How to design and implement a cyber security strategy

Critical Infrastructure Security Guide 2

© Tait Limited 2016.
Critical Infrastructure Security Guide 2: How to design and implement a cyber security strategy

Cyber security attacks are now real, present, and increasing in both their frequency and sophistication. While it is sometimes suggested that critical industries cannot risk interrupting operations to retrofit appropriate security, governments are now determined to impose regulatory controls in order to protect national critical infrastructure.

Faced with mandatory requirements to secure their industrial assets, communications network operators must be confident they have taken every precaution to protect their networks from attack. Each ICS is different and has unique requirements, so the complexity of security planning should not be underestimated. Experienced security professionals are required at every stage, from requirements capture, to design, implementation, testing and beyond, including involving them in periodic reviews and regular audits of all security policies, practices, management and reporting.

This guide provides a general introduction into the processes and technologies of cyber security, specifically in relation to the communications that integrate an ICS. Its purpose is to help managers and decision makers to understand the cyber-security implications of existing and emerging communications technologies, and how organizations can begin the process of protecting their assets from cyber-threats.

In this paper, you will learn about:

- Where to start
- Knowing which regulations apply
- Seven strategies for network security
- Where to go for more information

This guide should be read in conjunction with Critical Infrastructure Security Guide 1: What network operators need to understand about the cyber security threat.
WHERE TO START

Faced with all the threats and challenges described in the previous guide, where does an ICS operator start? You can begin by becoming familiar with these three goals for your cyber security challenge:

- To define and protect your frontiers and reduce the attack surface.
- To install mechanisms to detect intrusion and mitigate its effect.
- To create a dynamic and evolving process that can keep pace with the appearance of new threats.

Because the threat landscape is perpetually changing, you will need to regularly update your ICS security requirements, protection and monitoring measures. This is not a fit-and-forget exercise.

The following is a general framework to break down the task into clear steps.

Note that the process described here is not intended to replace specialist advice. We strongly recommend that you engage the services of a cyber security expert to ensure that your network is secured. However, it is also important that you understand the steps that need to be taken, and that you are well informed on the risks, threats and mitigation strategies available to you, so you are better equipped to work effectively in partnership with your chosen professional.

Step 1: Assess

Document the security requirements for your ICS. These are largely driven by the standards and regulations that apply to your industry, as well as by the unique configuration of your ICS.

You will need to:
- Recognize which cybersecurity regulations and standards are applicable,
- Identify all hardware, software and network components as well as all their interconnections that can provide access,
- Locate all potential points of access,
- Determine all the legitimate users and applications and the access privileges they require,

Step 2: Plan

There is no one-size-fits-all plan for making an ICS secure. Your ICS security assessment informs the project plan and helps to identify the stakeholders and experts required for your project team.

There will be a variety of options to consider for addressing the vulnerabilities identified by your assessment. Each ICS has its own special requirements that are uncovered during the Assessment phase. Professional expertise during the planning phase will prioritize which options to include in your plan.

However, it is possible to outline some strategies that operators typically use to mitigate the vulnerabilities of an ICS.
• Equipment replacement plan (removing components that cannot be secured).
• Change management plan for firmware, software, and OS patches/upgrades or reconfigurations.
• Network segmentation plan (firewalls, secure architecture, locking down unused ports, deploying ‘data diodes’ where one-way communications is sufficient).
• Application whitelisting to block access and execution of unknown applications.
• Encryption of transmissions.
• Monitoring and limiting remote accesses.
• Authentication plan, including multi-factor authentication, strict access control.
• Response and recovery plan which describes responses to specific threats and how to recover from them.
• Test plan, including penetration testing.

While not strictly a cyber security issue, you will also need a physical security plan for securing equipment and premises. This helps prevent direct attacks on your network, via malicious or accidental intrusion from equipment and devices such as smartphones, laptops, USBs etc.

**Step 3: Deploy**

Implement your ICS security plan, tackling the most urgent vulnerabilities first — the most common threats which could cause the most severe damage. Prioritizing vulnerabilities and threats can help to create a phased deployment plan.

Securing an industrial control system inevitably involves disrupting its 24/7 operations. Regulators and all levels of internal management must buy into the deployment project and compromise on policies and penalties that will cause any disruption. It is a matter of cost versus risk. Ensure that you have included trials of all your security procedures and your training plan before going live.

Increasingly, national and regional regulators are requiring mandatory compliance with security standards and certification under compliance programs. However, they are also a valuable source of advice and support on how to move from plans to deployment.

**Step 4: Monitor and Log**

It’s not a matter of if, but when a cyber security breach will occur. The one assumption you can safely make is that your network is not safe. You can expect to suffer a breach of security and should therefore have your response prepared in advance. Even with the best processes, tools and dedicated security personnel, a new form attack can get through.

A good starting point is to collect, store and regularly report data on all unexpected traffic or unusual accesses across your ICS, and keep histories so you can spot trends in security breaches. And while it may seem obvious, a vital aspect of mitigation is to avoid repeating the same mistakes — careful examination of the audit logs can be useful to establish what happened.

To ensure the best possible outcome, many organizations maintain a Computer Security Incident Response Team (CSIRT), trained to respond quickly and effectively to Cyber security incidents. The team is not usually responsible for detecting incidents — their role is to ensure that the response is coordinated to mitigate harm to the greatest degree possible. Your CSIRT needs a tested and regularly exercised response and recovery plan that describes and documents procedures for responding to an attack.

This might include:
• wholesale password resets,
• shutting down parts of the ICS network,
• running deep virus and malware checks.

A recovery plan should include regular backups of critical data that can be used to restore some or all of the ICS operation as quickly as possible.

Security specialists can use a variety of tools such as Intrusion Detection and Prevention Systems to detect and identify intrusions, log and report to the ICS operators, and even to prevent the intrusion from causing any real damage. However, such tools can also be analyzed by hackers looking for ways of avoiding detection, so you cannot rely exclusively on technology to detect an attack.
KNOWING WHICH REGULATIONS AND STANDARDS APPLY

Every industry sector has its own specific security threats and most often, is subject to mandatory requirements with governmental or other regulatory oversight. Regulatory bodies create industry guidelines and standards.

For example, the United States electrical utility sector is regulated by the Federal Energy Regulatory Commission (FERC) and North American Reliability Corporation (NERC). NERC has created specific regulations designed to protect against attacks that might compromise the bulk electrical system. They also publish important guidelines and suggested implementation notes that will be a valuable resource.

Most governments now regulate Critical Infrastructure Protection (CIP), including cyber security. These govern the infrastructure — energy, water, communications, etc — that are critical to the economy and society.

Globally, two closely-related groups of high-level standards have key bearing on CIP and the associated industries:

- **ISO27000** is a process framework from the International Organization for Standardization for operational security management. It is comprehensive and defines sector-specific guidelines. For example, ISO27032 provides guidelines for Cyber Security. (Standards and guidelines derived from ISO27000 are used throughout Europe.)

- **NIST SP 800** focuses on computer/cyber/IT security guidelines, recommendations and references from the US National Institute of Standards and Technology. NIST SP 800 is now widely used as the basis for other industry-specific recommendations. For example, NERC relies heavily on NIST SP 800 to create the NERC CIP version 5 regulations for the North American Bulk Electrical Supply industry.

Within the US, eight regional entities have delegated authority from NERC. (An example is WECC, the regional entity for the Western interconnect.) Regional entities coordinate and support interconnection members, most of which have active Cyber Security programs and can provide additional advice. In particular, the regional entities create Inherent Risk Assessment (IRA) reviews to provide a professional assessment and security compliance process for utilities. Regional authorities also maintain resource centers on their web sites, containing informative industry discussions and forums.

“...in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system, or energy management system separated from the enterprise network.”
SEVEN STRATEGIES FOR NETWORK SECURITY

Here are the most commonly-used security strategies that operators should consider as part of their security portfolio.

1. Isolating networks and traffic

Isolating traffic is a good way to deliver better Cyber Security outcomes. Internet connection sharing connects multiple LAN computers to the Internet through a single connection and a single IP address. Clearly, this represents a security risk, which must be mitigated. ICS traffic profiles and types — and the need for predictable, real-time performance — differ from normal corporate traffic. By definition corporate networks are normally attached to the internet. ICS systems should not be. The two should be separated, normally with industry-proven firewall technology. This involves carefully defining rules for all traffic that is allowed to flow across your border. Access is restricted to users who genuinely require it — and who can prove they are who they say they are. Isolation also applies to the type of traffic on the ICS network, restricting or removing traffic such as FTP, email and remote access. In fact, a serious risk analysis should be undertaken before allowing any new traffic on an ICS network.

Given that connections to the corporate network provide the greatest source of malicious code intrusions, it would seem obvious that severing ties to the corporate network would dramatically reduce ICS infections. Many ICS operators believe that they have no direct connections to the Internet and have successfully isolated their ICS from Internet hacks. However, as the US Department of Homeland Security reported:

"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system, or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network."

Risks from mixing ICS traffic with corporate traffic 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.

- **Denial of Service (DOS) attacks**
  This may be mounted from individual or groups of corporate workstations, without the knowledge of legitimate users who may have unwittingly loaded malicious code. It can be remotely triggered, and can occur at the interface from the node to the enterprise. Jammers disrupt consoles on the wide area network, and linking at the RF physical layer.

- **Unauthorized monitoring of ICS traffic**
  Monitoring traffic does not cause immediate damage but it can provide system information to an attacker who is then better able to mount an 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 why ICS traffic should be isolated from corporate traffic and be tightly controlled. Regularly testing border crossing points helps to ensure security systems are performing as expected.

In reality, it is practically impossible to fully isolate networks. By necessity, traffic is mixed, as IP phone systems, IP consoles, workforce management, location services and SCADA applications are integrated. Current approaches to separating traffic include:

- MPLS (multi-protocol label switching) to separate traffic based on packet labelling,
- Carrier Ethernet based on MetroEthernet technology connecting subscribers and operators to a metropolitan WAN.
2. Network segmentation

Another way to achieve better isolation is to break a large network into smaller subnetworks which act as operational zones, each with its own security requirements. To move from zone to zone a user or application must satisfy the security requirements of each zone.

Network segmentation, properly implemented, will limit free access across the network and can restrict the damage caused by a malicious intruder to the zone level. Your consultant or specialist can provide information and advice here.

3. Firewalling

Firewalls prevent unauthorized users — usually from the internet — from accessing private networks. Every ICS network will contain some open ports, and firewalls provide a level of protection for these. Messages entering or leaving the internet must pass through one or more firewalls, which examine each message and block those that do not conform to security criteria. However, firewalls are only truly effective when you have excellent knowledge of your core network elements and can map them to flows of data you will allow or block. Network components should be fully documented in a current, continuously-maintained network plan.

There are several types of firewall technology (and many protocols) and you should seek expert advice on choosing the right one. For example, ‘stateful inspection’ firewalls, joined through a secure portion of the network called a ‘demilitarized zone’ (DMZ) or ‘perimeter network’, can provide the high degree of isolation required. They perform dynamic packet filtering, checking packets to see if these are coming from the right connection rather than through a back door.

While segregating traffic can improve overall performance, this is more complex than deploying simple enterprise firewalls. Careful design will ensure that complexity does not result in delays or confusing configuration. In fact, firewalls should be the only dual-homed devices — simultaneously attached to two networks on the network.

Some sites pair two firewalls from different manufacturers, to further reduce the effect of compromise. There are many possibilities, including more layers of DMZ but excessive complexity should be avoided as it can lead to confusion. The firewalls and DMZ combination will:

- isolate traffic and segregate users,
- enforce secure authorization of all ICS users according to the organization’s policy (which should be regularly reviewed),
- enforce end-point ICS security where users only gain access to devices they are authorized for.
The diagram from NIST SP800-82 illustrates a general configuration for reasonable security and performance. Each customer solution needs to be designed to meet specific needs. Firewall configuration is beyond the scope of this document but should be carried out by an expert in both the equipment and the specific network. A useful starting point is “deny all” as a baseline, and to only allow traffic once it has been assessed for risk.

It is somewhat alarming to discover that many companies simply use the default configuration provided by the firewall supplier. As a result, a 2004 survey of 37 company firewalls found that:

- nearly 80% allowed “Any” services on inbound rules as well as unsecured access to the firewalls and the DMZ
- roughly 70% permitted devices outside the network perimeter to access and manage the firewall

What sort of traffic commonly travel across an ICS firewall and what risks do they pose? Firewall configuration should screen all traffic, block undesired traffic, and allow the rest only under particular circumstances.

**Common firewall protocols**

The following list gives some general guidance on common firewall protocols.

**DNS (Domain Name System)**

DNS converts domain addresses into real IP addresses. It is fundamental to the Internet but is normally not required to transition across the DMZ in either direction.

**NAT**

Network Address Translation is required by IPv4 to minimize consumption of IP domains. It remaps internal domains to single external IP addresses and is very widely used, as IPv4 address space becomes exhausted.

Without NAT, internal networks may not be able to communicate, but its use should be carefully controlled and domain mapping well documented. Some protocols, such as those requiring direct addressing, are broken by NAT and may require special tunneling modes. Consult a firewall specialist or vendor on the use of NAT, particularly with multicast traffic, to avoid unintended consequences from forwarded packets.

Although NAT is not required by IPv6 (which has no shortage of addresses), it may be needed to connect IPv4 and IPv6 networks.

**HTTP**

HTTP is the core protocol for web browsing, along with its secured version HTTPS. Base HTTP has no inherent security and should not be used to cross from a corporate network into the ICS. However, it is increasingly used to configure devices through embedded web servers, so it is essential to secure it as thoroughly as possible (such as only allowing HTTPS) and only to nominated devices. Some firewalls block scripts and Java, both common attack vectors carried by HTTP.

For example, Tait base stations use embedded web servers for remote access to network management. A digital certificate/key pair provides secured HTTPS access. (The key is encrypted while the certificate authenticates the key.) For maximum security, a certificate is generated and signed by an external authority trusted by the browser.

By default, the base station generates its own self-signed certificate. This allows traffic to be encrypted, but does not provide authentication. The browser displays a warning when connecting to the Web UI.

You can upload a certificate generated by a trusted authority. For a public network, the certificate may be obtained from a commercial provider. For a private network, it may be generated by the network’s own certificate authority, and the certificate added to each browser’s list of trusted authorities.
SNMP
SNMP is widely used to monitor and control devices remotely, and to send alerts. Most routine traffic is the result of periodic polls from a central Network Management System, which cause devices to send a structured message in response. SNMPv3 has limited security but earlier versions have no security and can potentially completely reset or reconfigure devices. (SNMP v3 uses SHA-1 and AES128 encryption and provides encryption and authentication in both directions.)

To balance useful functionality with the significant risk it poses, restrict SNMP to nominated stations and only between the DMZ and ICS; there should be no need for SNMP traffic from the corporate network; consider disabling SNMP unless it is specifically required.

DNP3
Critical for most SCADA applications, it originally had weak inherent security making it vulnerable to man-in-the-middle and spoofing attacks. An attacker could easily pose as, or control any device.

However installations may have a mixture of systems, so ideally, DNP3 should not be allowed past the DMZ. No DNP3 traffic should be accepted from the corporate network unless it is a requirement of the system architecture. Newer versions support IEC 62351-5, which provides authentication for IEC 60870-5/6 (SCADA)

FTP and TFTP
These file transfer protocols are convenient, but have little or no security so they pose a significant threat. If possible they should be prevented from crossing the DMZ.

There are some secured versions but they are not widely deployed and unless operated within a VPN tunnel, they should be used with care. Careful design is needed for any system that relies on FTP or TFTP and it is preferable to block these.

PING and ICMP
PING is useful to determine presence but that alone may be enough to compromise security so you should give very careful consideration to whether PING should be supported. Many systems do not allow it and disable ICMP echo and timestamp, especially on broadcast or multicast addresses.

Telnet
This older protocol provides remote terminal access to devices, similar to the DOS command line. A common attack vector, it is not secured and should not be allowed to transition the DMZ without being enclosed in a secured tunnel and linked with strong authentication to specific devices.

SMTP
A simple email transfer protocol, SMTP is widely deployed and is a common source of attacks. Many devices within an ICS will use it to send automated messages to control systems. The safest option is to prevent SMTP crossing the DMZ in either direction, but it is possible to secure outbound-only (such as ICS-to-corporate) with care.

DCOM
DCOM is a Microsoft protocol often used for Process Control through Remote Procedure Calls (RPC). Even when fully patched, RPC is probably the most common attack vector. Under no circumstances should it be allowed to originate from the corporate network, and only allowed between the ICS and the DMZ with care and understanding about what it is doing. DCOM is the source of much pain.

4. Why ‘Air Gapping’ is not enough
‘Air gapping’ refers to physically isolating the ICS control network from unsecured networks such as the Internet or a corporate LAN, so that there is a physical gap between them. The devices on one side of the gap cannot communicate with devices on the other side. Based on the assumption that threats mainly come from outside the ICS, this was considered an adequate security measure. Although external threats certainly receive more attention, some statistics suggest that cybersecurity may be more threatened from within, occurring while detection mechanisms are busy with outside threats. Internal threats are a significant problem.

While we commonly characterize internal threats as malicious, an internal attack is most likely to be accidental or opportunistic. Many employees can access your systems and network, plus
contractors, third-party support and service providers: you are likely to have cloud-based IT services with administration platforms that are not visible to your organization.

Identifying and mitigating internal threats involves seemingly-endless combinations and degrees of expertise, motivation and access specific to each individual. An expert advisor can tailor security solutions based on risk.

Apart from technical solutions, five strategies deserve mention:

- **Provide security access by role to increase visibility of individuals.**
- **Enforce strong authentication policies to ensure users are who they say they are.**
- **Separate duties and responsibilities to reduce opportunity for collusion or false accusation, which can prove costly.**
- **Regularly analyze logged data to identify irregularities such as repeated access to files. Organizations typically use data forensically, but it has greater value when analyzed to identify potential attacks.**
- **Assign specific individuals to search for and identify vulnerabilities — systems, processes and people not acting “normally” should trigger closer observation.**

5. **Controlling access: The human factor**

Whatever the system, and however carefully it is designed, it will still require access by people within your organization, opening up potential vulnerabilities.

Your access method should follow a documented process, driven by regulatory needs appropriate to your industry and informed by your expert risk analysis. It is hard to generalize, given each system has its own characteristics, so you should seek expert advice.

**Complexity**

Complex systems are hard to understand, so people may try to work around processes that restrict their ability to do their job. Every process should be carefully examined to see if can be simplified without compromising the outcomes. Employees should be involved in the process and encouraged to contribute towards its design.

**Ports**

People will access the ICS elements from computers. Each computer, and the ICS elements they connect to, responds to access requests through IP ports. These allow access to specific functions within a common IP address. For example, a device will have a single IP address but packets sent to its 80 port will be directed to an embedded web server. The catch is that devices can respond to many different ports and only a few of these may be documented. These ‘open ports’ represent a threat since they provide access to functions which may not be well protected. It is best practice to disable all unused ports.

Port scanning is the most basic way to look for open ports in a device, which is precisely how vulnerabilities are exploited. By incrementing the port number, responses can give vital clues about the software and structure of the device being targeted.

Defined points of contact with corporate networks should be through a DMZ (perimeter network) which is then isolated using firewalls. Servers that support ICS functions should be located on this DMZ and access restricted to specific individuals through robust, regularly changed passwords. Access to the DMZ must be logged to a separate device which is not part of the firewall.

Obviously, each network’s architecture and security requirements are different, and expert advice is needed. A recommended source of advice on ICS architecture strategies has been developed by the DHS in the Control Systems Security Program (CSSP). NIST SP 800-41, Guidelines on Firewalls and Firewall Policy provides general guidance for the selection of firewalls and the firewall policies.

**User access control**

User level access control is as important as network level access control.

Every intruder’s target is to gain access at the highest security level. Shared user accounts and weak passwords are common targets, so root or super-user accounts must be protected with strong passwords. Users should not use root or administrator accounts for day-to-day activities.
Access levels
Username/passwords provide basic access security combined with access levels. Passwords need to follow best practice rules established by the corporate IT department and access levels rigidly enforced: users should only be able to access equipment they are authorized for. Logging access to separate, secured servers is considered best practice but you should consult an expert to ensure these systems provide the levels of protection needed.
For example, Tait systems provide three access levels:

<table>
<thead>
<tr>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Access to all pages of the Web User Interface; carry out all function</td>
</tr>
<tr>
<td>Maintainer</td>
<td>Access all pages of the Web User Interface except. Tools&gt; User &gt;Admin</td>
</tr>
<tr>
<td>Guest</td>
<td>Access to 'Monitor' only</td>
</tr>
<tr>
<td>Disabled</td>
<td>Not permitted to log in or carry out any functions</td>
</tr>
</tbody>
</table>

Specific users are allocated to these categories through access tables through LDAP (Lightweight Directory Access Protocol) or RADIUS (Remote Authentication Dial-In User Service). When a user attempts to log in, the base station authenticates them using the LDAP directory to determine if they match one of the access rules. Each rule is, in effect, a query from the base station to the LDAP directory. (Queries are made in the order the rules appear in the table.) When a match is found, the user is logged in with the access associated with that rule. If a user doesn't match any rule in the table, access is denied.

6. Hardening defenses

Operating System Hardening
Attackers use operating system vulnerabilities to break into systems. Hardening the operating system reduces the attack-surface by disabling or shutting down unused services and ports of the system.
NIST SP 800-123 Guide to general server security gives good guidance on key server security principles such as simplicity, least privilege, defense in-depth and separation of privileges to consider when designing systems.

Encrypting communications
ICS and SCADA networks transmit data and commands as clear text. At one time, operators believed that the proprietary nature of the communications protocols and the highly specialized nature of the systems offered some form of protection. They thought that hackers would find the effort of breaching these systems too much hard work — a strategy that critics have dubbed ‘security by obscurity’. Unfortunately, competitors, nation-sponsored adversaries, hacktivists, and criminals have proved to have the patience, skills, tools, and motivation to eavesdrop on unprotected communications to understand and penetrate a control network.
By encrypting all communications, you remove eavesdropping as an way for hackers to learn the operation of your ICS. Open standard SCADA/PLC protocols such as Modbus or DNP3 are preferable to relying on unencrypted proprietary protocols.
• While Modbus itself has no built-in security, encryption add-ons are available.
• Secure DNP3 is compliant with the IEC 62351 standard for managing the security of data transfers, including encryption and authentication.

More general communications within a control network can take advantage of the data and voice security features offered by modern digital wireless technologies. For example, digital radio systems originally developed for public safety organizations require high levels of security throughout, incorporating user authentication and military-grade encryption technologies such as AES.
Remote access: Virtual private Networks (VPNs) and IPsec.

If network traffic must transit public networks or over public carriers, it is normal to create secured virtual tunnels. These tunnels create Virtual Private Networks (VPNs) and are in common use over the Internet.

VPNs operate at several levels of the ISO stack. For example, commonly-used TLS and SSH methods secure applications end to end, but IP security (IPsec) operates at the network layer, so it secures any applications transiting above it — not just specific ones. IPsec does not have to encrypt traffic within its tunnel but this is normally the point of the VPN.

A full description of IPsec is beyond the scope of this document and an industry professional can offer detailed advice. However, the following table represents common industry practice when configuring IPsec.

<table>
<thead>
<tr>
<th>Aspect of IPsec</th>
<th>Usual configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of key</td>
<td>Pre-shared, minimum passphrase 24 characters</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>AES256</td>
</tr>
<tr>
<td>Hash algorithm</td>
<td>SHA-2 (256)</td>
</tr>
<tr>
<td>IPsec security protocol and anti-replay</td>
<td>ESP</td>
</tr>
<tr>
<td>Security Association ISAKMP lifetime</td>
<td>360 mins</td>
</tr>
<tr>
<td>Security Association (ESP) lifetime</td>
<td>60mins</td>
</tr>
</tbody>
</table>

7. Maintenance, maintenance, maintenance

The most advanced cyber security system is only as good as your commitment to maintain it. A current inventory of all system software currently running releases is critical. This should include threat and vulnerability reports specific to the software inventory of the target system. And while it may seem obvious, it is equally important to establish a process to identify when new ones are added.

All systems within a working architecture must be patched and updated promptly, according to manufacturers’ recommendations and industry best practice. A regular program will ensure this is done, but it is important to control installation and to test updates before going live — manufacturers’ releases can sometimes expose new flaws, or cause issues that have nothing to do with security.

Automated tools to manage and identify system parameters can reduce the overhead of dealing with these issues, but they each have their limitations. User community forums provide advice on the relative stability of releases but need to be treated with caution. Not all the advice you read is qualified, and you should consult your security specialist before committing to any new system.

“Not all the advice you read is qualified, and you should consult your security specialist before committing to any new system.”
Where to go for more INFORMATION

The additional documents listed below provide a snapshot of the vast pool of resources that will give good guidance on how to deliver a secure industry best-practice design. The NIST-800-82 document is recommended as a particularly good starting point.

- O27032 Guidelines for Cyber Security
- ISO27033 Guidelines for IT network security
- IEC62351 ICT security for power system control operations
- IEC62443 Security for Industrial Automation and Control systems
- NIST-800-39 Managing information security risk
- NISTR 7628 Guidelines for smart grid cyber security infrastructure (links to NIST800)
- NIST-800-82 Guide to Industrial control systems security
- CPNI Good practice guides on firewall deployment for SCADA and on Security for Industrial Control Systems
- DHS Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies (October 2009)
- DHS Nation Cybersecurity and Communications Integration Center (NCCIC) “Seven Steps to Effectively Defend Industrial Control Systems” (2015)

About the author

Dr Jan Noordhof is an independent consultant based in New Zealand. He was previously Principal Consultant for Tait Communications (Americas), specializing in technical solutions for public safety, utilities, mining, oil and gas sectors. Other roles at Tait included VP Product Marketing, VP Sales Engineering and Marketing (for Latin America, Africa, Middle East, and Indian Sub-continent). Dr Noordhof was responsible for bringing the Tait APCO P25 system product to the global market.

Earlier projects included R&D and product engineering roles in analog and digital radio infrastructure development, software engineering, systems programming, telecommunications, embedded system design, and teaching at a number of universities.
BIBLIOGRAPHY
