which even light bulbs can become entry points for criminals.

Every connected item is a potential security hole. This was demonstrated when researchers from security consultancy Context were able to gain a network's password at a 30-meter distance from the targeted smart bulb. As the researchers explained, "Armed with knowledge of the encryption algorithm, key, initialization vector, and an understanding of the mesh network protocol we could then inject packets into the mesh network, capture the Wi-Fi details, and decrypt the credentials, all without any prior authentication or alerting of our presence." [6]

The sheer scale of the Internet of Things massively complicates familiar security issues. The number of Internet-connected devices is estimated to reach 50 billion by 2020. When so many devices with so many different connections are sloshing around so much data, it is difficult to see how the confidentiality, integrity and availability of data and communications can be guaranteed. The big issues seem to be:

- The exponential growth in the attack surface amplifies the vulnerabilities introduced by each device and the potential attack vectors.
- The attack surface mutates every time a new device is added to the IoT network in an uncontrolled and insecure manner. Each new device must be authenticated before it is can interact with other IoT devices in the network.
- The behaviour of an IoT network can be extremely hard to predict, so a reliable threat analysis may be unachievable. Many IoT devices under development can change their behaviour in response to data they receive or sense. As a result, working out their collective behaviour is a lot more complicated.

"...Every connected item is a potential security hole. This was demonstrated when researchers from security consultancy Context were able to gain a network's password at a 30-meter distance from the targeted smart bulb..."

- Typically, IoT devices and applications are designed to start up fast, work fast, and consume as few resources as possible. Security checks slow them down and consume resources. A check to ensure that every IoT device starts up securely with unhacked firmware and legitimate settings would seem to be a basic requirement. But unfortunately, the rush to market has often meant cutting corners on security so that measures like this are either absent or downgraded.
- It will be extremely hard to plug security holes in IoT networks with software patches. IoT devices contain firmware that is built upon an embedded operating system (for example smart phone firmware built on the Android operating system). These small, fast operating systems contain multiple vulnerabilities. Software patching of a hacked device may be very hard. Given the design history of crucial Internet linking equipment such as routers and switches, some security experts doubt that fixing security holes with software updates is even achievable:

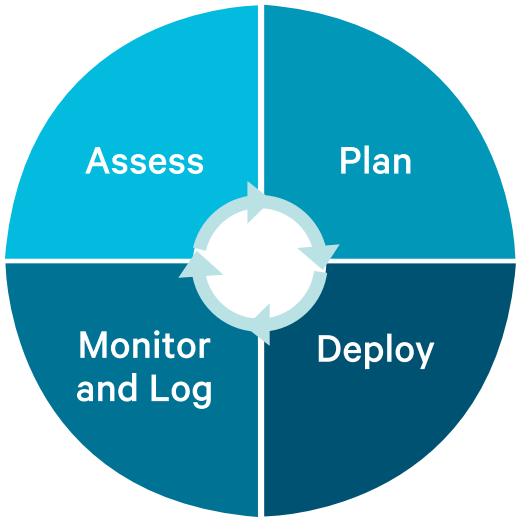
According to author Brruce Schneier, "We're at a crisis point now with regard to the security of embedded systems, where computing is embedded into the hardware itself—as with the Internet of Things. These embedded computers are riddled with vulnerabilities, and there's no good way to patch them." [7]

But despite all this, the Internet of Things is too valuable to abandon. Eventually, security solutions must be found in a mixture of new regulatory frameworks, best practice guidelines, secure designs, and perhaps, as some suggest, an alternative to the Internet to connect everything to everything.

"We're at a crisis point now with regard to the security of embedded systems, where computing is embedded into the hardware itself—as with the Internet of Things. These embedded computers are riddled with vulnerabilities, and there's no good way to patch them."

WHERE TO START

Faced with all these threats, where does an ICS operator start? A general framework helps to break down the overall process:



1. **Assess:**
   Discover and document the security requirements for your ICS. These will be driven by the standards and regulations that apply to your industry as well as by the unique configuration of your ICS.
2. **Plan:**
   Use your ICS security assessment to create a project plan and project team for protecting your ICS. There will be a variety of options to consider for addressing the vulnerabilities uncovered by your assessment.
3. **Deploy:**
   Implement your ICS security plan, tackling the most urgent vulnerabilities first. Ensure that you have included trials of all your security procedures and your training plan before going live.
4. **Monitor and Log:**
   Collect, store and regularly report data on all unexpected traffic or unusual accesses across your ICS. Keep histories in order to spot trends in security breaches.

To learn how to design and implement a cyber security strategy for your organization, see the second guide in this series:

Critical Infrastructure Security Guide 2:
How to design and implement a cyber security strategy

WHERE TO GO FOR MORE INFORMATION

There is no shortage of information and advice on cyber security issues for ICSs. As the threat level increases, governments and companies are increasing efforts to research cyber security, develop standards, and to inform ICS operators.

Most western governments have cybersecurity advisory groups, such as:

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) which operates under the US Department of Homeland Security. This web site at https://ics-cert.us-cert.gov/ includes a valuable information on Standards and References, Recommended Practices, and Alerts.
- US Computer Emergency Readiness Team (US-CERT) www.us-cert.gov)
- Multi-State Information Sharing and Analysis Centre (MS-ISAC https://msisac.cisecurity.org/advisories/).
- NIST Cyber security framework http://www.nist.gov/cyberframework/
- NSA/CSS Fact Sheet and Security Mitigation guides for ICS https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/ics.shtml.
- European Union Agency for Network and Information Security (ENISA) - Industrial Control Systems Security: Recommendations for Europe & Member States https://www.enisa.europa.eu/media/press-releases/industrial-control-systems-security-recommendations-for-europe-member-states. Their information and guidelines are globally relevant. Many security vendors provide a similar service and some specialize in specific threats.

Other web resources include:

- The Open Web Application Security Project (OWASP www.owasp.org). The diagram provides an example, identifying Cross-site Scripting as a threat, analysing its severity and providing recommendations.
- Cyber Security Evaluation Tool (CSET) which is described on the ICS-CERT web site (https://ics-cert.us-cert.gov/CSET-FAQ) as “a self-assessment software application for performing cybersecurity reviews of industrial control and enterprise network systems. The tool may be used by any organization to assess the security posture of cyber systems that manage a physical process or enterprise network. The tool also provides information that assists in resolving identified weaknesses and improving their overall security posture.”
- ISA99 (http://isa99.isa.org)
- Critical Controls information at https://www.cisecurity.org/critical-controls.cfm
- SANS Institute (https://www.sans.org)
- CERT UK (https://www.cert.gov.uk/)
- Centre for the Protection of National Infrastructure (http://www.cpni.gov.uk/)
- ICS-CERT https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities
- U. S. Department of Energy Control Systems Security Publications Library http://energy.gov/oe/services/technology-development/energy-delivery-systems-cybersecurity/control-systems-security-0
- Idaho National Laboratory Critical Infrastructure Protection Program https://www.inl.gov/research-program/critical-infrastructure-protection/
- National Vulnerability Database https://nvd.nist.gov/home.cfm

BIBLIOGRAPHY

1. Reuters February 25, 2016 http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K
2. R.J. Turk 'Cyber Incidents involving Control Systems' (Document INL/EXT-05-00671 October 2005).
3. SANS Report: The State of Security in Control Systems Today - Derek Harp and Bengt Gregory-Brow (June 2015)
4. Source ICS Cert Monitor September 2014 – February 2015
5. https://www.shodan.io/).
6. http://internetofthingsagenda.techtarget.com/definition/smart-bulb-smart-light-bulb
7. Bruce Schneier 'The Internet of Things Is Wildly Insecure—And Often Unpatchable', Wired January 6, 2014 (https://www.schneier.com/essays/archives/2014/01/the_internet_of_thin.html)

Stay updated with our latest contents

CONTACT US
www.taitradio.com/contact