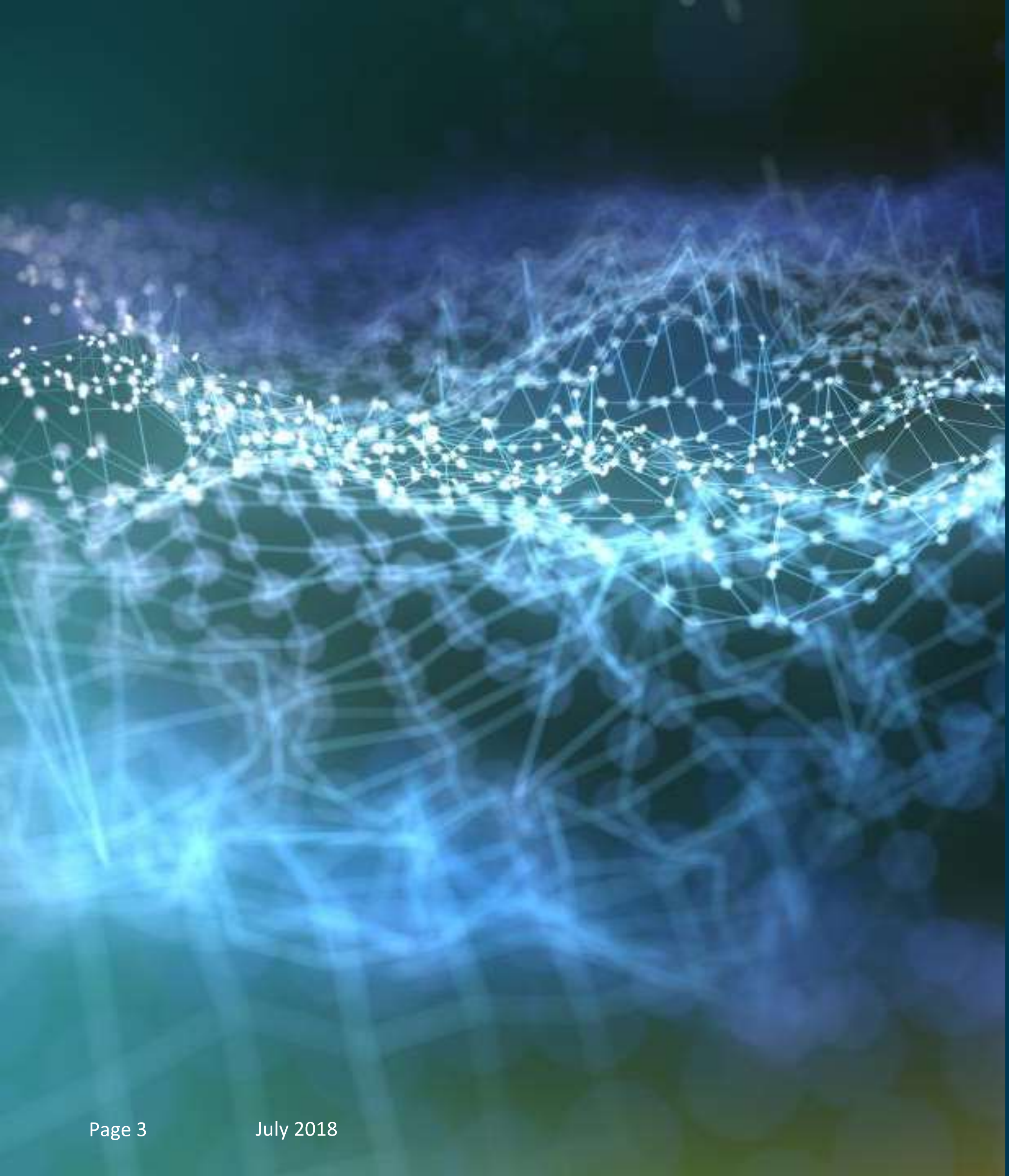
Charter
of Trust

Addressing cyber risks actively with Siemens solutions

Digitalization changes everything

Artificial intelligence and big data analytics are revolutionizing the way we make decisions. And billions of devices are being connected by the Internet of Things and are interacting on an entirely new level and scale.

Charter of Trust



A critical factor for the success of the digital economy

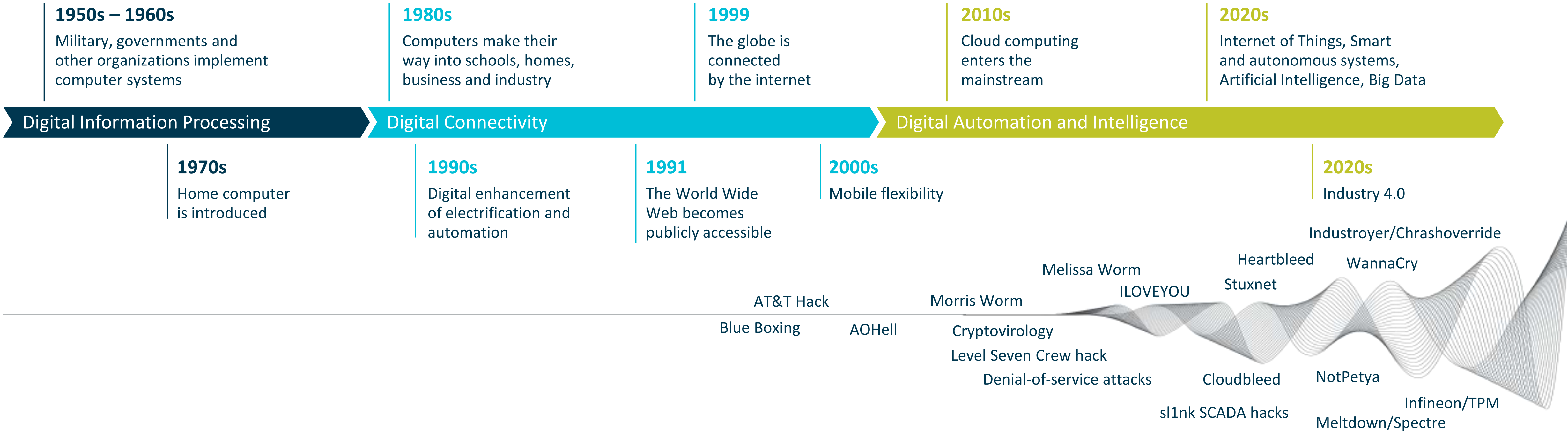
As much as these advances are improving our lives and economies, the risk of exposure to malicious cyber attacks is also growing dramatically.

- Crucial to the success of the digital economy
- Users need to trust that their digital technologies are safe and secure
- Digitalization and cybersecurity must evolve hand in hand

Charter of Trust

Cybersecurity

An increasingly critical factor for the success of the digital economy



1950s – 1960s
Military, governments and other organizations implement computer systems

1970s
Home computer is introduced

1980s
Computers make their way into schools, homes, business and industry

1990s
Digital enhancement of electrification and automation

1991
The World Wide Web becomes publicly accessible

1999
The globe is connected by the internet

2000s
Mobile flexibility

2010s
Cloud computing enters the mainstream

2020s
Internet of Things, Smart and autonomous systems, Artificial Intelligence, Big Data

2020s
Industry 4.0

Digital Information Processing

Digital Connectivity

Digital Automation and Intelligence

Blue Boxing
AT&T Hack
AOHell
Morris Worm
Cryptovirology
Level Seven Crew hack
Denial-of-service attacks
Melissa Worm
ILOVEYOU
sl1nk SCADA hacks
Stuxnet
Cloudbleed
Heartbleed
WannaCry
NotPetya
Industroyer/Chrashoverride
Infineon/TPM
Meltdown/Spectre

Charter of Trust

> “We can’t expect people to actively support the digital transformation if the security of data and networked systems is not guaranteed.”

That’s why Siemens will be working with partners from industry, government and society to sign a “Charter of Trust” – a charter aimed at three important objectives:

1. Protecting the data of individuals and companies
2. Preventing damage to people, companies and infrastructures
3. Establishing a reliable foundation on which confidence in a networked, digital world can take root and grow

Charter of Trust

Cybersecurity is going to be the most important security issue of the future

For both societies and companies
all over the world.

The digital transformation

will only succeed if we can rely on the security of data and connected systems. Digitalization and cybersecurity are two sides of the same coin.

That’s why we’re joining forces and working together on equal footing

in industry, government and society to promote a Charter of Trust that’s intended to make our digital world more secure.

The Charter focuses on three goals:

Protecting the data of individuals and companies; preventing harm to people, companies and infrastructures; and establishing a reliable foundation on which confidence in a networked digital world can take root and grow.

As pioneers in digitalization,

we are well aware of our responsibilities. With our partners in government, industry and society, we are taking a stand in favor of binding rules and standards that will create a new basis of trust and equality of competition.

Cybersecurity

A critical factor for the success of the digital economy

Charter
of Trust

For a secure digital world

Key principles

01 Ownership of cyber and IT security
02 Responsibility throughout the digital supply chain
03 Security by default
04 User-centricity
05 Innovation and co-creation
06 Education
07 Certification for critical infrastructure and solutions
08 Transparency and response
09 Regulatory framework
10 Joint initiatives

Charter
of Trust

A critical factor for the success of the digital economy

Key Principles

Charter of Trust for a secure digital world

charter-of-trust.com

01 Ownership of cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – "it is everyone's task".

02 Responsibility throughout the digital supply chain

Companies – and if necessary – governments must establish risk-based rules that ensure adequate protections across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity and availability by setting baseline standards such as

- **Identity and access management:** Connected devices must have secure identities and safe-guarding measures that only grant access to authorized users and devices
- **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate
- **Continuous protection:** Companies must offer updates, upgrades and patches throughout a reasonable lifecycle for their products, systems and services via a secure update mechanism

03 Security by default

Adopt the highest appropriate level of security and data protection and ensure that it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures and business models

04 User-centricity

Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems and services as well as guidance based on the customer's cybersecurity needs, impacts and risks

05 Innovation and co-creation

Combine domain know-how and deepen a joint under-standing between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage contractual Public Private Partnerships, among other things

06 Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education and trainings – in order to lead the transformation of skills and job profiles needed for the future

07 Certification for critical infrastructure and solutions

Companies and – if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions

08 Transparency and response

Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice, which focuses on critical infrastructure

09 Regulatory framework

Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs)

10 Joint initiatives

Drive joint initiatives including all relevant stakeholders in order to implement the above principles in the various parts of the digital world without undue delay

Charter of Trust

Charter
of Trust

The Charter of Trust

The principles

Principle 1

01 Ownership of cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – “it is everyone’s task”.

What does that mean and why is it so important?

People, organizations and entire societies must rely on digital technologies and will support this transformation only if the security of their data and networked systems can be ensured. It requires clear responsibilities at the highest levels – in companies as well as governments.

Concrete implementation steps

Siemens example

In January 2018 we established a new cybersecurity unit headed by Natalia Oropeza, our new Chief Cybersecurity Officer (CCSO). In this function, she reports directly to the Managing Board of Siemens AG. With this new position we’re fulfilling one of our requirements in the Charter of Trust.

“Cybersecurity is more than a challenge. It’s a huge opportunity. By setting standards with a dedicated and global team to make the digital world more secure, we are investing in the world's most valuable resource: TRUST.

Our concrete answers to today’s upcoming cybersecurity issues and our proposals for more advanced cybersecurity rules and standards are invaluable to our partners, stakeholders and societies around the world. That is what we call “ingenuity at work.”

Natalia Oropeza,

Chief Cybersecurity Officer, Siemens AG

Principle 2

02 Responsibility throughout the digital supply chain

Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity and availability by setting baseline standards such as:

Identity and access management

Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them

Encryption

Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate

Continuous protection

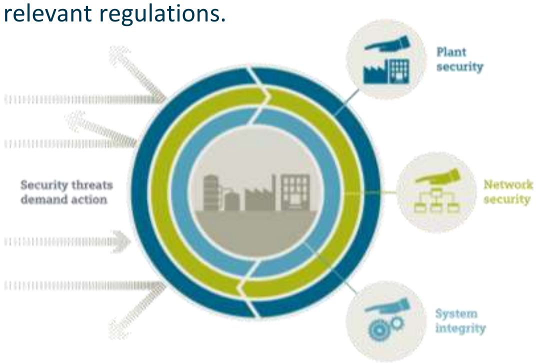
Companies must offer updates, upgrades and patches throughout a reasonable lifecycle for their products, systems and services via a secure update mechanism

Concrete implementation steps

Siemens example

To protect power plants from internal and external cyber attacks, all levels must be protected simultaneously – from the plant management level to the field level and from access control to copy protection.

With defense in-depth, Siemens provides a multi-layer concept that gives plants both all-round and in-depth protection. The concept is based on plant security, network security and system integrity as recommended by ISA 99/IEC 62443 and relevant regulations.



Responsibility throughout the supply chain – Why is it so important? A view from the industry perspective

Automotive

- Ensured plant availability
- Segmented and monitored communication
- Ensured remote communication
- Real-time communication based on cell-protection concept

Food and beverage

- Ensured traceability throughout the entire production process
- Ensured plant availability
- Segmented and monitored communication
- Compliance with critical infrastructure regulations

Glass and solar

- Ensured plant availability
- Highly sophisticated malware detection
- Ensured remote access
- Real-time communication based on cell protection concept

And more …

- Increased plant availability
- Ensured remote access
- Ensured user access
- …

Chemical

- Increased plant availability
- Ensured user access
- Segmented and monitored communication

Pharma

- Ensured traceability throughout the entire production process
- Ensured user access
- Ensured plant communication

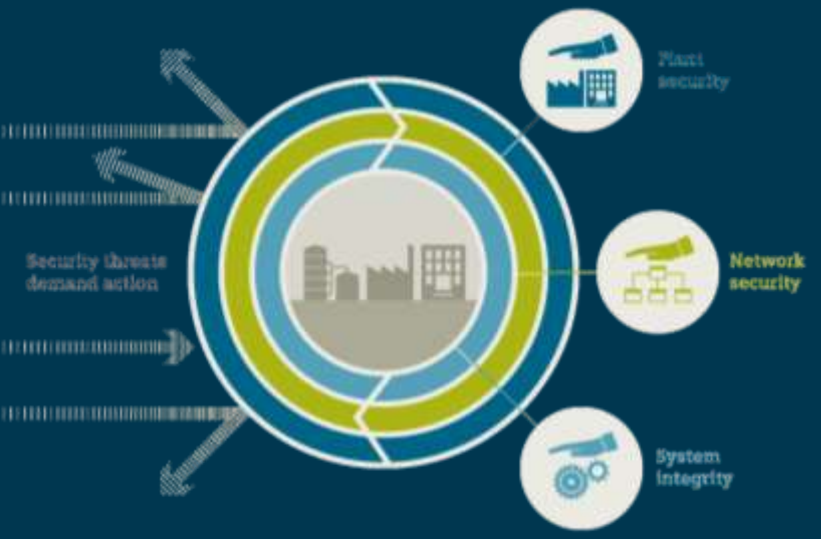
Water/wastewater

- Increased plant availability
- Ensured remote access
- Ensured user access
- Critical infrastructure regulations met

Charter of Trust

Responsibility throughout the digital supply chain

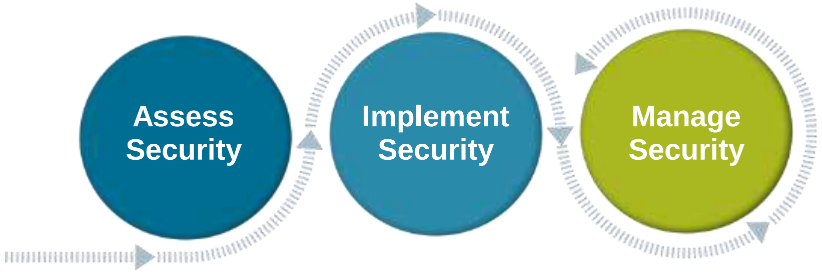
The Siemens security concept
defense in-depth



Siemens products and systems offer integrated security

- Know-how and copy protection
- Authentication and user management
- Firewall and VPN (Virtual Private Network)
- System hardening and continuous monitoring

Siemens Omnivise Cyber Security Risk Management



Principle 3

03 Security by default

Adopt the highest appropriate level of security and data protection and ensure that it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures and business models.

What does that mean and why is it so important?

Only if security requirements are already taken into account in the early phase of a product, especially in its design phase, can the highest appropriate level of security be offered proactively.

The same applies to all the other steps in the value chain – from the functionalities and the default security configuration settings of a product, to the manufacturing processes, technologies used and the operational processes. This also includes the underlying architectures and business models.

Concrete implementation steps

Siemens example

The Siemens Elektronikwerk Amberg is a prime example of a digital factory. The factory uses cutting-edge technologies to produce approximately 15 million SIMATIC products each year. Early on in the lifecycle, each SIMATIC product is analyzed for their functionalities as well as the necessary security measures to be integrated into their designs. A holistic security concept is applied throughout the lifecycle, from design and development, to the production and maintenance of the product.

> “Considering our extensive network, which multiplies the number of possible points of entry to our IT infrastructure, we cannot assume that yesterday’s solutions will protect against today’s potential threats.
>
> Since introducing SIEM, we have much higher transparency about the effectiveness of our measures to protect against cyberattacks.”

Gunter Beitinger,

Chief Executive Officer (CEO), Siemens Elektronikwerk Amberg

Principle 4

04 User-centricity

Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems and services as well as guidance based on the customer's cybersecurity needs, impacts and risks.

What does that mean and why is it so important?

Companies are exposed to the same risks as any other user of IT and the internet. In addition, companies are the targets of additional type of attacks that do not occur in the private environment. That's why companies need products, systems and services that meet their security needs – over an appropriate lifecycle.

Concrete implementation steps

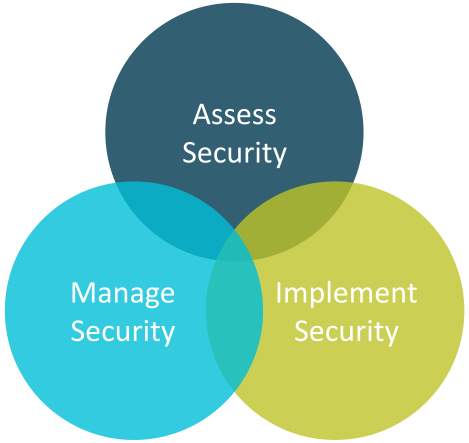
Siemens example

With Siemens Omnivise Cyber Security Services, energy companies benefit from the comprehensive know-how as well as the technical expertise of a global network of specialists for automation and cybersecurity.

The holistic approach of the industry-specific concept is based on state-of-the-art technologies as well as the applicable security rules and standards.

Siemens proactively offers security solutions along the industrial lifecycle. Threats and malware are detected at an early stage, vulnerabilities analyzed in detail and appropriate comprehensive security measures are initiated.

Continuous monitoring gives power plant operators the greatest possible transparency regarding the security of their facility and optimal investment protection at all times.

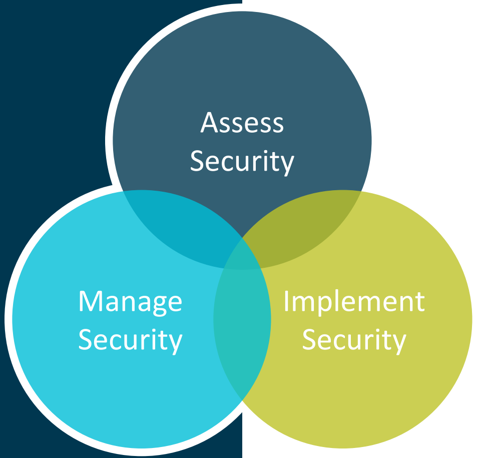


Charter of Trust

User-centricity

Siemens Omnivise Cyber Security Services

A triple dose of more security



Evaluation of current security status

- Analysis of threats and vulnerabilities to identify, evaluate and classify risks
- Assessment of business impact
- Execution from process engineering and automation view
- Basis for the establishment of a security program

Risk mitigation through implementation of security measures

- Design and implement technical security measures
- Develop and deploy security-relevant processes
- Enhance security awareness thanks to specific trainings

Comprehensive security through monitoring and proactive protection

- Close security gaps with continuous updates and backups
- Identify and handle security incidents thanks to continuous security monitoring
- Early adaptation to changing threat scenarios

Charter of Trust

Siemens offers cyber security packages tailored to understand and address the problem

Assess and Plan

Assessments

- Cyber Gap Assessment
- Vulnerability Assessment
- Baseline Compliance Assessment

Security Processes

- Incident Response Plan preparation & testing
- Disaster Recovery Plan preparation & testing

Protect

SPPA-T3000 Security Controls

- Secure Architecture
- Device Hardening
- Malware Pattern Updates
- Application Whitelisting

Additional Controls

- Secure Remote Access
- Data Diode
- OT Security Training

Detect and Respond ✓

Asset Management

- Asset Inventory and Change Monitoring

Multi-vendor

Powered by PAS

Vulnerability & Patch Management

- SPPA-T3000 Patch Management
- Advanced Vulnerability Management

Multi-vendor

Powered by tenable network security

Monitoring

- SPPA-T3000 Security Event Monitoring
- SPPA-T3000 Change Monitoring

Detection

- SPPA-T3000 Network Intrusion Detection System
- Network Anomaly Detection

Multi-vendor

Powered by DARKTRACE

Charter of Trust

Principle 5

05 Innovation and co-creation

Combine domain know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cyber-security measures to new threats; drive and encourage contractual Public Private Partnerships, among other things.

What does that mean and why is it so important?

Only if we intensify the cooperation between companies and policymakers and create a common understanding of cyber threats will we succeed in the long run.

That's why we need to build this partnership and increase our shared knowledge across industries, universities and R&D institutions.

Concrete implementation steps

Siemens example

Siemens has been taking a stand in cybersecurity for 30 years – through leading technologies, proven know-how and services as well as educational efforts. Currently, our company has about 1275 cybersecurity experts worldwide, which includes about 25 whitehead hackers who continuously challenge the security of both internal IT systems and products being shipped to customers.
The ability to supply customers with secure products and systems is a competitive advantage within a growing business field. The unique combination of technical know-how in Cybersecurity and the very deep domain know-how puts Siemens in an ideal position to be both a market and thought leader.
In our Core Technology Field (CCT), Cybersecurity experts from our Business Units and our central research and development unit – Corporate Technology – are working on new technologies for safeguarding critical infrastructure, protecting sensitive information and assuring business continuity.

Charter of Trust

Innovation and co-creation in our CCT Cybersecurity

Security Components, e.g.

- One-way gateway
- IoT public key infrastructure, identity and access management
- Small footprint IoT cryptography

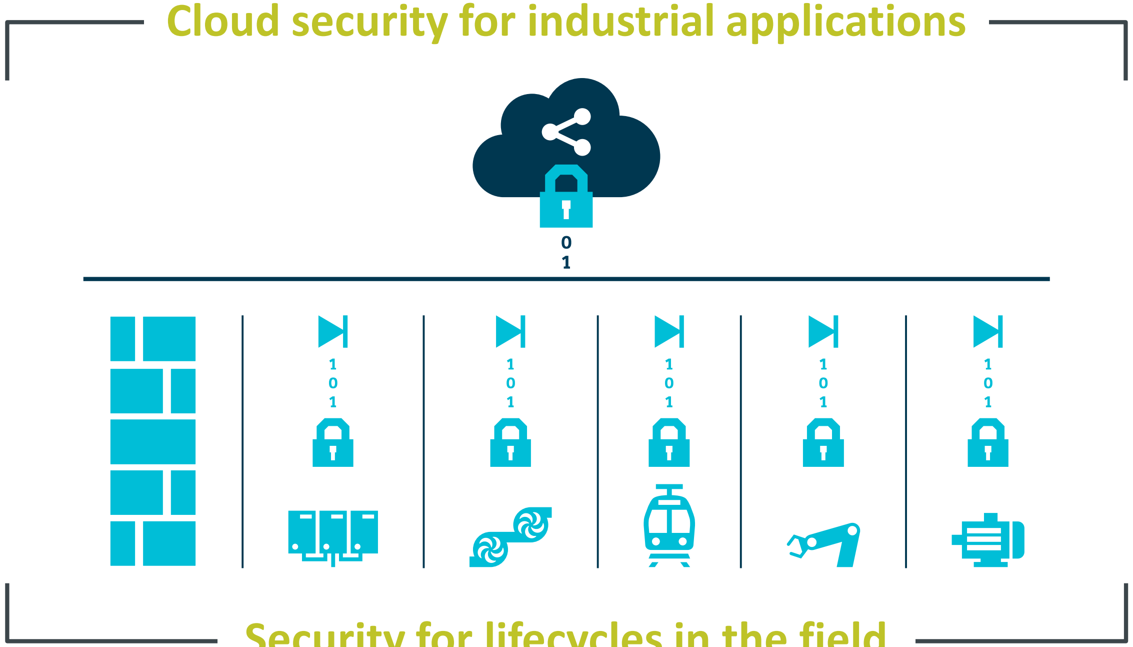
Security automation in R&D, e.g.

- Automated penetration testing
- Automated hardening and secure configuration

Technologies for security services in operations, e.g.

- Security analytics platform
- Artificial intelligence for security
- Automatic response, malware containment

Cloud security for industrial applications



Security for lifecycles in the field

Principle 6

06 Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education and trainings – in order to lead the transformation of skills and job profiles needed for the future.

What does that mean and why is it so important?

A significant number of cybersecurity incidents are attributed to human error or negligence. Raising everyone's awareness of cyber risks and protection measures is the first line of defense.

To continue developing IT security at the technological level, people need to be able to acquire the skills and qualifications that are needed for the digital transformation. Only in this way can people adapt to the new job profiles.

That's why corresponding supportive programs for schools, universities and companies should be continued and expanded.

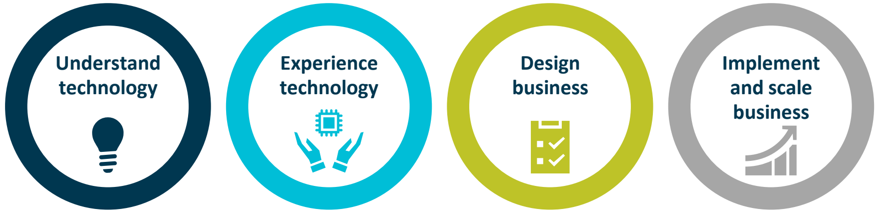
Concrete implementation steps

Siemens example

By carrying out regular cybersecurity awareness training sessions worldwide, Siemens ensures all employees have a high level of security awareness. We invest in building dedicated security expertise for products, solutions and services with a role-specific curriculum.

InfoSec Cards, for example, give practical hints categorized in different topics to support our employees in implementing Siemens-specific InfoSec rules and regulations. With annually renewed Trend Cards, we provide an overview of the most important current technical and non-technical trends in the broader field of cybersecurity that may possibly influence the Siemens portfolio.

And our "Applying Digitalization to your Business" training session, featuring cybersecurity as key element, has been rolled out throughout the company and consists of four important pillars:



Applying digitalization to our business

A hands-on training to accompany digital transformation

Principle 7

07 Certification for critical infrastructure and solutions

Companies and – if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions.

What does that mean and why is it so important?

Critical infrastructure and critical IoT solutions (e.g. autonomous cars, collaborative robots) will be increasingly exposed to cybersecurity threats. Independent certifications for security-relevant processes or security-relevant technical solutions can help to reduce the risk of cybersecurity incidents, where harm for life and limb of people are at risk.
It's up to companies – and governments, if necessary.

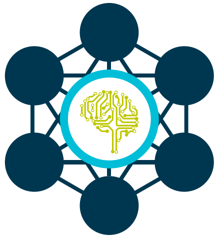
Concrete implementation steps

Siemens example

The biggest challenge facing cybersecurity standards is holistic, system-oriented approaches. Many existing standards focus on the level of the individual product or system. What is missing are standards for overarching topics such as Smart Cities, which then continue in concrete specifications for sub-areas such as mobility, energy and water supply.

One of the key platforms for building consensus on standards for requirements and procedures for assessing compliance is the IEC (International Electrotechnical Commission). It has already established more than 100 cybersecurity standards. Siemens was involved in around 90 percent of this. The overarching strategy of standardization work in the area of cybersecurity is being driven by Siemens within the IEC. In addition, Siemens is represented in many individual committees. The same applies to the committees at the IEEE, IEFF and ISO.

An example of the success of a holistic standard is IEC 62443. It defines basic standards for "Security by Design," holistically addressing operators as well as products and services included in IoT solutions. IEC 62443 is universally applicable, "from the high-speed locomotive to the light switch." It sets the standards that engineers should consider as early on as the design stage.



Principle 8

08 Transparency and response

Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today’s practice, which focusses on critical infrastructure.

What does that mean and why is it so important?

The digital world is all about one thing: Speed. When cyber attacks occur, you need an immediate, coordinated and goal-oriented response. That's why it's so important for companies to team up and work together to create an industrial cybersecurity network to instantly share new insights and information about attacks and incidents.

Concrete implementation steps

Siemens example

Siemens is a member of FIRST, the umbrella organization for all CERTS (Cyber Emergency Response Teams). We also have a very good relationship with national CERTs (such as US-CERT, CERT-EU and ICS-CERT) and law enforcement agencies (such as the FBI, BKA and Europol). And we gather Cyber Threat Intelligence and share them within these partners. We’ve formed partnerships for developing industrial IT and standards and collaborations with universities, business partners, customers, startups and respected research institutes for cybersecurity innovations. And with our own Cyber Defense Teams, we are waging a determined battle against approx. 1,000 cyber attacks every month.

> We have effective strategies that help us handle the large number of attacks, because we can incorporate our findings from defense activities directly into new technologies.

Thomas Schreck

Head of the Cyber Emergency Response Team at Siemens AG

Charter of Trust

Principle 9

09 Regulatory framework

Promote multilateral collaborations in regulation and standardi-zation to create a level playing field that matches the global reach of WTO; inclusion of rules for cybersecurity in Free Trade Agreements (FTAs).

What does that mean and why is it so important?

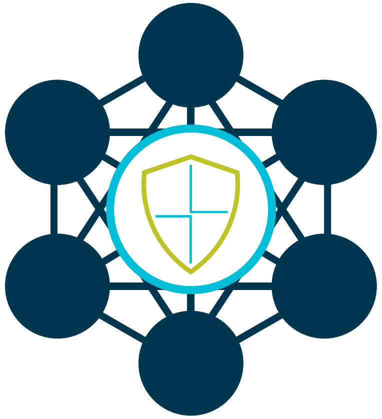
Regulation and standardization are only successful if they are based on multilateral cooperation. We therefore wish to expand these further in order to create a level playing field for all involved. The World Trade Organization, with its global reach, is our role model.
Cybersecurity is so important that it should also be included as an integral part of Free Trade Agreements.

Concrete implementation steps

Siemens example

Siemens welcomes all international networking on topics at every relevant level. We actively participate in a comprehensive cybersecurity network (relevant criminal prosecutors, ISA, FIRST, CERT Community, Software Assurance Forum for Excellence in Code (SAFECode)). We gather threat information and disseminate it through these partnerships.

Our Government Affairs activities, which include the initiative to create a Charter of Trust, are committed to helping bring cybersecurity to the agenda and translating it into concrete regulations and standards.



Principle 10

10 Joint initiatives

Drive joint initiatives including all relevant stakeholders in order to implement the aforementioned principles in the various parts of the digital world without undue delay.

What does that mean and why is it so important?

Only when we become active together will we achieve our goals. The Charter of Trust is therefore an important nucleus for further joint initiatives to promptly implement the 10 principles in the various areas of the digital world.

Concrete implementation steps

Siemens example

On February 16 at the MSC, we laid the cornerstone for the joint “Charter of Trust” initiative with partners – aspiring and desiring to recruit more comrades in arms for our initiative worldwide and to create a digital world that is based on trust in the digital and hyper-connected world. One that’s independent of competitors and regions. Trust must not stop at geographical or industry borders. And this can only be a starting point. This is not a challenge that can be solved by this group or any individual company alone. That’s why we invite companies sharing our ambition and ownership for trust to join the Charter of Trust initiative. We also invite governments of the world and civil society to engage in a focused dialogue: Trust matters to everyone. It’s everyone’s task.

Charter of Trust
We Sign for Cybersecurity
Charter of Trust for a Secure Digital World | Signing Event on February 16 2018
Munich Security Conference
Münchner Sicherheitskonferenz
msc
IBM
NXP
SIEMENS

Charter
of Trust

We sign for cybersecurity!

Charter of Trust

We sign for cybersecurity! We sign the Charter of Trust.

SIEMENS AES AIRBUS Allianz Atos cisco DAIMLER DELLTechnologies

enel IBM Munich Security Conference Münchner Sicherheitskonferenz msc NXP SGS T · · TOTAL TÜV SÜD

Backup

Strong cyber programs focus on developing three key areas

Assess and Plan

- What do I need to protect?
- What are my threats?
- Here are my vulnerabilities and weaknesses?
- How do I create a cyber roadmap?

Protect

- What protection do I put in place (at every level)?
- What cyber capabilities do I need to have?
- How do I test my cyber protections?

Detect

- How do I know I have been breeched?
- How do I know when new vulnerabilities are announced?

Respond

- How do I best respond to an attack?
- How to quickly recover from a disaster?
- How do I make sure it doesn’t happen again?

Charter
of Trust

Vulnerability Management Overview

Receive single view of vulnerabilities across your OT network, regardless of vendor. Focus your patch management process on closing priority vulnerabilities. Access experts to help you manage critical issues

Solution

Siemens service utilizing Tenable's Industrial Cyber Software

Installed and configuration by Siemens Experts

Training for your team by Siemens to use and interpret the software

Monthly reports and weekly alerts to augment your internal team

Access to our experts on-demand via our hotline

What Tenable's Industrial Cyber Technology does

- OT-native solution based on Nessus Network Monitor
- Provides companies safe and continuous visibility into their production networks to reduce cyber exposure
- Automatically collects known vulnerabilities from a variety of external sources
- Passively scans your systems to see which vulnerabilities exist and if they are being exploited
- Prioritizes vulnerabilities based on threat intelligence

tenable network security

Benefits:

1. Enables resource constrained organizations to **focus only on most critical alerts**, backed by Siemens expertise
2. **Vulnerability intelligence** backed by analysis to enable **rapid prioritization and remediation**
3. Greater understanding of the **operational implications** of cyber risk and how to address them

Asset Monitoring Overview

Receive single view of vulnerabilities across your OT network, regardless of vendor. Focus your patch management process on closing priority vulnerabilities. Access experts to help you manage critical issues.

Solution

Siemens service utilizing PAS's Cyber Integrity

Installed and configuration by Siemens Experts

Training for your team by Siemens to use and interpret the software

Monthly reports and weekly alerts to augment your internal team

Access to our experts on-demand via our hotline

What PAS' Cyber Integrity Technology does

- Automates inventory and cyber asset configurations
- Establishes a security baseline and monitors configuration data changes
- Drives incident responses to unauthorized changes or security events
- Enforces compliance standards including NERC CIP, IEC 62443, and NIST 800-82

Benefits:

1. **Automated asset discovery** with unparalleled vendor and protocol coverage in ICS environments
2. Siemens delivers security team training, dashboard creation and other forms of support to **empower in-house teams** to strengthen their OT cyber posture
3. **Automated configuration management** identifies configuration changes

Network Monitoring Overview

Monitor OT networks for anomalous activity. Focus on identifying and alerting unusual behavior.
Access experts to help you manage critical issues and understand technology results

What you get

Siemens service utilizing Darktrace's Industrial Immune System

Installed and configuration by Siemens Experts

Training for your team by Siemens to use and interpret the software

Monthly reports and weekly alerts to augment your internal team

Access to our experts on-demand

via our hotline

What Darktrace's Industrial Immune System tech. does

- Implements a real-time "immune system" for operational technologies to identify anomalous network activity
- Utilizes machine learning algorithms to baseline network traffic
- Provides real-time visibility to live situations, while enabling in-depth investigations into historical activity
- Passively ingests data as to not disturb operations

DARKTRACE

Benefits:

1. Siemens undertakes investigations to **provide clear operational context and insights that help manage and prioritize alerts**
2. Enables resource constrained organizations to **focus only on most critical alerts**, backed by Siemens expertise
3. Offers unmatched insights into OT: empowers organizations to **make smarter, faster security decisions**