SMARTER SECURITY FOR MANUFACTURING IN THE **INDUSTRY 4.0** ERA

INDUSTRY 4.0 CYBER RESILIENCE FOR THE MANUFACTURING OF THE FUTURE

EXECUTIVE SUMMARY

Change is happening right across the manufacturing industry. The need for increased agility and flexibility has created Industry 4.0, or the Industrial Internet, where everything, from assembly line machine to delivery truck, is being connected with everything else, via the Internet. In this fourth industrial revolution, the fusion of physical and virtual worlds into global networks of cyber-physical systems is radically changing production control. While this brings benefits – in lower costs and higher efficiency – it also increases the risks. The complexity of managing production and supplier networks across the value chain grows enormously. It's a challenge that cyber criminals are exploiting.

Manufacturing is a highly lucrative target for their activities, ranging from cyber espionage, such as theft of intellectual property, to sabotage with worms grabbing control of industrial plants.

However, manufacturers need not despair. Securing IT systems and processes, smart technologies and interconnected supply chains against even the most sophisticated attackers is possible. Achieving cyber resilience involves diligence, good practice and risk management that's supported by the right security strategy and technologies. With these strategies in place, manufacturers can increase their success and competitiveness by taking advantage of all that Industry 4.0 offers, while controlling the risks.

TOWARDS INDUSTRY 4.0

The manufacturing industry is going through great changes. The fourth revolution, driven by the Internet of Things, is happening. It is creating intelligent networks – connecting machines, work and systems – that can autonomously exchange information, trigger actions and control each other independently.

In fact, it's estimated that 85% of companies will have implemented Industry 4.0 solutions in all important business divisions in five years time. By 2020 that will represent €140 billion spent annually in Europe[1].

In manufacturing, these cyber-physical systems cover smart machines, storage systems and production facilities – not just in one factory but across many.

Smart factories take a completely new approach to production – products can be identified, located and moved by alternative routes as needed. Manufacturing systems are connected with business processes as well as external networks, across the value chain, and managed in real-time.

These changes will impact the whole supply chain – from design, prototyping, ordering, industrial processing and sales, up to maintenance and service – with your business partners becoming more closely intertwined with your business.

It involves the integration of business systems that were once separate. Operational technology (OT) that once drove production processes is now merging with general Office IT. It also means that you are likely to have more suppliers to coordinate – often globally, with longer transport times and more manufacturing steps.

Flexible, lean manufacturing delivered by the industrial Internet is predicted to increase productivity and resource efficiency by 18% in the next five years and reduce inventories and costs by some 2.6% annually.

While the integration of systems that were once separate benefits manufacturers, it also carries risks- in particular to security. Processes that were once isolated are now vulnerable to cyber attack, both directly and indirectly.

THE ORIGINS OF INDUSTRY 4.0

The use of IT to computerize manufacturing is viewed as the fourth industrial revolution.

1.0 INDUSTRY 1.0
water and steam power used to mechanize production

2.0 INDUSTRY 2.0
electric power driving mass production

3.0 INDUSTRY 3.0
IT power to automate production

4.0 INDUSTRY 4.0
computerization of manufacturing and digital transformation

Originating in Germany, the term Industry 4.0 (Industrie 4.0) is more commonly known in some countries as the Industrial Internet. It is also referred to as the Integrated Internet, Smart Industry and Smart Manufacturing.

MANUFACTURERS UNDER THREAT

CYBER SABOTAGE[2] SHUTS DOWN THE BLAST FURNACE

A cyber attack on a German steel mill shows how office systems can be used to infiltrate plants and access control systems.

Attackers
Used a spear phishing campaign of emails and social engineering techniques to trick targeted individuals into opening messages that stole login credentials.

Aim
Access plant's office network and then production systems to sabotage equipment.

Impact
Forced the unscheduled and sudden shutdown of a blast furnace causing `massive damage', according to a BSI report.

MANUFACTURING THREAT LANDSCAPE

Together, the challenges of the Industrial Internet escalate the threat of damage from cyber attacks that manipulate processing and workflow systems. They can cause disruptions or longer outages, at enormous cost. As a recent Deloitte survey[3] shows, manufacturers believe that the potential for cyber risk will increase with the transformation to Industry 4.0.

Cyber risk [Scale 1-5]

Question: Do you think that the digital transformation to industry 4.0 could further increase cyber risk for manufacturing companies?

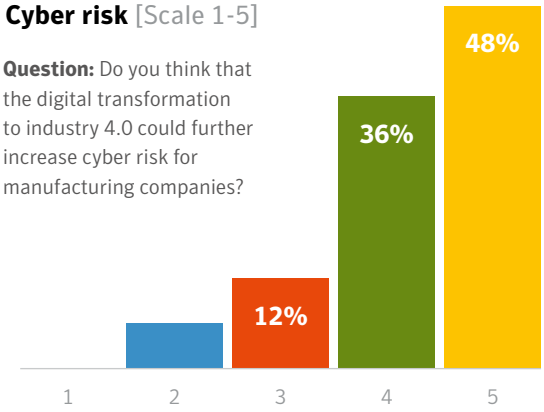

Figure 1: Increase in cyber risk expected
(Source Deloitte: Industry 4.0 Challenges and Solutions for the digital transformation and use of exponential technologies)

We're used to seeing targeted attacks on the manufacturing sector by hackers and cyber criminals. Attacks range from cyber-crime tactics, stealing confidential data and IP on new designs and products, to cyber sabotage of industrial processes or the IT data center.

In 2014, manufacturing was the top target for spear-phishing attacks, suffering 20% of all attacks, a significant increase from 13% the year before[4]. These targeted email attacks against individuals at manufacturing companies were part of cyber-crime tactics designed to steal access credentials to Office IT or OT systems.

According to the 2016 Symantec Internet Security Threat Report (ISTR issue 21), the manufacturing sector remained among the top 3 industries targeted by spear phishing attacks. With the increase in connectivity, the threat to manufacturing remains significant.

The Internet of Things means more devices than ever are being connected to the Industrial Internet. Gartner estimates that this year, 5.5 million new things will get connected every day, with a total of 6.4 billion connected things worldwide – 30% more than the year before.

The result is that Industrial Controls Systems (ICS) are a prime target. These systems are increasingly Internet enabled for easier monitoring and control. But moving to open systems with IP addresses creates more avenues for attack – especially if Internet access is poorly protected and ICS protocols for authentication are weak.

The U.S. Department of Homeland Security reported that cyber attacks on the manufacturing sector nearly doubled in one year[5]. This increase in security incidents comes at a great cost. Total financial losses attributed to security compromises jumped 38% over the year before, according to the PwC study 'The Global State of Information Security Survey 2015 – Industry'[6]. The convergence of Operational IT (OT) and traditional Office IT creates a new level of risk. A threat to Office IT is no longer isolated and can equally become a problem for Operational Technology systems.

The message is clear: to make the digital transformation to Industry 4.0 safely, manufacturing firms need to actively strengthen cyber risk management.

Zero-Day Vulnerabilities, Annual Total

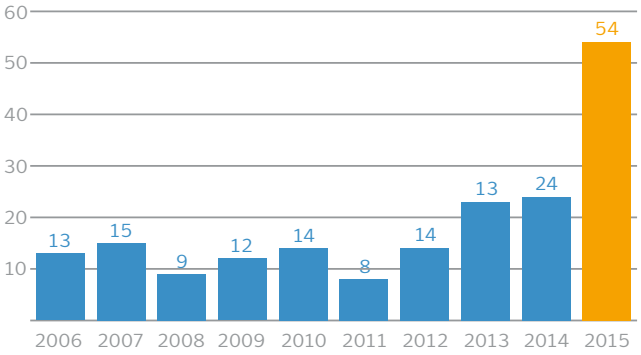

Figure 2: The highest number of zero-day vulnerabilities was disclosed in 2015 (Source: Symantec ISTR 21)

Vulnerabilities Disclosed in Industrial Control Systems

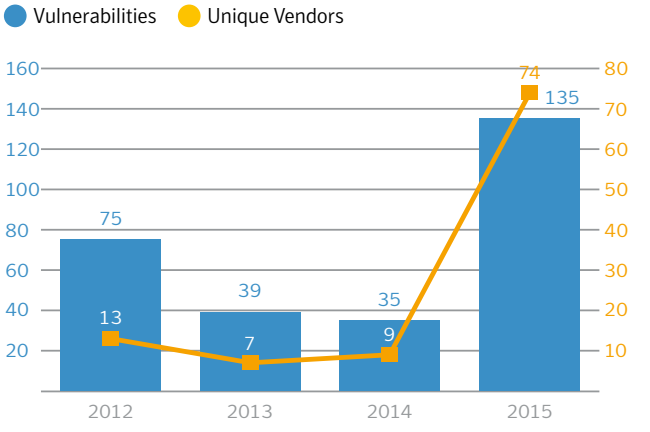

Figure 3: Vulnerabilities grew significantly in 2015 (Source: Symantec ISTR 21)

MANAGING CYBER RISK – RECOMMENDATIONS FOR MANUFACTURING FIRMS

Just as manufacturing firms spend time and resources on ensuring that machinery is properly maintained and serviced, so the same levels of care and attention must be paid to security.

Start with a risk management process

This involves:

1. **Prioritizing risks, defining policies and automating assessment processes (IT Governance, Risk and Compliance (IT GRC))** – that span all of your IT and OT/ICS environments.
2. **Enforcing IT policies and automate compliance (ISO 27005)** – with built-in automation and workflow to not only identify threats, but also remediate incidents as they occur or anticipate them before they happen.
3. **Communicating IT and OT risk in business-related terms** – using the IT GRC framework, which involves various steps from identifying critical assets through to continuous audit processes (see figure 4).

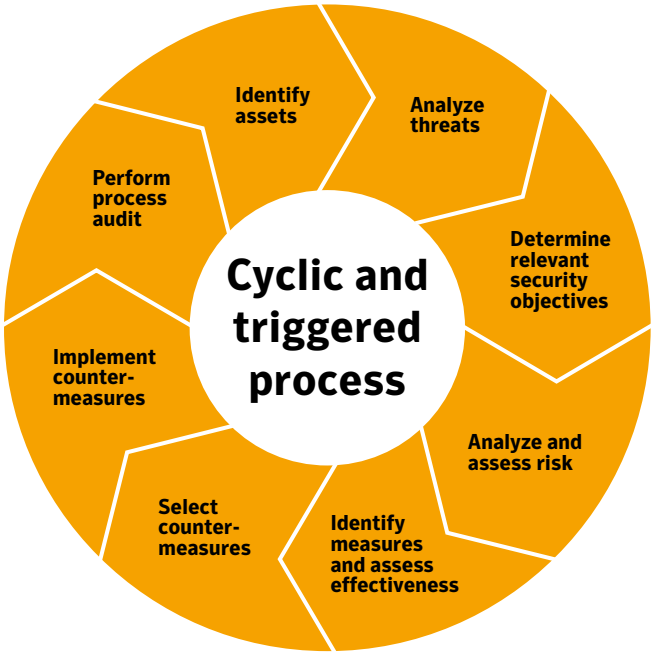

Figure 4: A cyclic GRC process as the foundation for ICS security (Source: IEC 62443)

Recommendations for setting your strategy to improve overall security and compliance

Best practice highlights the key steps needed to translate a risk management process into a fully-developed strategy for creating secure and compliant systems.

Manage the secure convergence of Office IT and OT

Fully realizing the benefits of Industry 4.0 in greater efficiencies and lower costs will involve integrating previously separate Office IT and OT systems. Standards like ISA 95 provide a framework for managing the flow of information between these systems.

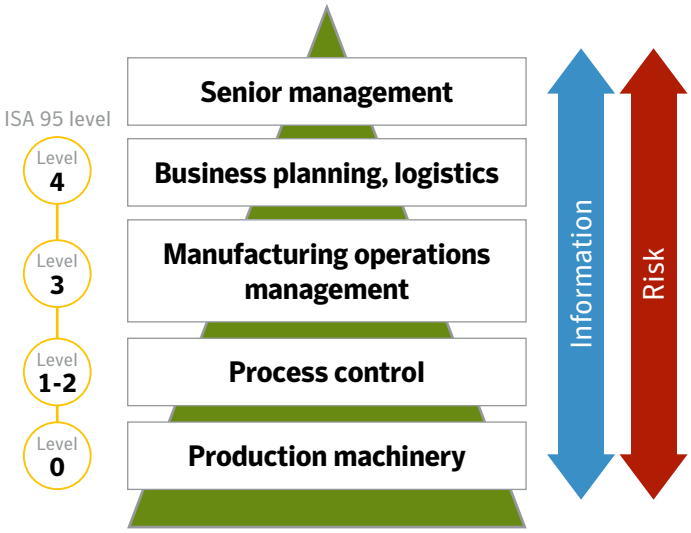

Figure 5: Flow of information and risk through an 'industrial internet connected' manufacturing organization

This flow of information provides the visibility across operations that allows senior management to speed decision-making and execution. However, the greater flow of information also widens the risks. When OT and IT systems are connected, there is the potential that threats, which may have been isolated to one system before, could pose a more severe risk to both.

Secure industrial control systems

Any industrial control system (ICS) that interacts with the physical world must be secure. Initially, that will mean an assessment to establish the potential hazard and risk, such as that outlined in the health and safety standard IEC 61508. Then, follow the recommendations for providing cyber security technologies and protection for improving control system security, set out in standards such as NIST SP800-82, ISA-99 or IEC 62443. These are essentially best practices for any information security regime.

Manage IOT devices and embedded systems

The move to the Industrial Internet will inevitably increase the number of smart devices you use in order to improve operational efficiency. Security in these embedded systems is about managing and protecting data, identity and services across the entire supply chain, to avoid these devices being compromised and opening up new threats.

Currently, there are few regulations in place. This increases the risk of cyber attacks. Many smart devices have a lifetime of 15 years or more, and are often not easy to access and replace. As many use non-standard hardware and proprietary firmware in embedded systems (such as sensors and pumps), standard computer security software can't be deployed. One way forward is to use device certificates and public key infrastructure (PKI) architectures. Implementing PKI into embedded systems secures the communication layer, creating a system that verifies the authenticity, configuration, and integrity of connected devices. This way, PKIs are ideal for large-scale security deployments that require a high level of security with minimal impact on performance.

Protect confidential information and intellectual property

Highly confidential data must be encrypted to ensure that only authorized users have access. Securing the perimeter of networks to exclude unauthorized traffic, deploying anti-malware, and hardening software on all IT and OT systems will also help prevent attacks. Data loss prevention solutions in conjunction with encryption should be considered to protect high value data assets. They also block any activity, that could potentially compromise your data.

Include business partners in the cyber risk program

As you share manufacturing data across supply chains, you need to assess the security strategies of business partners and contractors and close any gaps. Often, data sharing is through cloud-based applications or cloud storage. Yet, while 61% of businesses surveyed in a PwC study used some form of cloud computing, only 53% had a security strategy[7]. In fact, encryption, identity and context-based, access control across multiple cloud applications provide the best cornerstone for solving cloud security challenges.

Prepare in advance, detect and respond fast

Any risk management strategy and plan needs to define who will be responsible for identifying threats and vulnerabilities, how such risks will be prioritized, and how mitigation strategies will be evaluated. This process needs to be continually evaluated. The good news is it doesn't have to be done from scratch. 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.

It is impossible for manufacturers to be 100% secure from sophisticated attacks and data breaches. When the inevitable data breaches and illegal access to sensitive systems become evident that having a Response Plan becomes essential.

Even with the best preventative measures, attackers can 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, Advanced Threat Protection (ATP) and constant monitoring of logs and network traffic can alert administrators to suspicious activity. Investigating these warning signs can show intrusions in progress, allowing immediate action to be taken to contain and remediate the attack.

These measures should be part of the Incident Response plan you have ready. That plan should also consider:

- A proper crisis/PR management strategy to secure the reputation of the company
- Cyber insurance – to protect against financial loss that could otherwise cripple the company

SECURE YOUR PATH TO INDUSTRY 4.0 WITH SYMANTEC'S UNIFIED SECURITY STRATEGY

Comprehensive protection involves visibility across all systems – from attempted logins to every network connection – as well as intelligence on the latest exploits and attacks. Symantec's Unified Security Strategy offers that end-to-end view to help block, detect and remediate attacks, protect information and reduce risk.

- **Threat Protection** – stops attacks by securing all traditional and emerging endpoints, servers and network gateways
- **Information Protection** – integrated data and identity protection avoids loss of confidential information and only allows access from/to authenticated business partners
- **Cyber Security Services** – provide skills and resources to detect incidents and breaches faster than manufacturers could do by themselves

All these security solutions and services are backed by the **Unified Security Analytics Platform**, the largest civilian threat intelligence network for advanced security decisions of known and unknown threats. This powerful analytics platform is also ideal for protecting IoT devices in the production process by discovering suspicious anomalies in the network traffic so you can respond to them in a timely manner.

Symantec's Unified Security Strategy not only secures the manufacturing processes, it also builds comprehensive security into manufactured goods – such as connected, automated or even autonomous cars.

Cyber Security Services

Monitoring, Incident Response, Simulation, Adversary Threat Intelligence

Threat Protection

Endpoints **Datacenter** **Gateways**

- Advanced Threat Protection Across All Control Points
- Built-in Forensics and Remediation within Each Control Point
- Integrated Protection of Server Workloads: On-Premise, Virtual, and Cloud
- Cloud-Based Management for Endpoints, Datacenter, and Gateways

Information Protection

Data **Identities**

- Integrated Data and Identity Protection
- Cloud Security Broker for Cloud and Mobile Apps
- User and Behavioral Analytics
- Cloud-based Encryption and Key Management

Unified Security Analytics Platform

- Log and Telemetry Collection
- Integrated Threat and Behavioral Analysis
- Unified Incident Management and Customer Hub
- Inline Integrations for Closed-loop Actionable Intelligence
- Regional and Industry Benchmarking

SYMANTEC SOLUTIONS FOR PROTECTION ON YOUR WAY TO INDUSTRY 4.0

Threat Protection Information Protection Cyber Security Services

Data Center Security

Protects critical servers, hardens ICS control systems and provides compliance.

Works on systems that can't be patched easily or which run operating systems that are no longer supported (Windows NT, XP, 2003 Server and others).

Embedded Security – Critical System Protection

Lightweight security client for industrial IoT devices.

Used by many manufacturing suppliers to build security that has small footprint and uses minimal power resources into industrial control devices.

Validation and ID Protection Service (VIP)

Strong authentication that gives organizations secure access to networks.

Weak authentication is a huge vulnerability in most ICS systems, which is why authorized access to OT and Office IT systems, applications and data – on-premise and in the cloud – is a cornerstone of Symantec's security strategy.

Managed PKI Service

Provides trust-based security to authenticate IoT devices and ensure only trusted components communicate between each other in a production environment. Symantec already protects more than 1 Billion IoT devices and application entities enabling manufacturing companies to tighten integration with business partners.

Encryption (PGP)

Protects confidential information in manufacturing firms in use, in transit or at rest. Often deployed in cooperation with DLP.

Cyber Security Services (CSS)

Addresses the critical shortage of security expertise and extends security capabilities.

The Symantec ISTR report shows that smaller manufacturing companies or suppliers are increasingly being attacked and infiltrated with malicious code. They are easy victims for criminals due to their lack in security skills and processes. CSS provide additional insight and context across Managed Security Services (MSS), DeepSight™ Intelligence, Incident Response and Security Simulation as well as input for the right cyber insurance approach.

Control Compliance Suite

Manufacturing risk and security reporting to support IT Governance Risk and Compliance.

Enables auto-discovery of systems in Office IT and OT, automates security assessments of procedural and technical controls, collects and normalizes evidence data from third-party products, and calculates and aggregates risk scores.

Email and Web Security

Secures the gateway control points to Email and Web with on-premise or cloud services.

Endpoint Protection and Management

Secure, deploy and manage endpoints with standard operating systems.

Advanced Threat Protection (ATP)

New solution that uncovers, prioritises and remediates advanced attacks across many manufacturing control points.
The first product in the market that does this across the endpoint, network and email control points from a single console, without having to deploy any new agents.

Anomaly Detection for Industrial Control Systems

New solution which detects IoT devices and their network traffic.

By identifying IoT devices and analyzing their network traffic, the solution creates a detailed asset map. Using Deep Packet Inspection (DPI) it proactively identifies attacks against ICS networks and flags any suspicious activities.

Data Loss Prevention (DLP)

Discovers all types of confidential data with content-aware detection technologies and pre-defined templates for manufacturing companies

DLP detects data stored across endpoints, mobiles, storage systems, networks and even in the cloud – particularly important as IDC estimates that 50% of customer data will be in the public cloud by the end of 2016, compared to less than 5% in 2013.

Identity Access Manager (SAM)

Solves cloud security challenges.

Uses identity and context-based access control across multiple cloud and web based applications.

A GLOBAL FORCE TO DEVELOP YOUR CYBER RESILIENCE

Moving towards Industry 4.0 is a huge task. It impacts many areas in today's manufacturing industry – not just security. We understand that not all manufacturing companies have the skills and resources to independently deploy and run the new security and compliance processes that Industry 4.0 requires.

So Symantec leverages its strong relationships with leading global consultancy firms and system integrators. Together, we can help you develop the appropriate strategies and measures to route your organization to Industry 4.0, safely. While Symantec has the proven technical expertise, solutions and threat analysis in cyber security, our strategic partners can help with the business processes, providing project management, **risk and compliance assessments.**

Additionally, our partners can support in a range of areas:

Incident and breach response – IR plan development, public relations and crisis management, expert witness and litigation support.

Cyber Insurance – using threat and risk telemetry to recommend best suitable insurance products and policies to clients.

Outsourcing and Managed Services - Managed Data Loss Prevention, Compliance as a Service and others.

Innovative compliance solution rolled out in just three months

Symantec and our strategic alliance partners worked together to rapidly implement a compliance reporting service designed to meet complex compliance requirements for a large European manufacturer.

Completed in just twelve weeks, the innovative managed service covered more than 5,000 servers (UNIX and Windows) and 400 databases and middleware systems across Europe.

Cyber Security Services

Monitoring, Incident Response, Simulation, Adversary Threat Intelligence

Threat Protection

Endpoints

Data center

Gateways

Information Protection

Data

Identities

Unified Security Analytics Platform

Log and Telemetry Collection

Integrated Threat and Behavioral Analysis

Unified Incident Management and Customer Hub

Inline Integrations for Closed-loop Actionable Intelligence

Regional and Industry Benchmarking

Global Strategic Partner Ecosystem

Penetration Testing
Malicious Activity Assessment
Risk Assessment
Data Classification

DLP Assessment
Incident Response
Cyber Insurance
System Integration

Outsourcing/Hosting
Managed DLP
Compliance as a Service
Compliance Reporting Service

ABOUT SYMANTEC

Founded in 1982, Symantec has evolved to become the global leader in cyber security, with more than 11,000 employees in more than 35 countries. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

FURTHER READING

- Symantec ISTR Report 20: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf
- Symantec ISTR Report 21: https://www.symantec.com/security-center/threat-report
- Building Comprehensive Security into Cars – Symantec White Paper: http://www.symantec.com/content/en/us/enterprise/other_resources/building-security-into-cars-iot_en-us.pdf
- Insecurity in the Internet of Things (Symantec Blog): http://www.symantec.com/connect/blogs/iot-security-risks
- Symantec Industry website: https://www.symantec.com/solutions/industrial-control
- Symantec secures Rockwell Automation Industrial Control and Business Intelligence Solutions: https://www.symantec.com/content/dam/symantec/docs/other-resources/symantec-secures-rockwell-en.pdf

SOURCES

1. Deloitte: Industry 4.0 Challenges and Solutions for the digital transformation and use of exponential technologies
2. Annual report, German Federal Office for Information Security (BSI), December 2014
3. Symantec ISTR Report 20
4. Symantec ISTR Report 21
5. Symantec: The need for security in an evolving industry
6. Deloitte: Industry 4.0 Challenges and Solutions for the digital transformation and use of exponential technologies
7. Deloitte: Global Cyber Executive Briefing: Manufacturing
8. US sees jump in cyber attacks on critical manufacturing infrastructures, report by Jim Finkle
9. PwC: Addressing security risks in an interconnected world – Industrial segment; Key findings from 'The Global State of Information Security Survey 2015'
10. Strategy and PWC: Industry 4.0 & Opportunities and Challenges of the Industrial Internet, 2014

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
- VDI (Verein Deutscher Ingenieure) VDE 2182

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