SIEMENS

Corporate Technology

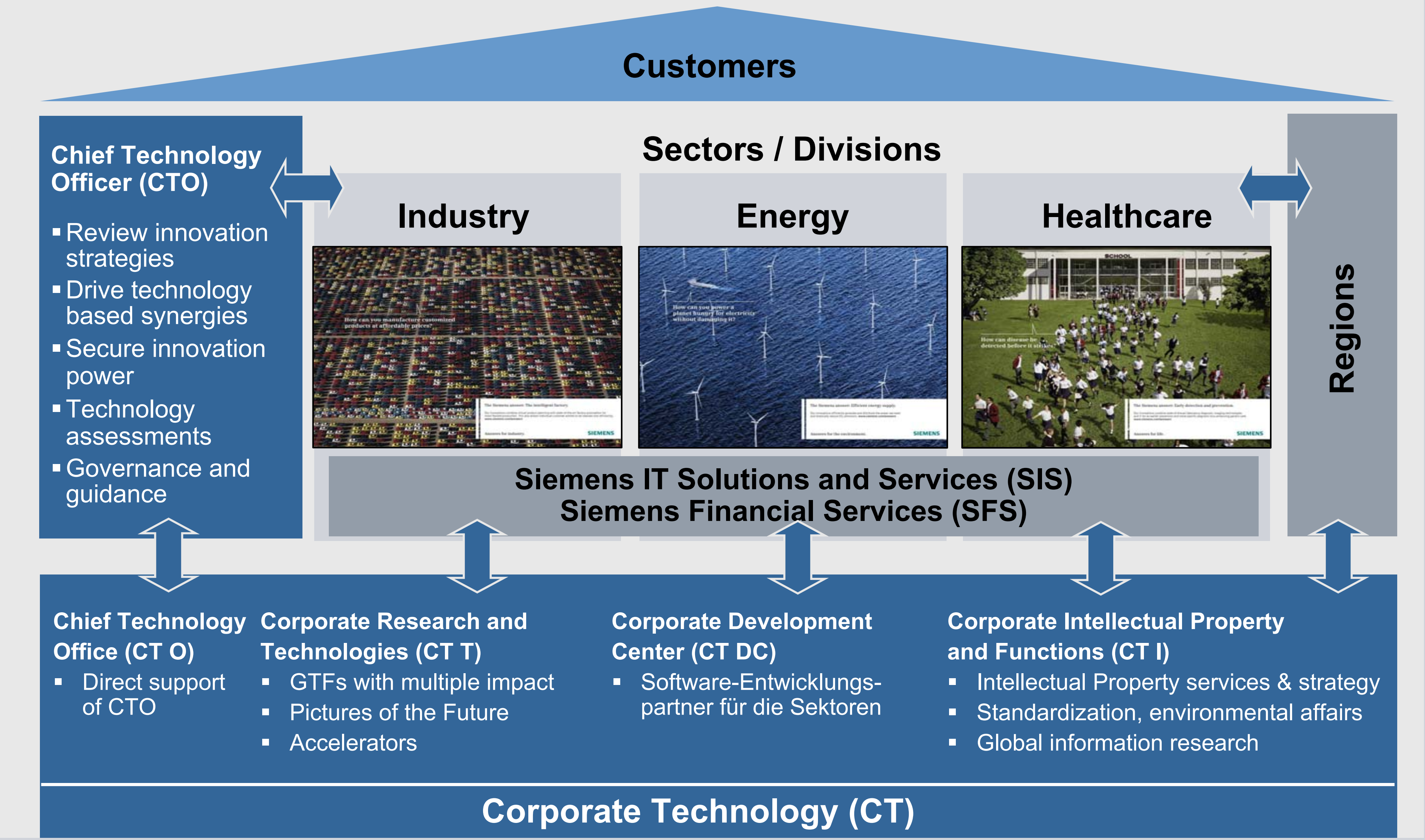
Rollout of Security Credentials in Industrial Environments

SECURWARE 2010

Rainer Falk, Steffen Fries
GTF IT Security

Corporate Technology

Networking the integrated technology company



How can you manufacture customized products at affordable prices?
The Siemens answer: The intelligent factory.
Answers for industry.
SIEMENS
How can you power a planet hungry for electricity without damaging it?
The Siemens answer: Efficient energy supply.
Answers for the environment.
SIEMENS
SCHOOL
How can disease be detected before it strikes?
The Siemens answer: Early detection and prevention.
Answers for life.
SIEMENS

Customers

Chief Technology Officer (CTO)

- Review innovation strategies
- Drive technology based synergies
- Secure innovation power
- Technology assessments
- Governance and guidance

Sectors / Divisions

Industry

Energy

Healthcare

Regions

Siemens IT Solutions and Services (SIS)
Siemens Financial Services (SFS)

Chief Technology Office (CT O)

- Direct support of CTO

Corporate Research and Technologies (CT T)

- GTFs with multiple impact
- Pictures of the Future
- Accelerators

Corporate Development Center (CT DC)

- Software-Entwicklungs-partner für die Sektoren

Corporate Intellectual Property and Functions (CT I)

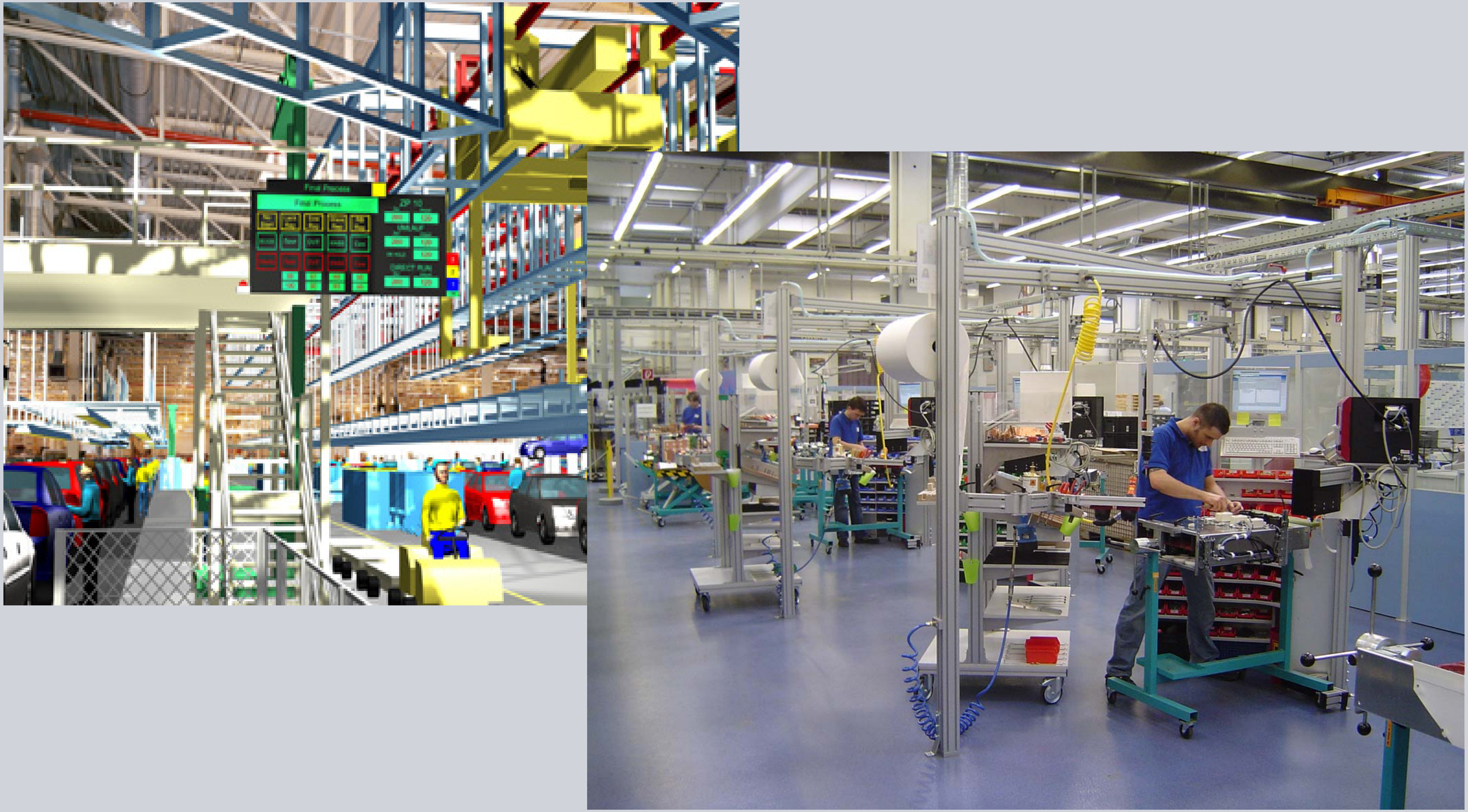
- Intellectual Property services & strategy
- Standardization, environmental affairs
- Global information research

Corporate Technology (CT)

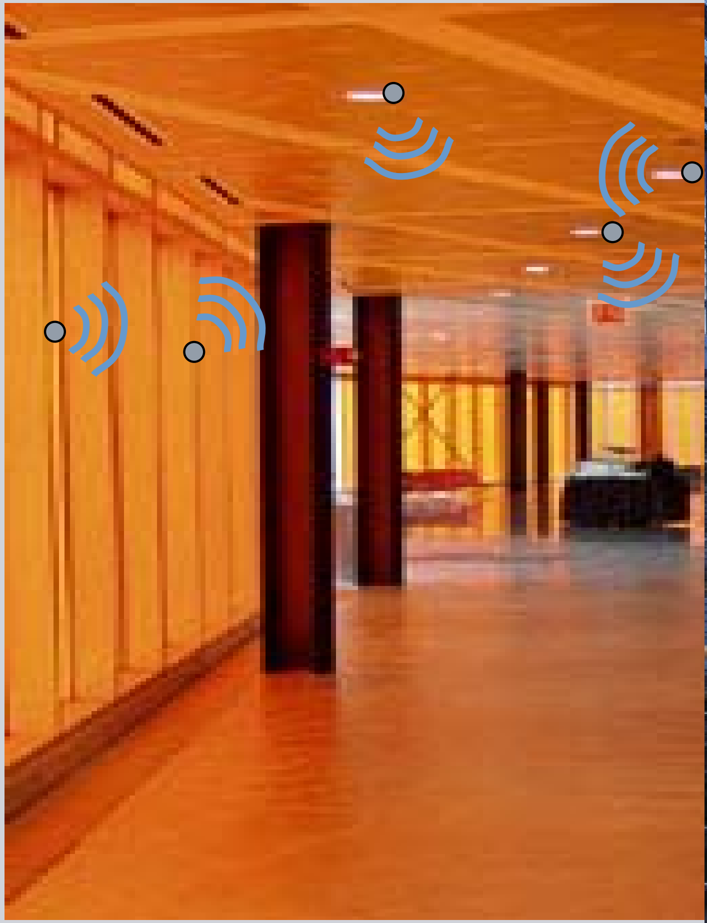
Motivation

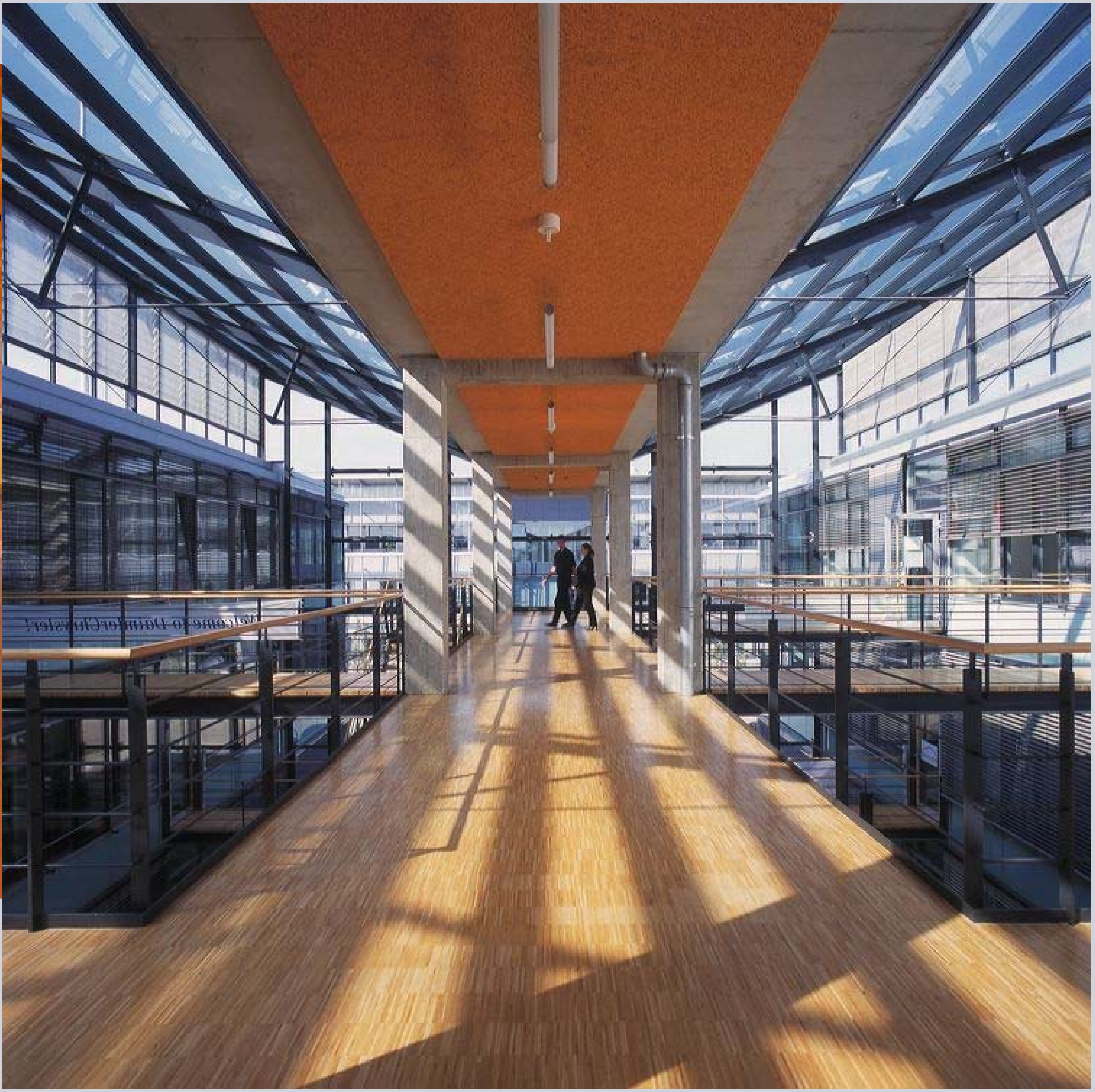
Industrial Environments: Process Automation

Industrial Environments: Factory Automation

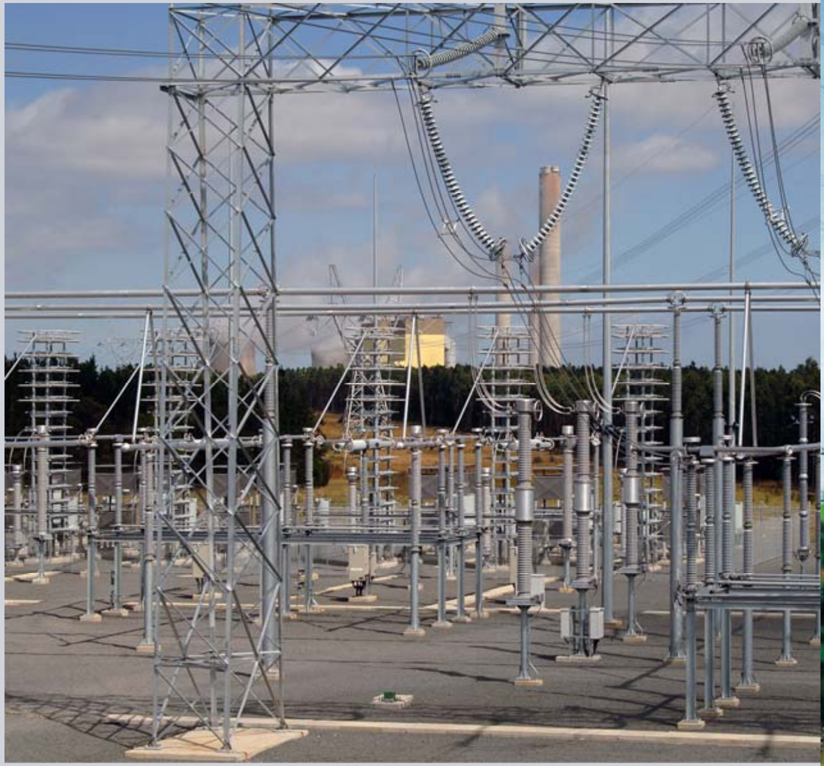


Industrial Environments: Building Automation





Industrial Environments: Energy Automation

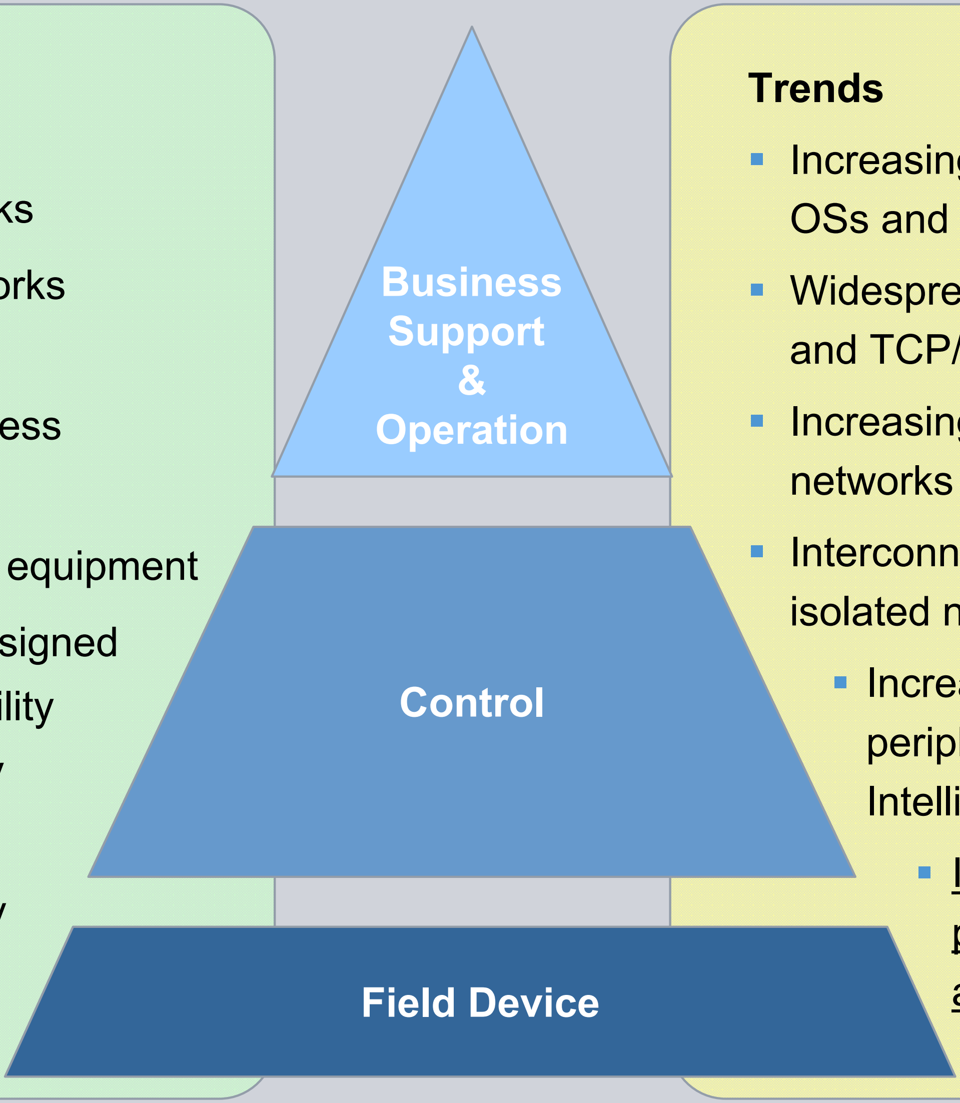


IT-Security Becomes a Pre-requisite for Future Control Systems Driven by Convergence of Safety & Security

SIEMENS

Status

- Predominantly isolated communication networks
- Often proprietary networks and applications
- Physically secured access to networks
- Long lifetime of control equipment
- Systems are mainly designed for performance, reliability and safety, not security
- Often availability is the most important security objective



Trends

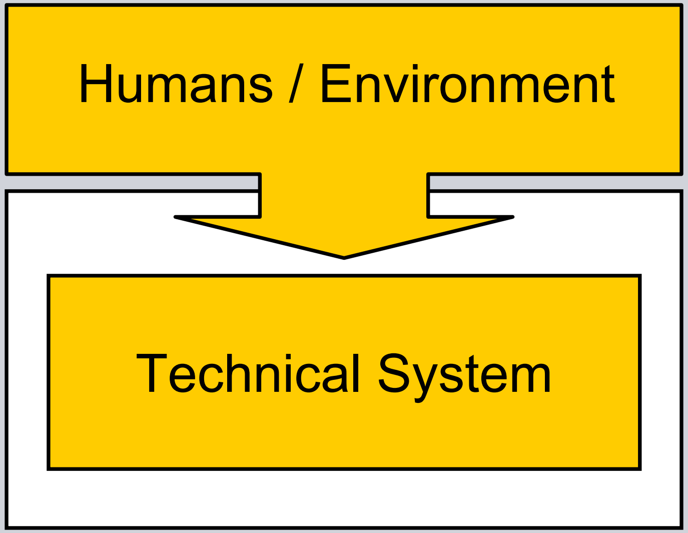
- Increasing usage of standard OSs and applications
- Widespread usage of Ethernet and TCP/IP (including Internet)
- Increasing usage of wireless networks
- Interconnection of formerly isolated networks
  - Increasing intelligence in peripheral components (e.g. Intelligent Access Devices)
    - <u>IT-security becomes a pre-requisite for safety applications</u>

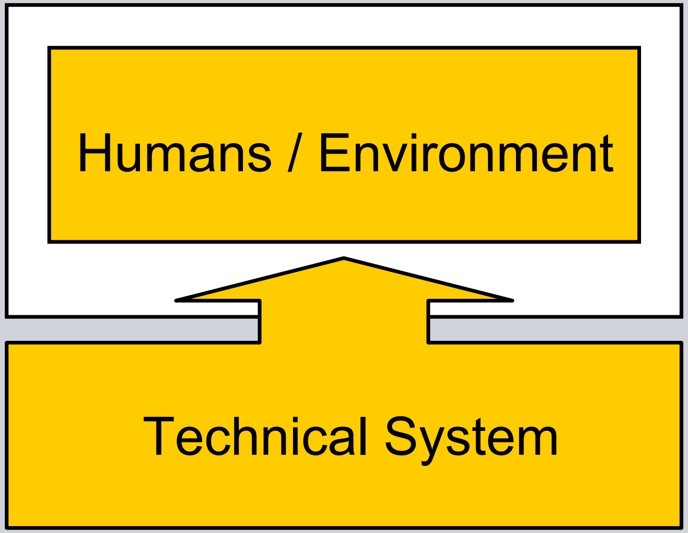
SIEMENS

Security and Safety

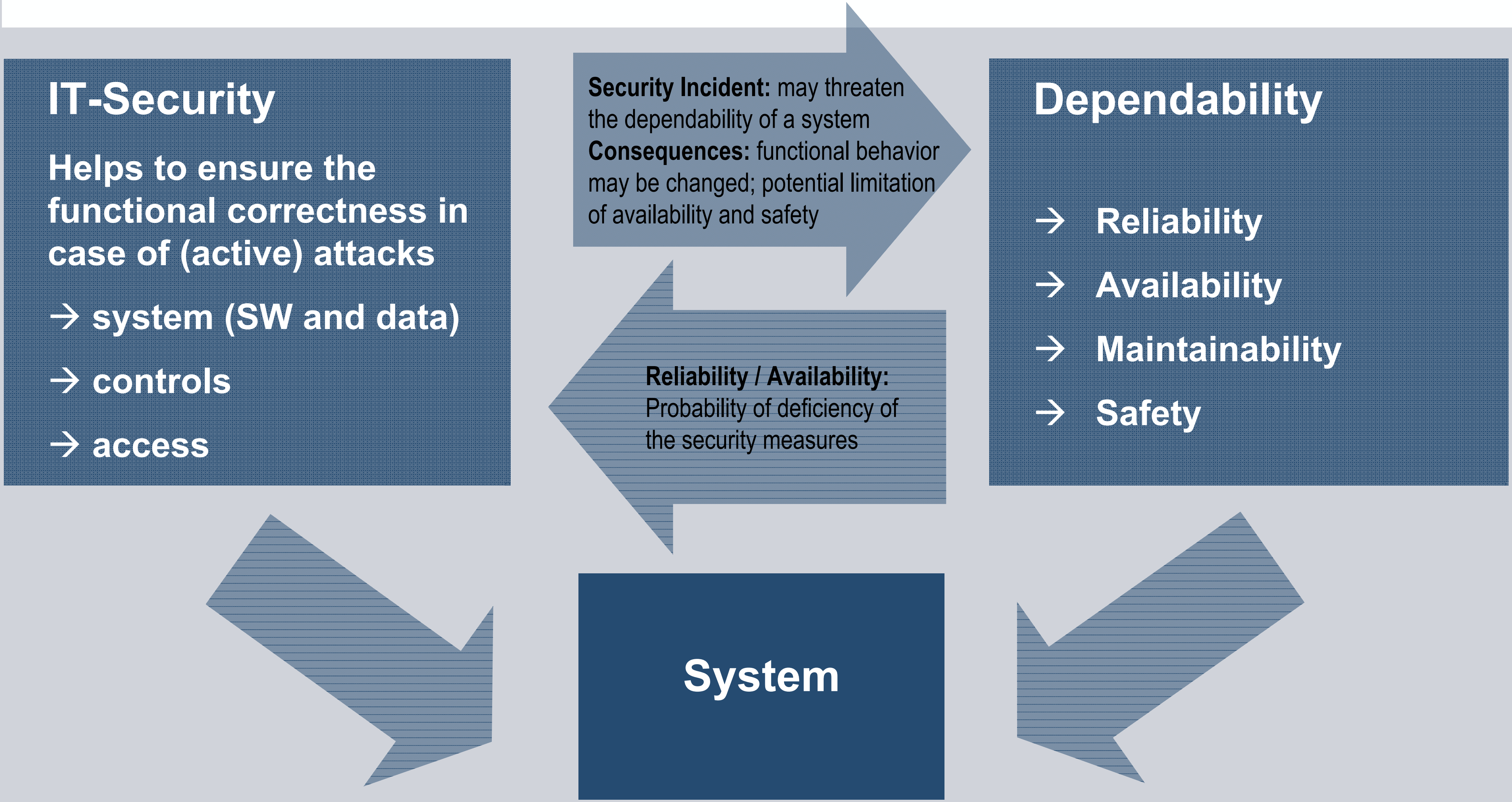
Security / IT Security:
Prevention of consequences of threats to a system (intentionally) caused by humans and/or environment

Safety:
Prevention of threats to humans and environment caused by technical systems





Interrelation Between
IT-Security and Dependability of a System



IT-Security

Helps to ensure the functional correctness in case of (active) attacks

→ system (SW and data)

→ controls

→ access

Security Incident: may threaten the dependability of a system
Consequences: functional behavior may be changed; potential limitation of availability and safety

Reliability / Availability: Probability of deficiency of the security measures

Dependability

→ Reliability

→ Availability

→ Maintainability

→ Safety

System

Remark: Failures caused by security attacks cannot be assumed to be independent !
⇒ Therefore classical safety/failure analyses do not cover them properly

Example:
Maroochy Waste Water Incident

SIEMENS

Queensland, Australia, 2000:
Former contractor took control of 150 sewage pumping stations. Over a 3-month period, he released one million liters of untreated sewage.

Unauthorized access to the control system over a unsecured communication path.

Communications sent by radio links to wastewater pumping stations were being lost
Pumps were not working properly
Alarms put in place to alert staff to faults were not going off

Remark: Failures caused by security attacks cannot be assumed to be independent !
⇒ Therefore classical safety/failure analyses do not cover them properly

Example:
Potential Derogation of Dependability through Security

SIEMENS

- The usage of standard anti-virus software may lead to blocking of safety relevant communication
- Standard anti-virus software typically requires human interaction
- Usage of IT-security mechanisms may occupy too many system resources

Standard IT-security mechanisms known from the office world have to be adapted to meet dependability requirements

Example: Usage of “Plagiarisms” Influences System Behavior

SIEMENS

China, 2008:

System performance of mobile networks were decreased noticeably.
The service company instructed for maintenance used cheaper plagiarisms instead of original spare parts.

IT-security measures (e.g. not forgeable „genuineness chip“) can help to identify and thereby reduce the usage of plagiarisms.

SIEMENS

Differences and Security Applications

Automation Network Specifics:
Focus on Different Security Requirements

SIEMENS

	Office	Automation Network
Confidentiality (Data)	High	Low – Medium
Integrity (Data)	Medium	High
Availability / Reliability (System)	Medium	High
Non-Repudiation	Medium	High
Component Lifetime	Short - medium	Long

▶ “Office“ Security Concepts are not directly applicable for Automation Networks

Embedded Security Mechanisms Provide Essential Functionality for Ensuring System Integrity

Security is required to ensure Safety-relevant system properties in environments exposed to attacks

Plant Integrity Check

Verify integrity of overall plant installation
(deployed components, cabling, software).
This ensures detection of unauthorized changes of the plant installation.

Original spare parts (Anti-Counterfeiting)

Ensure that original spare parts are installed, and not counterfeited replacements with poor quality.

Software Integrity Check

Ensure that firmware and configuration has not been altered.
Device is going to regular operation only with valid software configuration.

Secure Software Update

Ensure that only approved software updates are installed. Ensure that software is installed in compliance with defined update procedures. defined

Encrypted Machine Communication

Encrypted communication prevents manipulation and interception of machine control and service data when transmitted over networks (device control, plant, and public networks / remote service).

SIEMENS

Credential Lifecycle

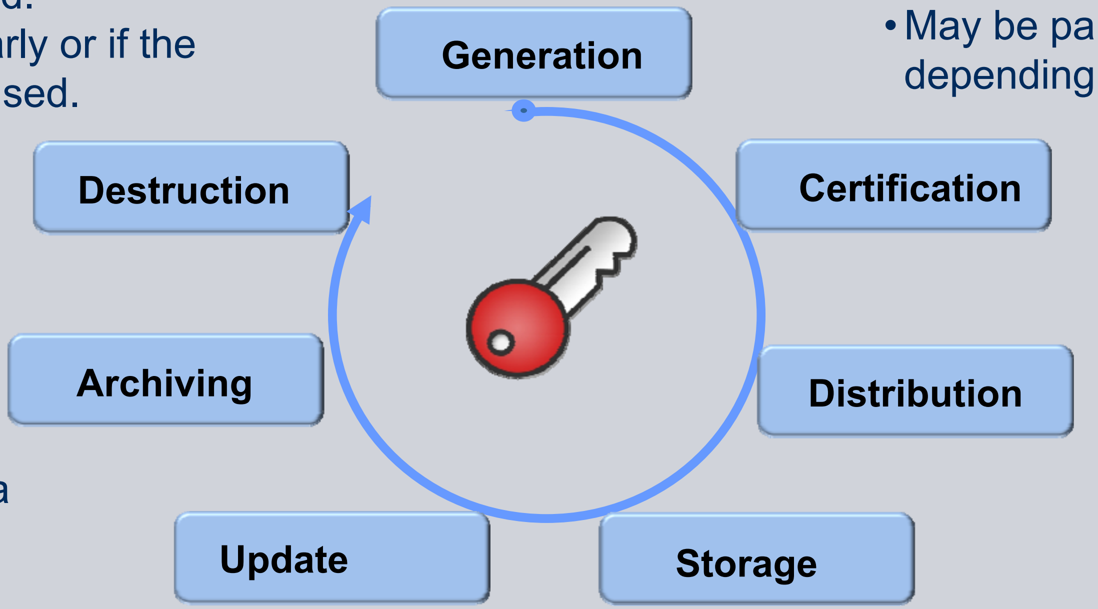
Security Credential Have to be Managed Along Their Whole Lifecycle

SIEMENS

- Internal Generation (e.g., CSR)
- External Generation
- Long term keys, session keys

- Session keys destructed after session ending
- Long term keys are deleted, after keys have been renewed.
- Lifetime may end regularly or if the key has been compromised.

- Typically done for asymmetric keys through a certificate authority (CA)
- May be part of the key generation, depending on the credential



Generation

Certification

Distribution

Storage

Update

Archiving

Destruction

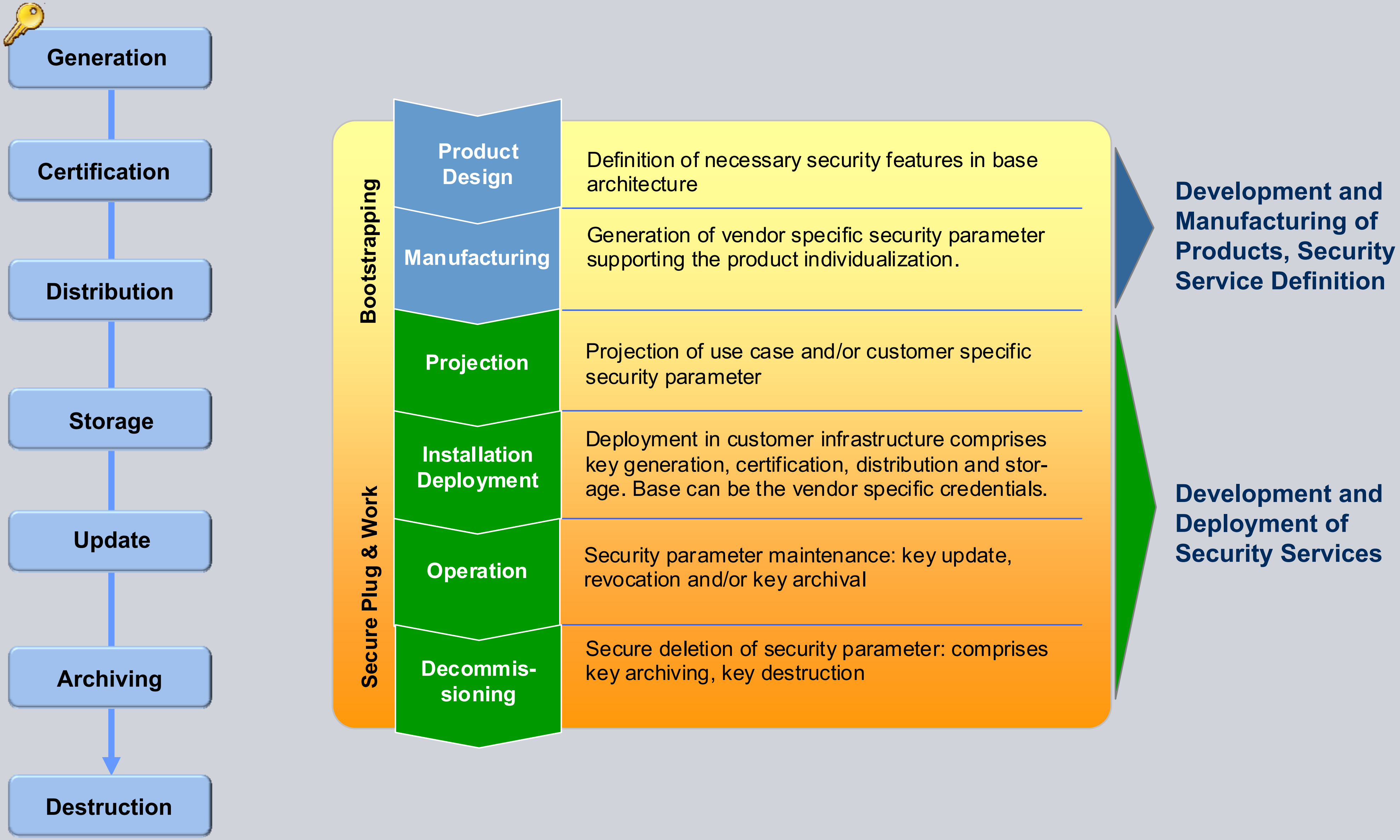
- Typically long term (secure or private) keys are archived to enable access to encrypted data

- Depends on generation method
- offline/online (in-band, out-of-band)

- Cryptographic keys have a dedicated lifetime
- may be performed by the security protocol
- based on a given security policy

- obfuscated in firmware, software
- in secured memory (e.g., flash)
- separate hardware module (e.g., smart card or a trusted platform module)

Security Credential Lifecycle Management – a Service Accompanying Products



Product Design: Definition of necessary security features in base architecture

Manufacturing: Generation of vendor specific security parameter supporting the product individualization.

Projection: Projection of use case and/or customer specific security parameter

Installation Deployment: Deployment in customer infrastructure comprises key generation, certification, distribution and storage. Base can be the vendor specific credentials.

Operation: Security parameter maintenance: key update, revocation and/or key archival

Decommissioning: Secure deletion of security parameter: comprises key archiving, key destruction

Development and Manufacturing of Products, Security Service Definition

Development and Deployment of Security Services

SIEMENS

Potential Approaches

Different Approaches can be Followed for Security Parameter Rollout

Offline parameter distribution

- Performed using dedicated engineering tools directly connected to the device or via a separate network
- Requires a (mobile or fixed) engineering station in the offline network having all parameter sets for the devices to be bootstrapped available.

Out-of-band parameter distribution

- Separate logical or physical communication channel used to configure security parameter. Basically resembles the offline distribution approach using an online connection instead of the separate physical network.
- Devices may already possess a cryptographic credential, which can be provided by the device manufacturer.

In-band parameter distribution

- Distribution using the same communication channels as used during regular operation
- May be based on pre-configured device identifier (like the MAC address), manufacturer installed security credentials or even liaison devices.

Credential Bootstrapping has to be Suitable for Addressed Environment

Outlook

SIEMENS

Research Topics – Security and Device Authentication

Industrial systems for all verticals like energy, transportation, automation systems, health require secure device authentication and machine-2-machine communication as a core security feature. Siemens is a leading provider for technology and solutions in these areas.

Situation

- Machine-2-Machine connectivity down to field devices is a major driver for Future Internet. Potentially more than 60 Billion devices will be connected. All industries are affected including manufacturing, process, building, energy automation, transportation, health.
- Device authentication is the prerequisite to ensure an appropriate protection of communication between different devices. This is the basis to realize secure device-oriented services like secure control, monitoring, remote service, metering, licensing or anti counterfeiting.
- Device credentials (keys, certificates) have to be generated and managed efficiently
- The non-human security environment requires new device-oriented security and identity infrastructures.
- The huge number of devices and the specific application environment require a zero-configuration effort.
- Process comprises the generation (short and long term), distribution and implementation of initial security parameter of the target devices

Topics

- Efficient cryptographic mechanisms for device authentication and secure device communication
- device security platform module
- device-oriented security and identity infrastructure (processes, scalability, limits of authority, privacy)
- Plug-and-play security to avoid administrative burden
- secure device-oriented services