SIEMENS
Ingenuity for life

Cyber Security as THE Key Enabler for Digitalization

Dr. Norbert Gaus | July 2018

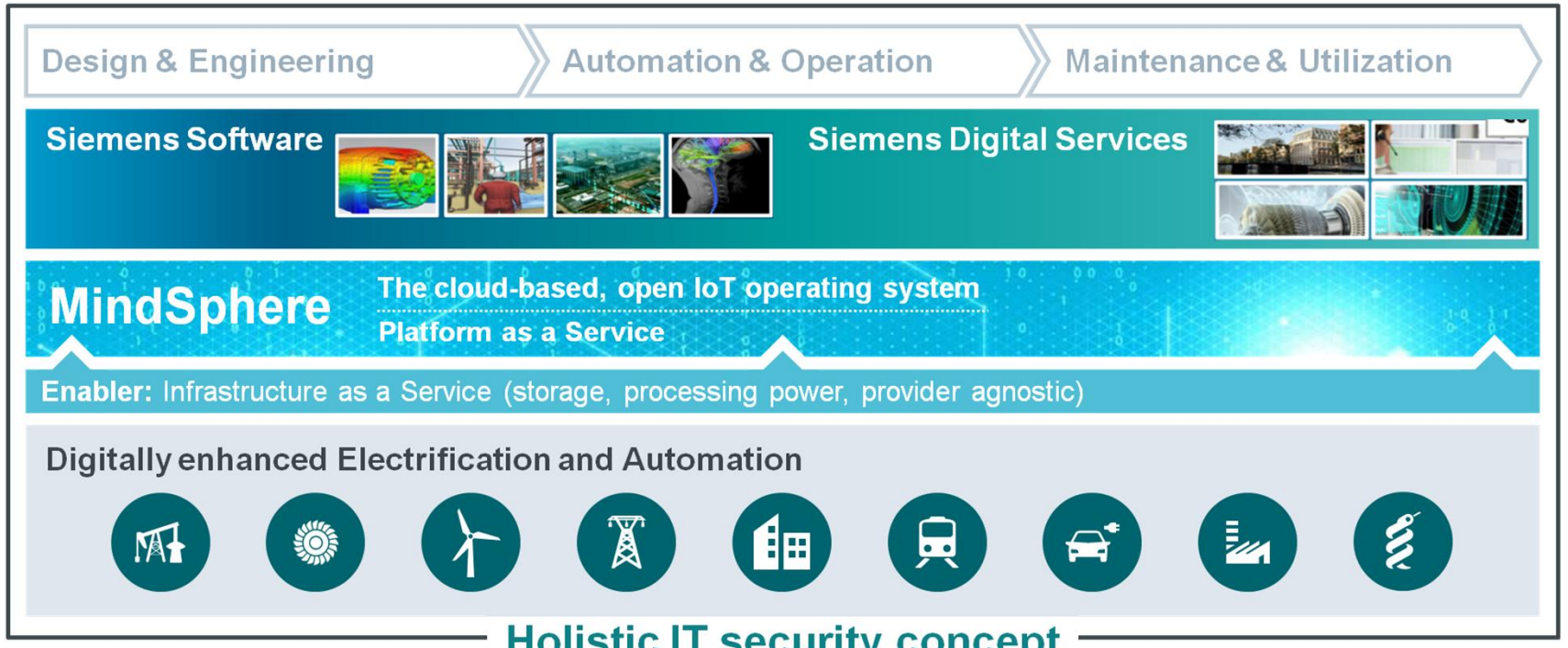
Digitalization is changing everything …
…we address Digitalization with a holistic approach

SIEMENS
Ingenuity for life

Value creation processes
Smart factory, smart plant, smart buildings

Digitally enhanced products
Smart products and solutions

Business models
Smart services



Innovation with a clear focus – Siemens Company Core Technologies

SIEMENS
Ingenuity for life

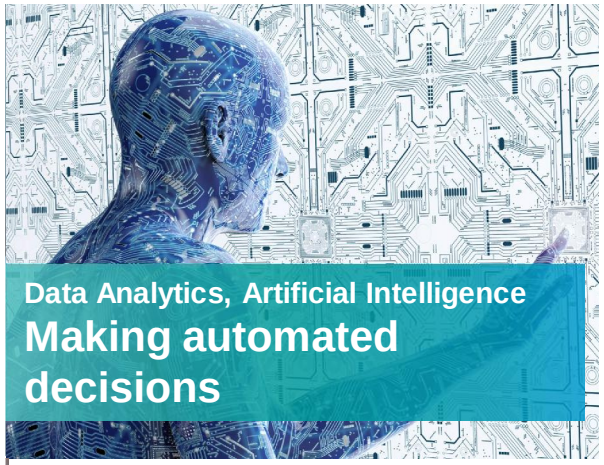
- Additive Manufacturing
- Autonomous Robotics
- Blockchain Applications
- Connected (e)Mobility
- Connectivity and Edge Devices
- Cybersecurity
- Data Analytics, Artificial Intelligence
- Distributed Energy Systems
- Energy Storage
- Future of Automation
- Materials
- Power Electronics
- Simulation and Digital Twin
- Software Systems and Processes

Company Core Technologies to drive Innovation in Digitalization

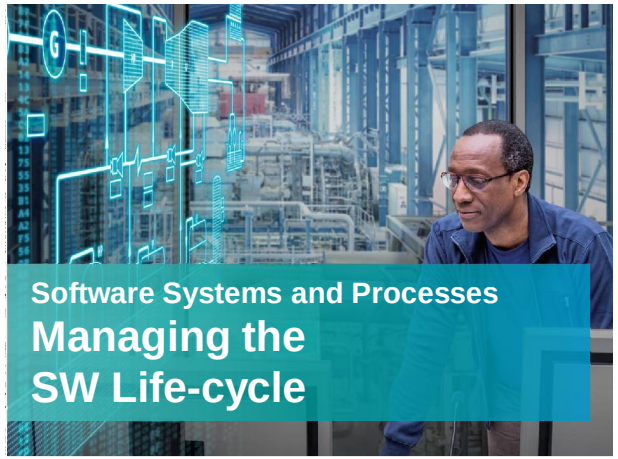
SIEMENS
Ingenuity for life

Connectivity and Edge Devices
Devices become intelligent and connected

Simulation and Digital Twin
Expanding the Digital Twin



Data Analytics, Artificial Intelligence
Making automated decisions



Software Systems and Processes
Managing the SW Life-cycle

Future of Automation
From automated towards autonomous systems

Autonomous Robotics
Controlling pervasive robotics

Connected (e)Mobility
Mobility is electric, connected, autonomous

Block-chain Applications
Managing Transactions

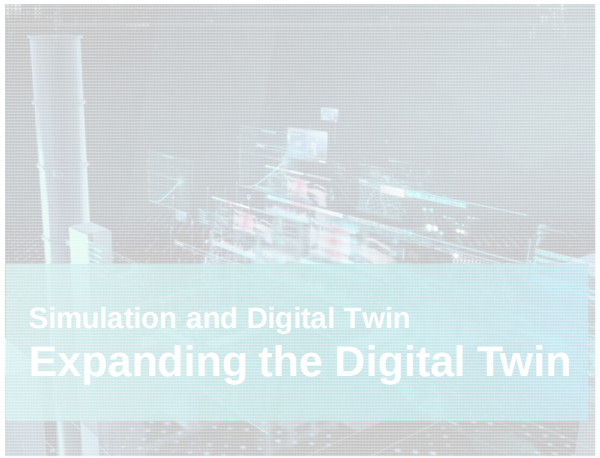
Cyber Security

Enabling Digitalization

Cyber Security is a key enabler to Digitalization

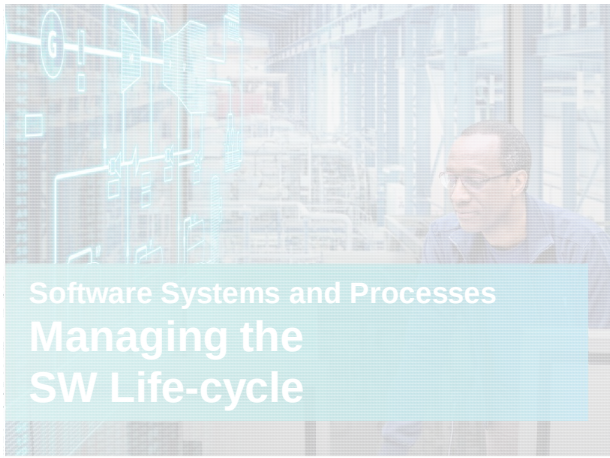
SIEMENS
Ingenuity for life

Connectivity and Edge Devices
Devices become intelligent and connected



Simulation and Digital Twin
Expanding the Digital Twin

Data Analytics, Artificial Intelligence
Making automated decisions



Software Systems and Processes
Managing the SW Life-cycle

Cyber Security
Enabling Digitalization

Cybersecurity – An increasingly critical factor for the success of the digital economy

SIEMENS
Ingenuity for life

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

1999
The globe is connected by the internet

1991
The World Wide Web becomes publicly accessible

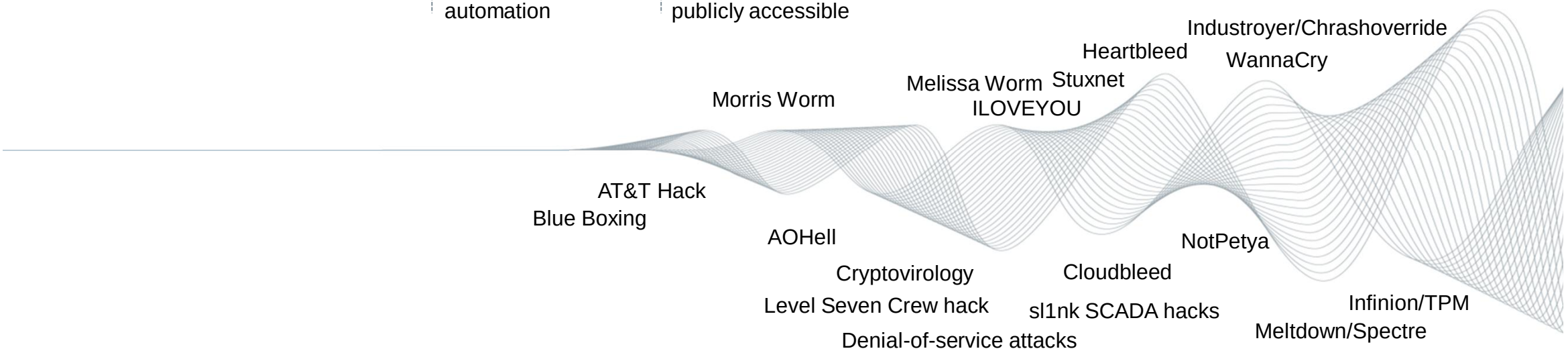
2000s
Mobile flexibility

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**



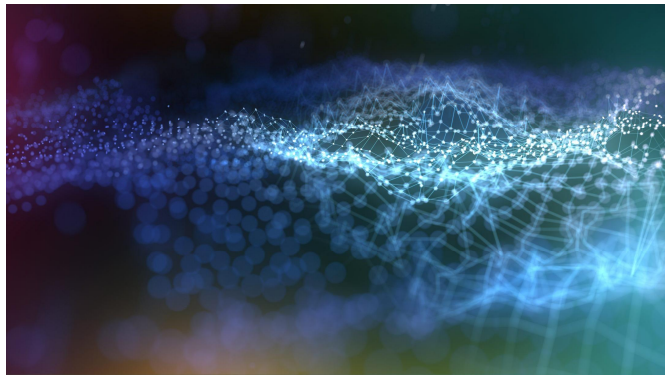
The challenges to Cyber Security require new approaches to technologies

SIEMENS
Ingenuity for life

Digitalization

Connected Industrial Control Systems offer new levels of efficiency and productivity …

but they also create new possibilities to cyber attacks



Business Units

Cyber Security technology to use for my future products/solutions?

How to secure existing installations?

How to securely connect to the cloud for digital services?

How to scale effort in CyberSecurity?

What is the technology to drive security services business?

Standards and regulations

e.g. IEC 62443 Security Levels

SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
SL3	Protection against intentional violation using sophisticated means, moderate resources, ICS specific skills, moderate motivation
SL4	Protection against intentional violation using sophisticated means, extended resources, ICS specific skills, high motivation

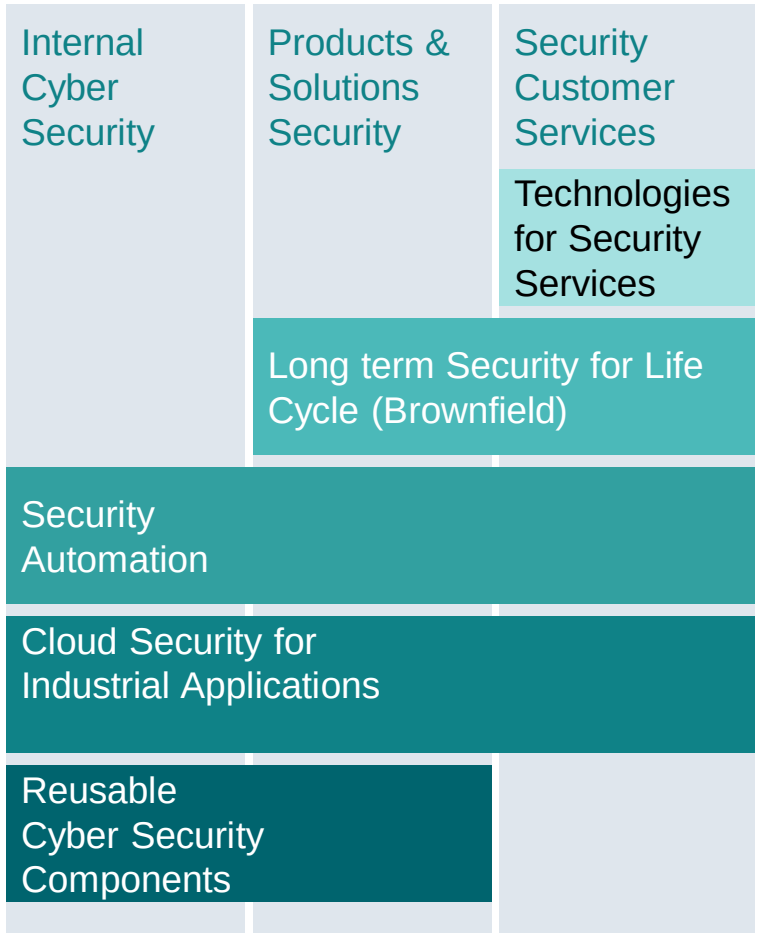
Need for Cyber Security Technology

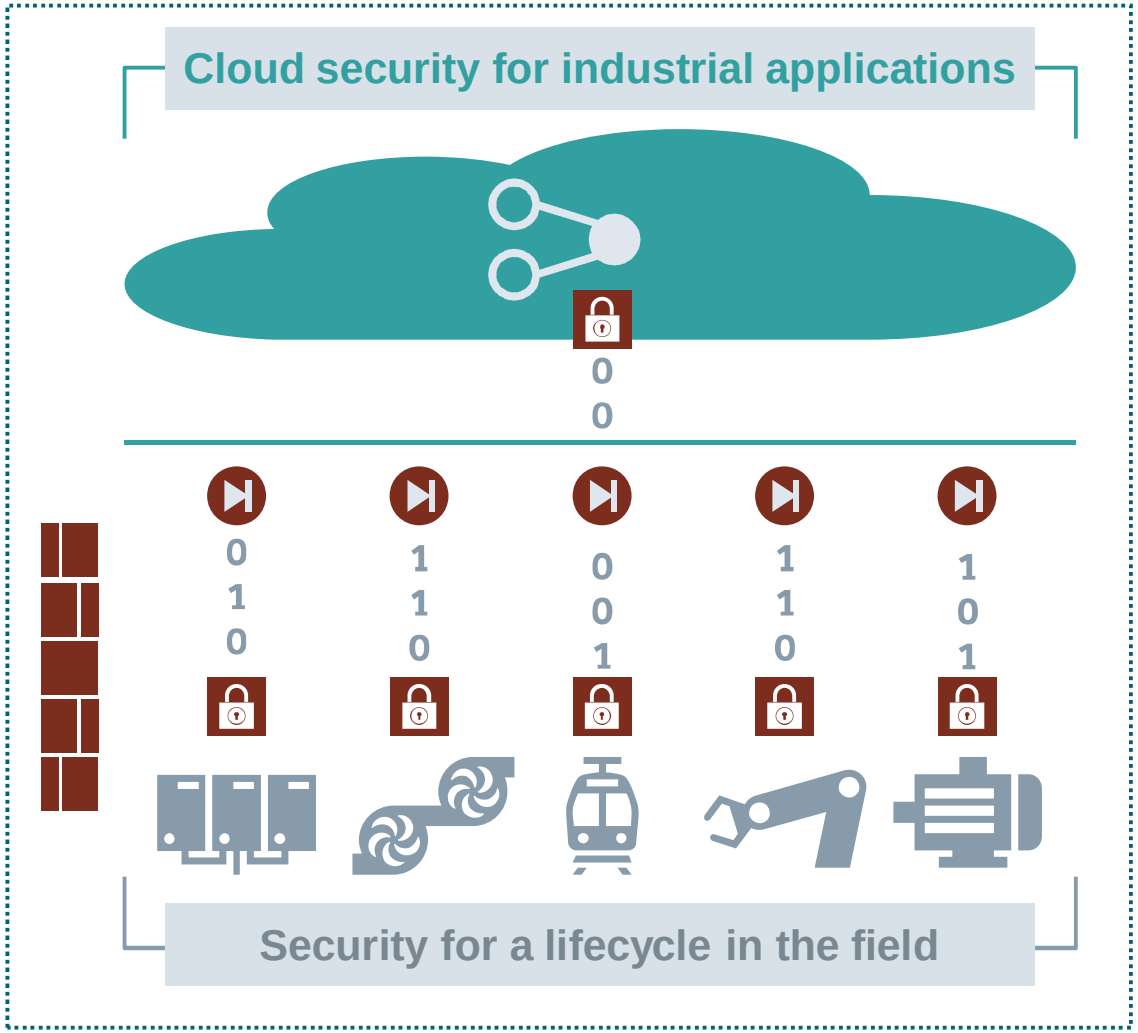
ICS: Industrial Control System | **IEC:** International Electrotechnical Commission

Scoping of CCT Cyber Security – Five action fields derived from business needs

SIEMENS
Ingenuity for life

Cyber Security Action Fields





Cyber Security
Protecting industrial infrastructure along their entire lifecycle

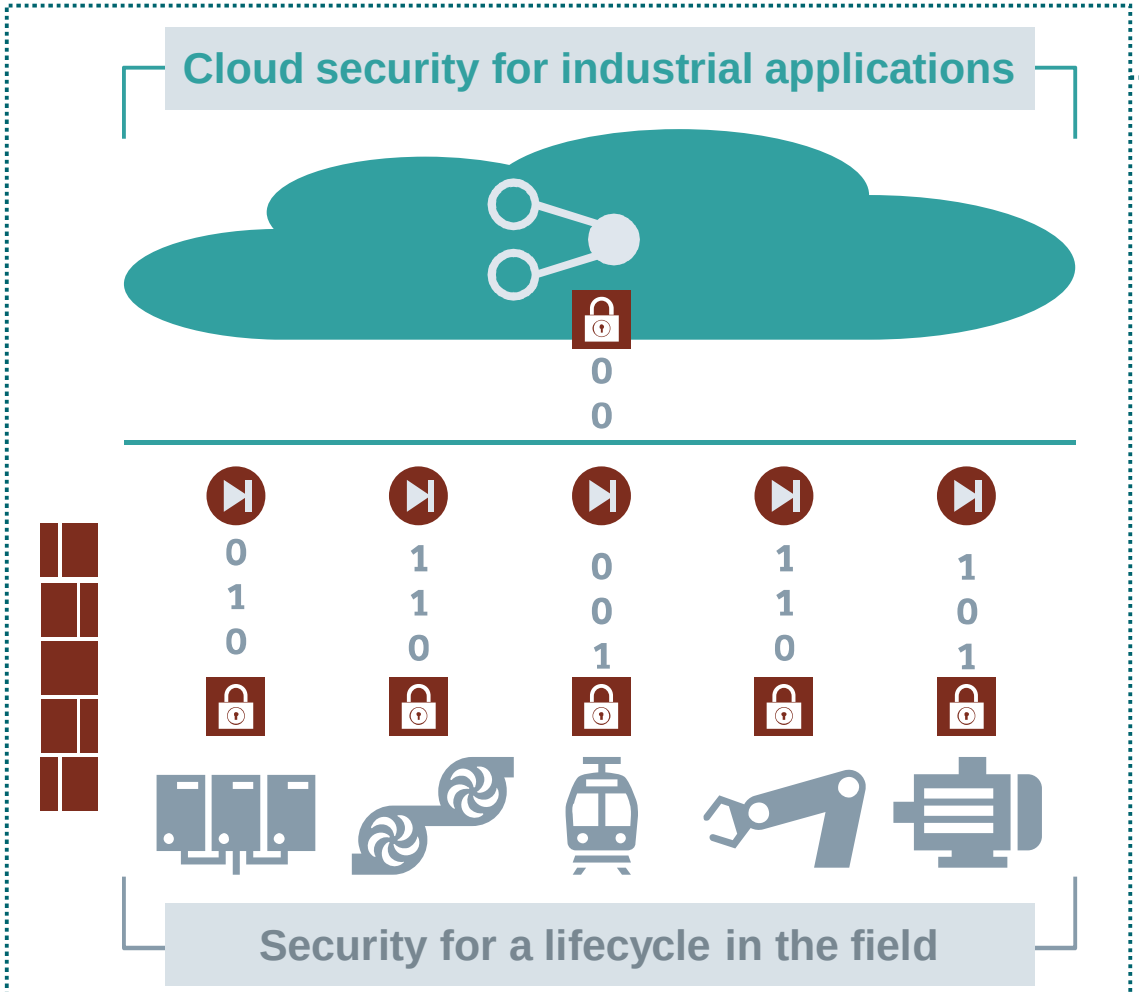
SIEMENS
Ingenuity for life

Security Components, e.g.

- One-way gateway
- IoT public key infra-structure, 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.

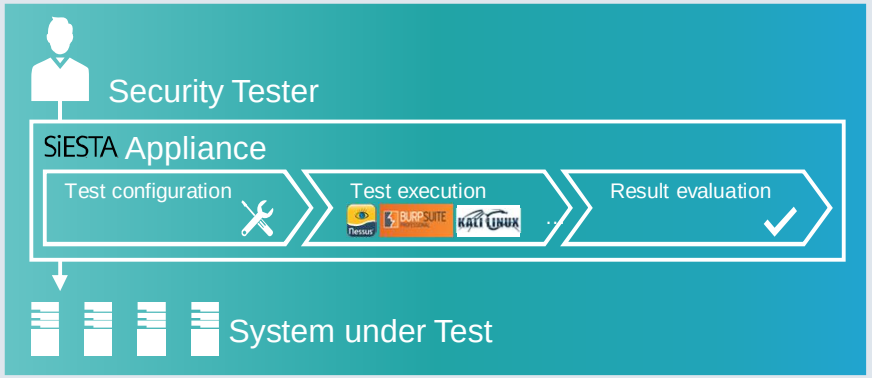
- Security analytics platform
- Artificial intelligence for security
- Automatic response – malware containment

Automated penetration testing and small footprint crypto enabled PKI

SIEMENS
Ingenuity for life

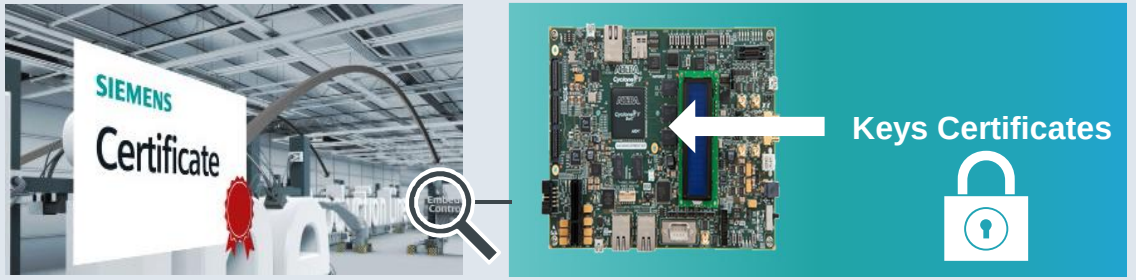
Automated Penetration Testing

- Accelerates and improves SW development
- Uses state-of-the-art security scanners and automatically updates with new attack patterns out of a central database
- Extended with automated hardening and support security standard for industrial control systems (IEC 62443)



Trust anchor and small footprint cryptography

- Central PKI service in secure environment
- Central signature service
- Secure key generation and storage using small footprint Elliptic Curve Cryptography
- Support of various platforms: crypto controller, FPGA, Software
- Tool kit for easy integration into products



PKI = Public Key Infrastructure; **HW** = Hardware; **SW** = Software; **FW** = Firmware

Cyber Security – long term research topics

SIEMENS
Ingenuity for life

Self-Securing Systems Design

Security Validation on Digital Twin

NextGen Patching

Security for Co-operative Autonom-ous Systems

Post Quantum Crypto

Homomorphic Encryption

Automated Forensics and Malware Analysis

Secure Cloud based Realtime Control

Supply Chain Security

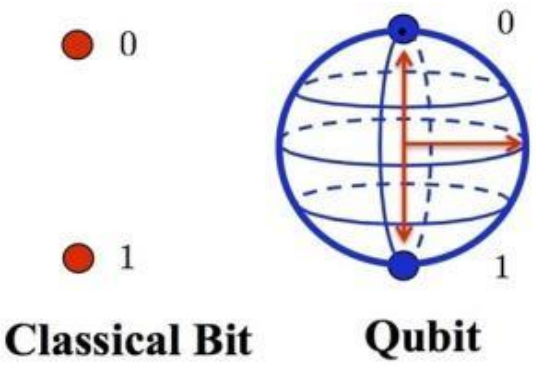
...

Post Quantum Crypto – Siemens products need to be protected from Quantum Computer attacks

SIEMENS
Ingenuity for life

Challenges

- Quantum Computers are able to break classical public key crypto (e.g. RSA) used for key distribution and signatures
- Current used hash functions (e.g. SHA family) and symmetric algorithms (e.g. AES encryption) are resistant against QC attacks
- Estimation: >1,000,000 qubits required to break current public keys, needing ~8 – 30 years of technology progress
- IBM: 50 qubits (2017), Google announced 72 qubits for 2018



Effects on Siemens

- Public key crypto has advantages (e.g. key negotiation, digital signatures) and is therefore used in many Siermens products
- Industrial products life-cycle is 20+ years Þ might become vulnerable to future QC attacks

Research Priorities

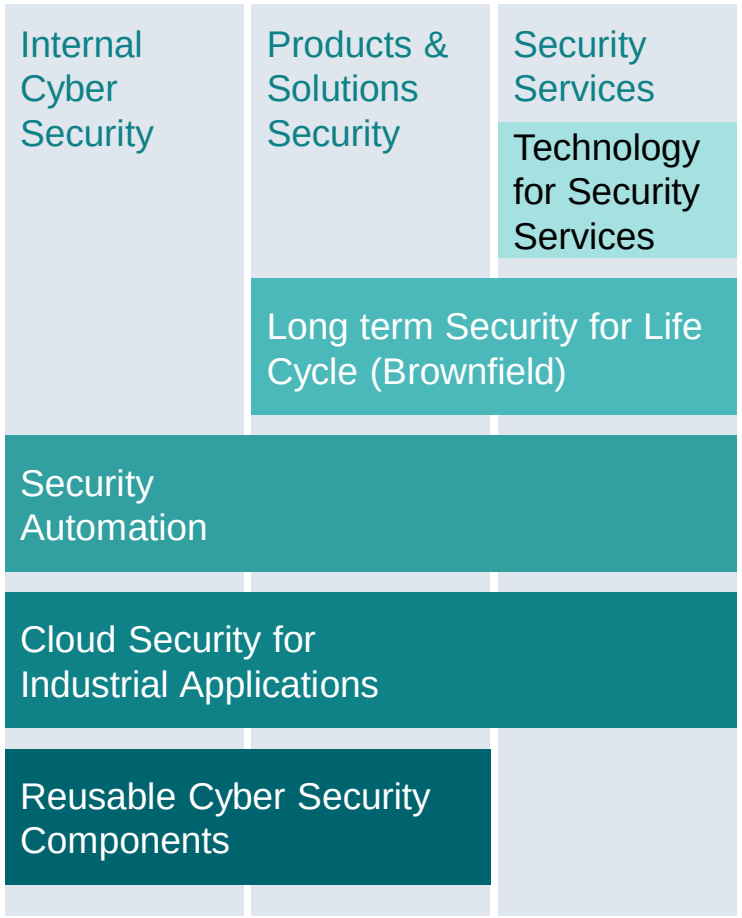
- Upcoming quantum secure crypto algorithms for usage within critical infrastructure, e.g. memory, realtime
- Design for crypto agility: ability to upgrade to crypto algorithms

QC: Quantum Computer | **RSA:** Rivest-Shamir-Adleman algorithm | **SHA:** Secure Hash Algorithm | **AES:** Advanced Encryption Standard

Cyber Security – Technology to secure Siemens

SIEMENS
Ingenuity for life

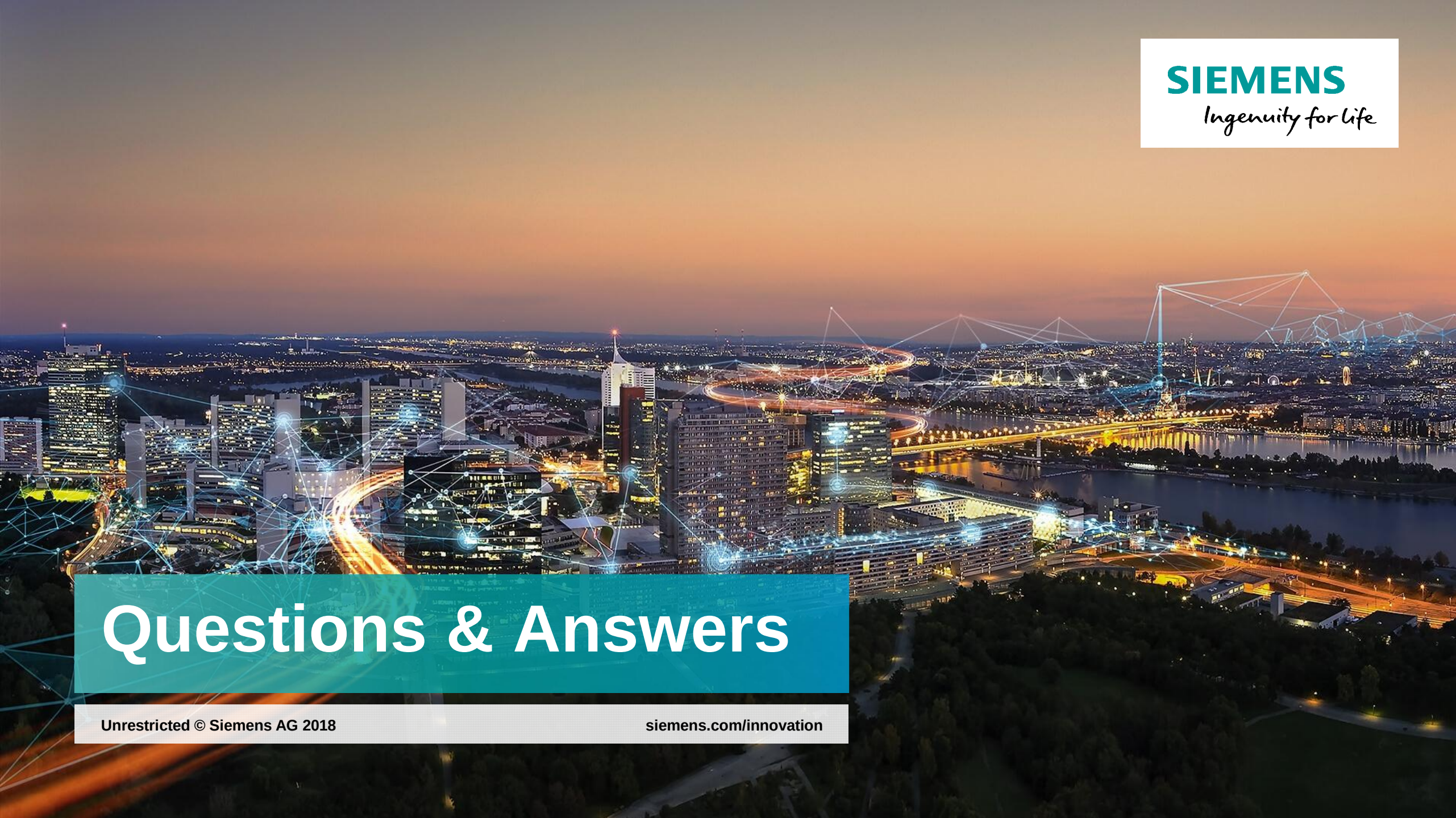
Cyber Security Action Fields



… protect our customers infrastructure

… automate and scale solutions to systematically address Cyber Security needs

… provide innovative and future-proof technology



SIEMENS
Ingenuity for life

Questions & Answers