The need for security in an evolving industry

Towards agile **manufacturing**

Contents

Introduction

Manufacturing is evolving. Changing customer requirements combined with the constant pressure to reduce costs and improve productivity are driving manufacturers to adopt new business models to retain a competitive edge.

The concept of 'agile manufacturing' is becoming a key business differentiator, highlighting manufacturers that are able to thrive in unpredictable, complex, environments by focusing on individual customer needs and forming partnerships with third parties.

Businesses that are able to integrate their disparate IT systems and manufacturing systems are in the best position to capitalise on this market trend. However, such integration can expose organisations to new risks. Changing cyber security threats, particularly relating to Industrial Control Systems (ICS), mean that attackers could potentially execute malicious code on production systems to suit their own ends.

This report considers the challenges associated with integrating operational and enterprise systems and how these can be managed to maximise opportunities while minimising risk.

The evolution of manufacturing

Progressive manufacturers, no longer content to ship finished goods with limited after-sales support, are offering additional services to customers[1]. These not only add value, but also offer new sources of revenue while providing information on how customers actually use products. These insights then allow agile manufacturers to refine and improve their product offerings to meet the changing needs of the market.

In turn, customers are no longer content to purchase from a standard range of products. Customers expect, and will search for, customised products that meet specific requirements. Old, 'push', manufacturing models of 'make-to-stock' are not efficient when customers demand choice. In contrast, 'build-to-order' models are much more efficient at meeting the needs of a changing market[2,3].

However, these models can prove unsatisfactory if a customer requires a single proof-of-concept product, which may in turn lead to large orders; or when meeting the requirements of a lucrative one-off product that other suppliers may not be able to fulfill. These customer 'pull' models require more flexible approaches to manufacturing, such as 'engineer-to-order'.

Opportunities exist for adaptive organisations to seize these increased opportunities to supply new products and services or to increase quality and reduce costs. As few organisations are able to manufacture their own products from end-to-end without relying on assistance from third parties, this can result in increasingly extended and complex supply chains, which are not without risk. The increasingly connected nature of an extended supply chain means that distant disruptions to supply or sudden increases in demand can affect the production of apparently unrelated items. Managers need to ensure that their supply chain is resilient and can withstand disruption. Equally, maintaining the integrity of the supply chain so that components and their constituent parts are as specified and not defective or fraudulent is no trivial task, as the pressure to control costs may tempt some suppliers to cut corners.

Creating an agile organisation

To meet these new market challenges, manufacturers must adopt new methods of working. Partnerships with external organisations need to be forged, so that resources, expertise and production capacity can be shared to rapidly respond to changing customer requirements.

Organisations may already utilise computer aided design (CAD) tools and computer aided manufacturing (CAM) systems to increase efficiency and to share designs and production capacity with partners. However, the ability to fulfil an order is as reliant on enterprise systems as it is on production systems. To create an agile manufacturing organisation, these two systems need to be tightly integrated and combine new functionalities like after-sales and value-added services with customer management systems.

Standards, such as ISA-95 and IEC 62264, describe how operational and enterprise systems can be linked together to create an organisation enabled for 'agile manufacturing'. Although such integration offers many opportunities, it also exposes organisations to new risks that must be correctly managed.

Managing cyber security and risk

Senior managers may be comfortable with their organisation's current management of risk, however, in their desire to deliver new IT systems and infrastructure, new risks may be overlooked.

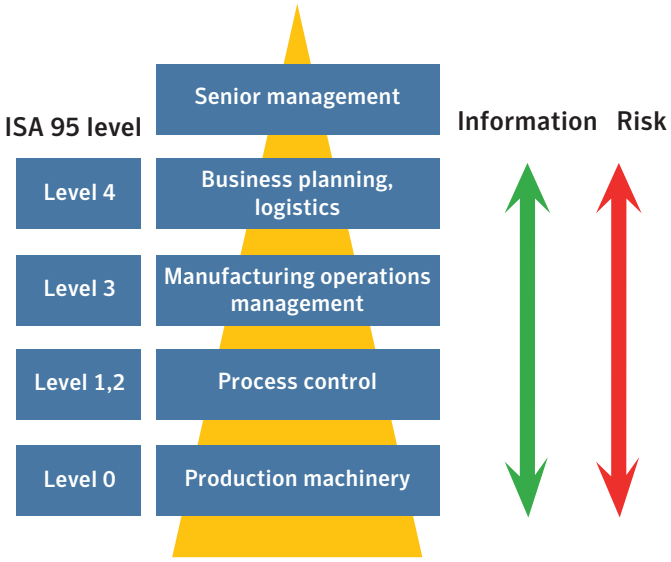

Figure 1. Flow of information and risk through the agile manufacturing organisation.

ISA 95 describes the data flows between connected enterprise systems and production systems that enable senior management to direct the agile organisation. This flow of information from low level to high level systems, and vice versa, through the stack of levels described in the standard, allows a greater degree of transparency of operation which facilitates faster management decision-making and execution. However, associated with this flow of information is also a sharing of risk. As operational systems and enterprise systems become interconnected and reliant on systems above and below them in the stack, information security risks can also permeate the stack. As a result, risks that were previously considered non-critical may increase in severity when systems are interconnected, as the consequences of a threat may impact upon disparate but connected systems.

Just as production managers need to ensure that machinery is properly maintained and serviced, so the same levels of care and attention must be paid to IT systems.

Data theft

The ability to design items digitally using CAD software and send the designs as files to CAM systems has greatly facilitated the manufacturing process. Design files can easily be shared with colleagues or partners for feedback, refinements or estimates of costs and production lead times.

However, the downside is that product designs can be copied, stolen or sent to unscrupulous competitors at the touch of a button. Equally, sales contacts and production schedules held in electronic formats can be copied and passed to competitors.

For rogue companies, stealing product designs can be very profitable. They can adopt a low-cost production model, potentially located in a jurisdiction with lax intellectual property law enforcement, or distribute products through illegitimate distribution channels.

System availability

In a networked manufacturing environment, unavailability of any of the systems can lead to outages that are entirely preventable. Companies should be aware of the common causes of IT outages and how to protect against them.

Areas for consideration include:

Component	Failure mode	Mitigation
Network connectivity	Networks may suffer from congestion or router failure which prevents systems from communicating.	A separate dedicated network for production systems.
Power systems	Power failure will stop IT systems from functioning and contribute to hardware failures.	Uninterruptable power supplies for IT systems.
Hardware	Most IT hardware is reliable for long periods, but high operating temperatures can cause hardware failures	IT equipment is kept in a temperature controlled environment.
Disk drives	Disk drives may become corrupted or fail completely causing IT systems to fail.	Dual disk drive systems are RAID configured to provide redundancy, allowing failed disk drives to be replaced.
Operating systems	Operating system upgrades are necessary to protect systems from vulnerabilities and to fix bugs but may cause the operating system to become unstable, leading to outages.	Systems are locked down and a change management system is instigated, so any changes are tested and there is an ability to roll-back quickly.
Software	Software upgrades are necessary to fix bugs and vulnerabilities, but may introduce additional bugs and cause the software to become unstable.	A change management system ensures that any changes are tested and authorised, and a strategy is in place to roll-back changes if necessary.

Change management

Over time, IT systems, including the hardware, operating systems, software and networks, will need changing. Organisations should anticipate this and adopt a ‘plan, do, check, act’ methodology. The advantages of making the change should be considered and balanced against the risks of not making the change. If a change is made, a strategy to reverse or roll-back the change should be prepared. Subsequently, the effectiveness of the change should be assessed and any potential deficiencies remedied.

Protecting against cyber attacks

Mass-market malware is a risk for any organisation as it is designed solely to make money for the attacker by infecting any computer. Typically, infected computers may attempt to send spam or participate in denial of service attacks; however, malware may also seek out personal or confidential data that can be resold. Any unencrypted confidential information held on infected machines should be assumed to have been compromised unless proved otherwise.

Malware can infiltrate systems through operators opening malicious emails and being tricked into installing malware, or from browsing infected websites. Infected websites may be entirely legitimate in nature, but have become compromised through the activity of attackers and primed to remotely install malware on the machines of visitors with vulnerable software. Infected USB sticks can also introduce malware into an organisation when used to transfer files.

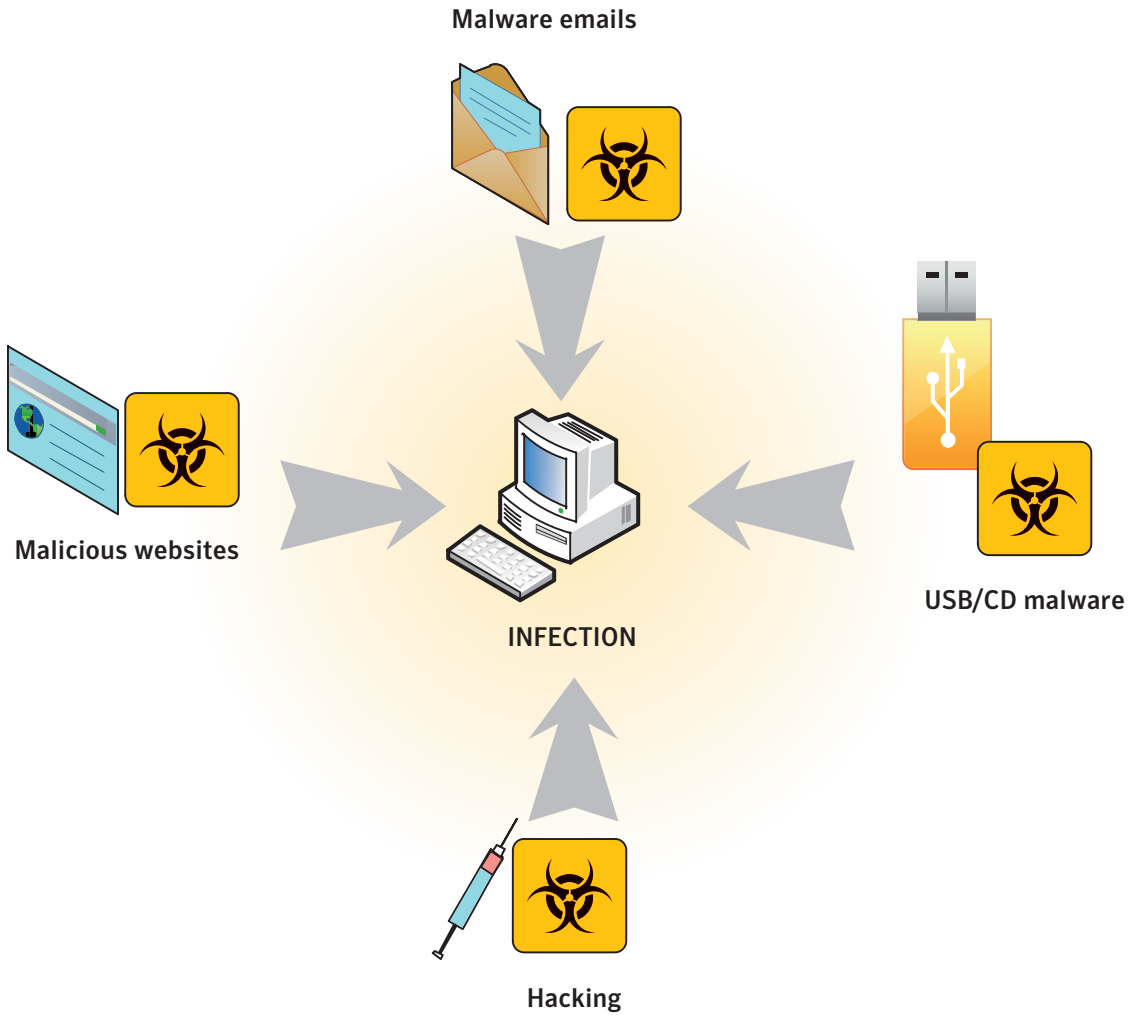

Figure 2. Means by which computer systems can be infected by malware.

Malware is also used in hacking attacks, where an attacker exploits a vulnerability to execute commands on the compromised machine. They can then download and install their own malware on the machine and use this to launch further hacking attacks on more machines within the network.

Such attacks require a level of skill and forethought that is not apparent in most mass-market attacks. Sophisticated attackers may target organisations and search for means to gain access. In order to do this, bespoke malware can be sent to previously researched individuals within the organisation, using socially engineered emails that appear legitimate to all but the most suspicious end user.

The motives of mass-market attacks are usually purely financial, but the objectives of targeted attackers may include:

- Industrial espionage – seeking to compromise company secrets or product designs that can be sold for profit or used for competitive advantage.
- Politically motivated – designed to cause visible disruption to an organisation.
- Motivated by profit – attempting to gain access to financial systems or threatening to cause expensive outages if not paid off.

ICS vulnerabilities

For many years ICS, also known as Supervisory Control and Data Acquisition (SCADA) systems, were only considered to be a theoretical target for malware. Because such systems run proprietary operating systems and software, it was believed that attackers would not have the resources to develop effective malware to penetrate them.

The Stuxnet malware discovered in June 2010 changed this perception. This program appeared to be written to affect only specific high-speed centrifuges at a nuclear facility in Iran[4]. It was capable of transiently speeding up or slowing down the centrifuges, then returning them to normal operation for prolonged periods of time, without alerting operators[5]. This subtle malfunction is believed to have had a severe impact on Iranian attempts at uranium purification and destroyed up to a thousand centrifuges[6].

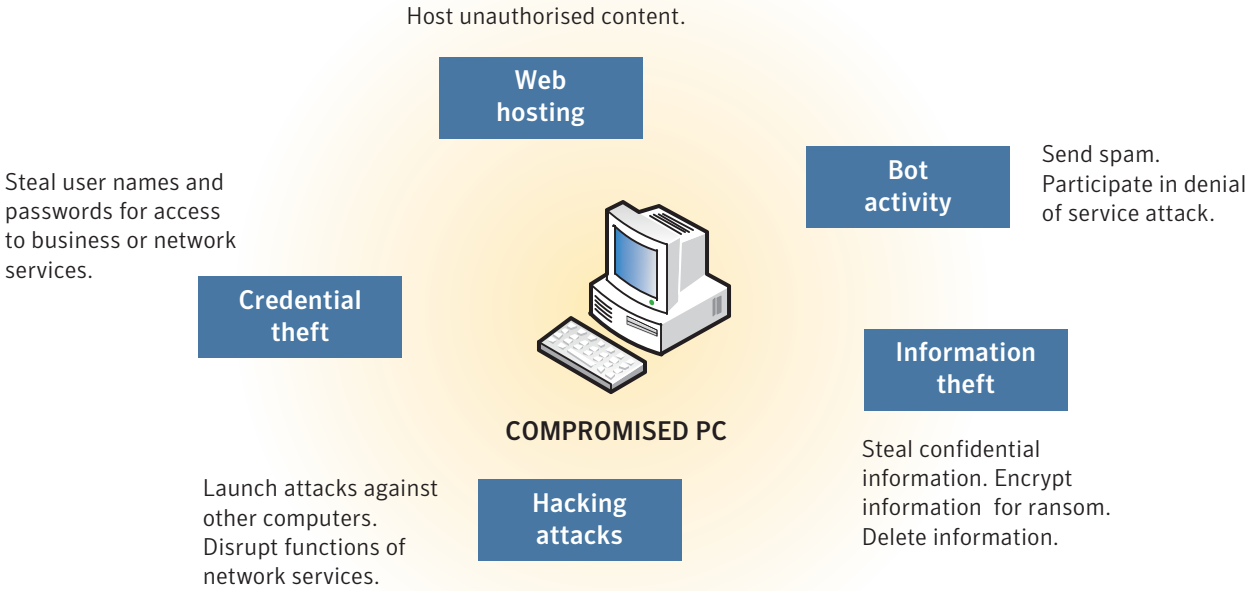

Figure 3. Possible outcomes following malware infection.

Since the discovery of Stuxnet, much work has been performed on searching for vulnerabilities in ICS that could be exploited by attackers. It has also stimulated the development of tools that can be used to identify vulnerable systems accessible over the Internet, as well as ones that remotely exploit vulnerabilities to install malware on the system[7,8].

Organisations should also be aware that attackers do not necessarily need to gain access to computer systems in order to issue unauthorised commands to ICS. These systems may not have been designed with security in mind, allowing imaginative attackers to find ways of bypassing legitimate control systems to issue their own commands. In 2008, a teenager was allegedly able to modify a TV remote control to change the points on the Lodz tram system, subsequently derailing four trains[9].

Although the data held on ICS is unlikely to be highly confidential, attacks on such systems may result in damage to machinery and lengthy outages, not to mention undermining the integrity of the system. ICS differ from other IT systems as they interact with the physical world. The compromising of ICS by attackers, and the ability of malicious individuals to control machinery is a potential safety issue that spans the domains of both information security and health and safety.

Building security into products

Designers should not underestimate the ingenuity of attackers in identifying security weaknesses in manufactured products, especially when there are tangible financial gains to be made from compromising the product.

Examples include:

- Thieves were allegedly able to take advantage of a vulnerability in electronic hotel door locks by exploiting the programming port to gain access to hotel rooms and steal items[10].
- High-end cars have been driven away by thieves without keys, in part by accessing a diagnostics port on the dashboard and using it to programme a blank key fob, which can then be used to open and start the car[11].

Manufacturers must consider the security of any components containing electronic systems, checking that any computer code within the product meets, and has been tested against, functional requirements and that it does not have any unintended security risks. Complex products are often made from assembled components, and if any of these contain computer code, it is vital to ensure that it does not contain any faulty or malicious functionality.

Security therefore needs to be part of the initial specification of electronic systems as well as the software development process. Product designers need to ensure that vulnerabilities are minimised, and that unauthorised users cannot breach the system. Nevertheless, sooner or later, vulnerabilities will be discovered, in which case designers need to ensure that their systems can be swiftly updated with authorised fixes.

Manufacturing compliance

Automated production lines are also exposed to new risks that require new methods of assurance. Stuxnet has shown that sophisticated attackers may compromise production systems potentially causing unpredictable effects.

Cyber attacks against machinery are an emerging issue: they are known to be possible and have occurred, however, there is very little information available regarding frequency. Equally, at the moment, it is not possible to accurately quantify what the consequences of an attack may be. Engineers responsible for evaluating cyber attacks against machinery must use their best judgement. Given the resources of attackers and the ease by which attacks can be launched, it would be prudent to consider that attacks are likely to occur at least once during the lifetime of machinery. Computer controlled machinery that may be subject to malicious input has safety implications that need to be considered as part of a safety assurance programme.

IEC 61508 is a standard commonly applied to assure the safe functioning of equipment. The consideration of safety, from the conception of the system through the entire life cycle, as well as striving to reduce risks to a level as low as practically possible, are very relevant to protecting against information security risks. Edition 2.0 of the standard specifies that security should be taken into consideration as part of hazard and risk analysis. The process of identifying mitigation strategies to protect against risks is the same for both security and safety.

IEC 62443 describes how organisations can implement cyber security management systems to create a regime appropriate for ICS. This standard also considers cyber security as a health and safety issue, describing how risks to safety can be evaluated alongside information security risk to prioritise which require addressing first.

The materials that enter the manufacturing chain also need assuring to the required standard. Traditionally, this has been the role of quality control. In the case where components contain computer code, ensuring that this code meets requirements and does not contain any faulty or malicious functionality is vital.

In many cases, manufacturers trust their suppliers to supply computer code that is fit for purpose. Where a higher degree of assurance is required, purchasers can source components that contain software that has been certified to have been produced to a formal security standard, such as ISO 15408, also known as the Common Criteria.

This standard allows organisations to define certain security properties for a target, how these properties have been evaluated and the depth of rigor of the evaluation. Although this does not ensure a product is completely secure, it does provide a framework from which companies can determine if products meet their particular security requirements.

Preparing in advance

As the move to agile manufacturing requires closer integration with other IT systems, the manufacturing system will be exposed to a new range of threats. In order to identify these threats and deploy suitable mitigation strategies, organisations need to develop a risk management strategy and process.

The plan should define who will be responsible for identifying threats and vulnerabilities, how such risks will be identified and prioritised, and how mitigation strategies will be evaluated. This strategy needs to be implemented as a process and continually evaluated.

Rather than attempting to create an ad-hoc process from scratch, adoption of standards such as ISO 27005 and NIST SP 800-30 provide frameworks that make the process of identifying and managing risk more likely to succeed.

Although cyber security threats tend to get the most press and attention, organisations need to prioritise common reasons for system failure and outages within their organisation. Integrated manufacturing systems are likely to be affected by outages in systems, such as financial or customer management, which are coupled to the manufacturing system; although this may not initially be realised.

Ensuring that regularly updated anti-virus software is installed on all systems, including servers, protects against the vast majority of threats due to malicious code.

Like any IT system, ICS may contain software vulnerabilities, so keeping the operating system and any software fully patched is important. However, a fully-patched system may still be at risk as not all vulnerabilities will have a patch available and some systems may only be certified to operate with a specified configuration and system version. Due to their high security requirements, ICS should be on a separate network with only the ports necessary for communicating with other systems open on the firewall.

Even the best preventative measures may allow an attacker to gain access to sensitive systems. In this case, it is vital to detect the attack as soon as possible, isolate affected systems and take remedial action. Intrusion detection systems and constant monitoring of logs and network traffic can alert administrators to suspicious activity on sensitive systems. Investigation of these warning signs can identify intrusions in progress, and again, immediate action can be taken to contain and remediate the attack.

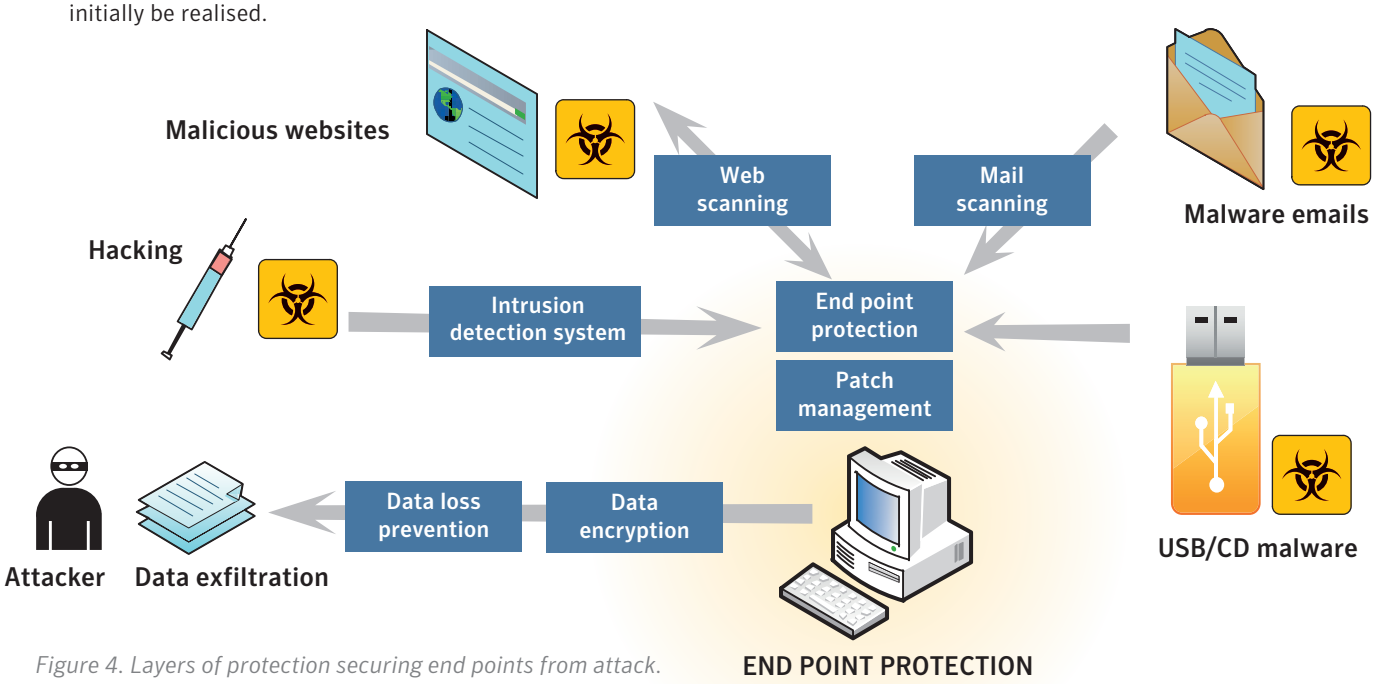

Figure 4. Layers of protection securing end points from attack.

Recommendations

Securing manufacturing systems involves considering security as an integral part of the manufacturing process. Each of the separate systems within the process requires an appropriate degree of security to avoid outages and to protect valuable intellectual property.

However, security isn't something that can be deployed out of a box and then neglected. Security is an ongoing process that is refined and improved according to changes in an organisation's operations as well as changes in the threat environment.

Implementing security measures need not be onerous, as existing compliance standards can offer a framework of best practice.

Manage risk

Adopting a robust risk management process, such as ISO 27005, which underpins a managed approach to information security as described in the ISO 27000 family of standards, should ensure that risks are correctly identified and managed, and can be seen as the first step in securing manufacturing systems.

As part of applying a risk management process, manufacturers should identify the particular security issues specific to their organisation. These risks are likely to include the availability of key systems, the confidentiality of intellectual property and the integrity and availability of ICS.

Protect data

Data assets that have high confidentiality requirements can be encrypted to ensure that only authorised users have access. Ensuring that users are correctly authenticated and that unauthorised users are kept locked out of systems is part of the same strategy. Securing the perimeter of networks to exclude unauthorised traffic and deploying anti-malware software on all systems will also help prevent attacks.

Companies should adopt a defence in depth strategy. Systems with high security requirements should be located on separate networks, which are closely monitored, so that incursions are swiftly identified and resolved before harm can be caused.

Data loss prevention systems should be considered to identify where high value data assets are held within the organisation and to block any activity, legitimate or otherwise, that may cause them to become compromised.

Organisations should ensure that regularly updated antivirus software is installed on all systems, including servers and follow best practices in the prevention of malware infection and the rapid detection and remediation of malware incursions.

Minimise outages

As outages will undoubtedly occur, it is important to take steps to improve system recovery time.

Deploying redundant systems, so that another component can take over if one fails, is one way of minimising outages, especially those due to hardware failure. Implementing regular system backups and ensuring that systems can be quickly restored to a stable state assists quick recovery from outages, especially when these are due to changes in software or operating system configuration.

Secure industrial control systems

Security of any ICS that interact with the physical world must be addressed within a health and safety framework, such as IEC 61508. Additionally, organisations should adopt the recommendations of standards relating to the computer security of ICS, such as NIST SP800-82, ISA-99 or IEC 62443. The implementation of these recommendations need not be burdensome on organisations as in many cases these recommendations are the best practices for any information security regime.

Safeguard product security

Product designers need to consider the security of their products and how this may be tested and assured. Adoption of a framework, such as that described in ISO 15026, allows manufacturers to make assertions supported by evidence regarding the security of their products. Alternatively the Common Criteria of ISO 15408 can be used by customers and manufacturers to specify security requirements and how these can be tested.

Conclusion

The manufacturing industry is evolving. The need for increased agility and flexibility is leading to automated manufacturing systems becoming integrated with enterprise IT systems. However, this close integration is exposing manufacturing systems to risks that need to be managed in order to ensure continued production as well as the integrity of the production process.

However, organisations should not despair. Securing systems against even the most sophisticated of attackers is not impossible but can be achieved through the application of diligence, good practice and the adoption of a risk management process.

The future world of integrated manufacturing systems offers many possibilities and the successful companies will be those that are able to seize the advantages while controlling the risks.

Relevant standards

Risk Management

ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management
ISO/IEC 27005 Information technology – Security techniques – Information security risk management
ISO/IEC 27035 Information technology – Security techniques – Information security incident management
NIST SP 800-30 Risk Management Guide for Information Technology Systems

Risk Enumeration

ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security
ISO/IEC TR 15026 Systems and software engineering – Systems and software assurance
IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems

System Integration

IEC 62264 Enterprise-control system integration
ISA-95 Enterprise-Control System Integration

Securing ICS

NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security
IEC 62443 Industrial communication networks – Network and system security
ISA-99 Industrial Automation and Control Systems Security

Further reading

Symantec 2012 State of Information Report
http://www.symantec.com/about/news/theme.jsp?themeid=state-of-information

Symantec Internet Security Threat Report, Volume 17
http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=threat_report_17

Symantec White Paper: Why Data Loss Prevention?
https://www4.symantec.com/Vrt/offer?a_id=78074

Symantec White Paper: Organizational Security and the Insider Threat: Malicious, Negligent and Well-Meaning Insiders
https://www4.symantec.com/Vrt/offer?a_id=108920

Symantec White Paper: Data Loss Prevention and Monitoring in the Workplace: Best Practice Guide for Europe
https://www4.symantec.com/Vrt/offer?a_id=153244

B Zhu, "A Taxonomy of Cyber Attacks on SCADA Systems", in proceedings of the Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, pp. 380-388 (2011)
http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6142258

References

1 M Davis, "Innovation Insight: Original Solution Orchestrators Extend Innovation in the Demand-Driven Supply Chain", Gartner. Gartner ID: G00233864 (2012)

2 JK Roehrich, G Parry, A Graves, "Implementing build-to-order strategies: enablers and barriers in the European automotive industry". International Journal of Automotive Technology and Management. 11(3), pp. 221-235 (2011).

3 J Miemczyk, M Howard, "Supply strategies for build-to-order: managing global auto operations", Supply Chain Management: An International Journal, 13(1), pp. 3 – 8 (2008).

4 BBC News, "Stuxnet hit Iran Nuclear Plants", 22nd Nov 2010. http://www.bbc.co.uk/news/technology-11809827

5 N Falliere, L O Murchu, E Chien, "W32.Stuxnet Dossier", Symantec White Paper. (2011)
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

6 D Albright, P Brannan, C Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment", Institute for Science and International Security Report 22nd December 2010.
http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf

7 ICS Alert, "Control System Internet Accessibility", ICS-ALERT-10-301-01, 28th October 2010.
https://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf

8 ICS Alert Update, "Increasing Threat to Industrial Control Systems", ICS-ALERT-12-046-01A, 25th October 2012.
http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-046-01A.pdf

9 G Richards, "Hackers vs slackers - [control security]", Engineering & Technology, 3(19), pp. 40 – 43 (2008).
http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4783239

10 A Greenberg, "Security Flaw In Common Keycard Locks Exploited In String Of Hotel Room Break-Ins", Forbes, 26th November 2012.
http://www.forbes.com/sites/andygreenberg/2012/11/26/security-flaw-in-common-keycard-locks-exploited-in-string-of-hotel-room-break-ins/

11 J Leyden, "Got a BMW? Thicko thieves can EASILY NICK IT with $30 box", The Register, 17th September 2012.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec is a global leader in providing security, storage and systems management solutions to help customers secure and manage their information and identities.