Cyber Security for Industries

Dr. Rainer Falk (rainer.falk@siemens.com)

Siemens – Vision 2020

Downtown Singapore

The partner of choice for

- Electrification
- Automation
- Digitalization

Siemens stands for the electrification of the world

SIEMENS

Our innovative power in figures

Siemens as a whole and Corporate Technology

Expenditures for research and development – our greatest strength

€4.4 billion

Expenditures for R&D –
€400 million more than in fiscal 2014

28,800

R&D employees[1]

Inventions and patents – securing our future

8,600

inventions[1]

4,300

patent applications

University cooperations – our knowledge edge

7

CKI universities

17

principal partner universities

[1] In fiscal 2014

Corporate Technology – our competence center for innovation and business excellence[2]

7,800

employees worldwide

5,100

software developers

1,600

researchers

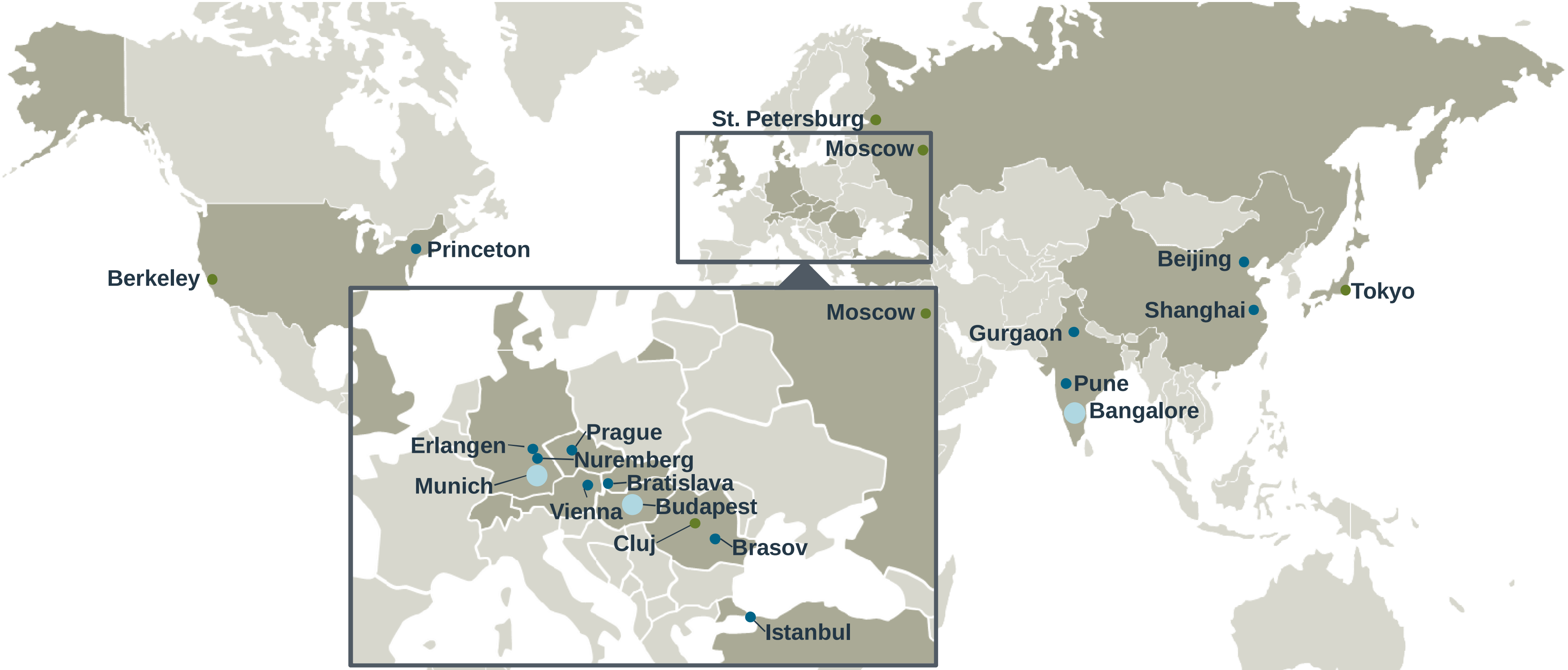
400

patent experts

[2] Employee figures: status May 2015

Our global presence

Partner to customers all over the world

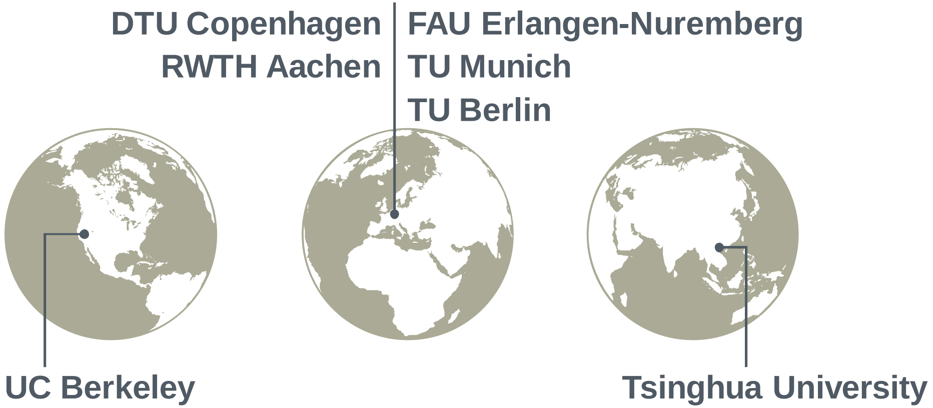


▨ Country with CT facility ▨ > 500 employees ■ 100 – 500 employees ■ Other selected facilities

Status May 2015

Our areas of activity: Research cooperations

Overcoming the silo mentality and tapping potential



DTU Copenhagen
RWTH Aachen

FAU Erlangen-Nuremberg
TU Munich
TU Berlin

UC Berkeley

Tsinghua University

7
CKI universities

17
principal partner universities

- We network with leading universities and non-university research institutes around the world.
- With Open Innovation, we strengthen Siemens’ innovative power and tap the potential of a networked, open company.
- We link the industrial and academic worlds and thus promote intensive research and recruiting activities.
- Our cooperation with seven top universities and the “Centers of Knowledge Interchange” (CKIs) that we set up there are an excellent example of this.

Our organization
Corporate Technology at a glance

Corporate Technology (CT)

CTO – Prof. Dr. Siegfried Russwurm

Business Excellence, Quality Management, *top*⁺

- Business excellence
- Quality management
- Internal process and production consulting

Corporate Development Center

- Development partner in the areas of software, firmware and hardware as well as engineering

evosoft

- Competence center for horizontal and vertical product and system integration

Corporate Intellectual Property

- Protection, use and defense of intellectual property
- Patent and brand protection law

Innovative Ventures

- Access to external innovations
- Start-up foundation
- Commercialization of innovations

New Technology Fields

- Research into potentially disruptive innovations with high market potential

Research and Technology Center

- Development of technologies with a broad impact
- Incubator for innovations of our portfolio

Technology and Innovation Management

- Siemens' technology and innovation agenda
- Standardization, positioning regarding research policy
- Provision of publications relating to R&D

University Relations

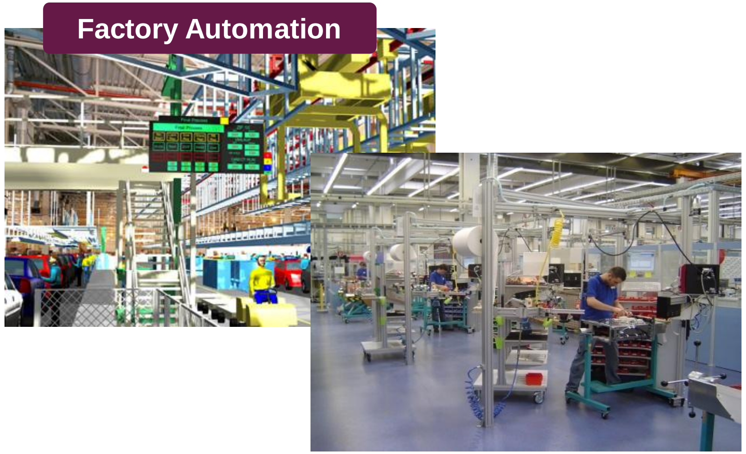
- Global access to the academic world
- Top positioning in terms of university cooperations

Status May 2015

Increasing intelligence and open communication drive security requirements in various industrial environments

Process Automation

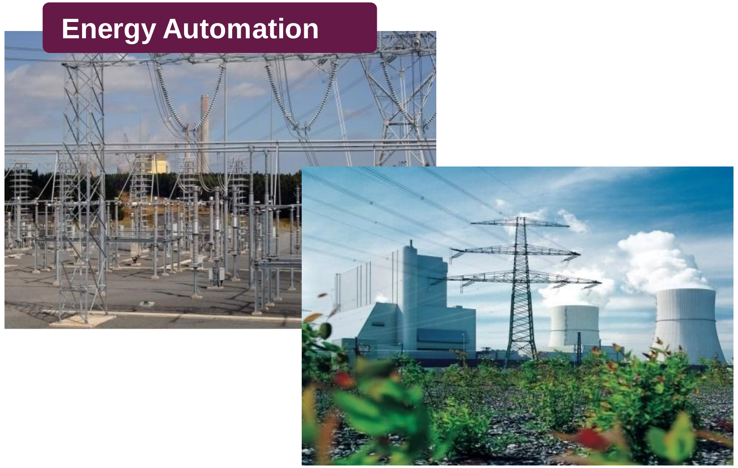
Factory Automation



Urban Infrastructures

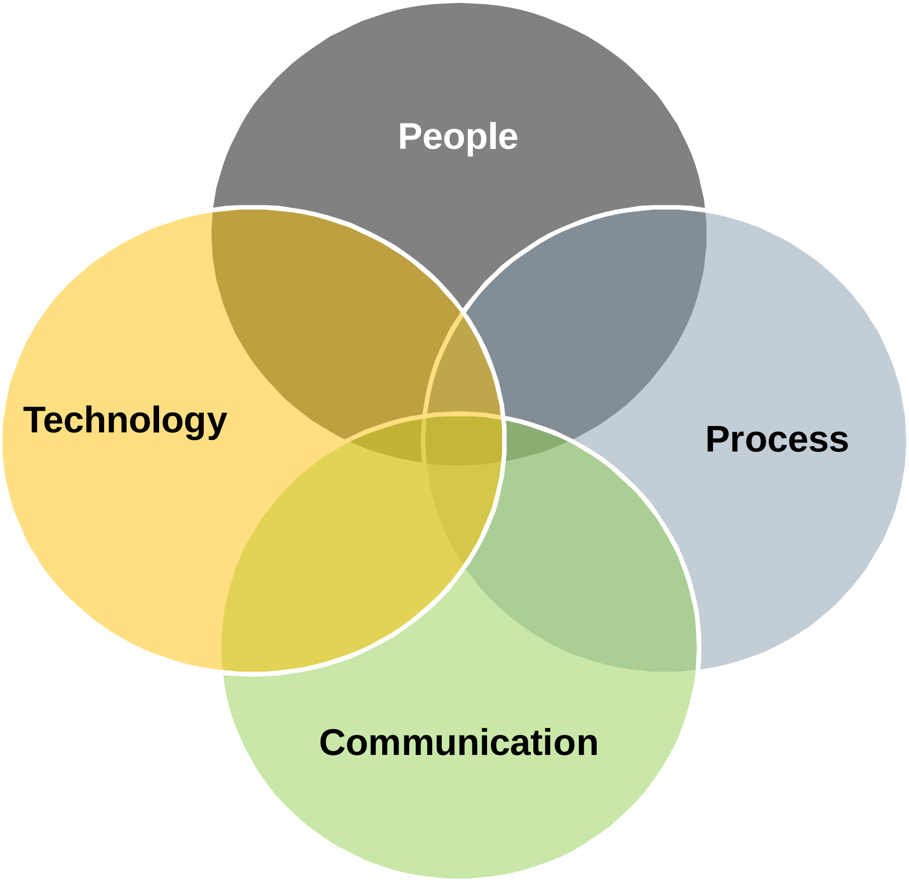
Building Automation

Energy Automation



Mobility Systems

Cyber security needs a holistic approach



Our industrial society confesses a growing demand for IT-Security

IT Security trends are determined by drivers such as:

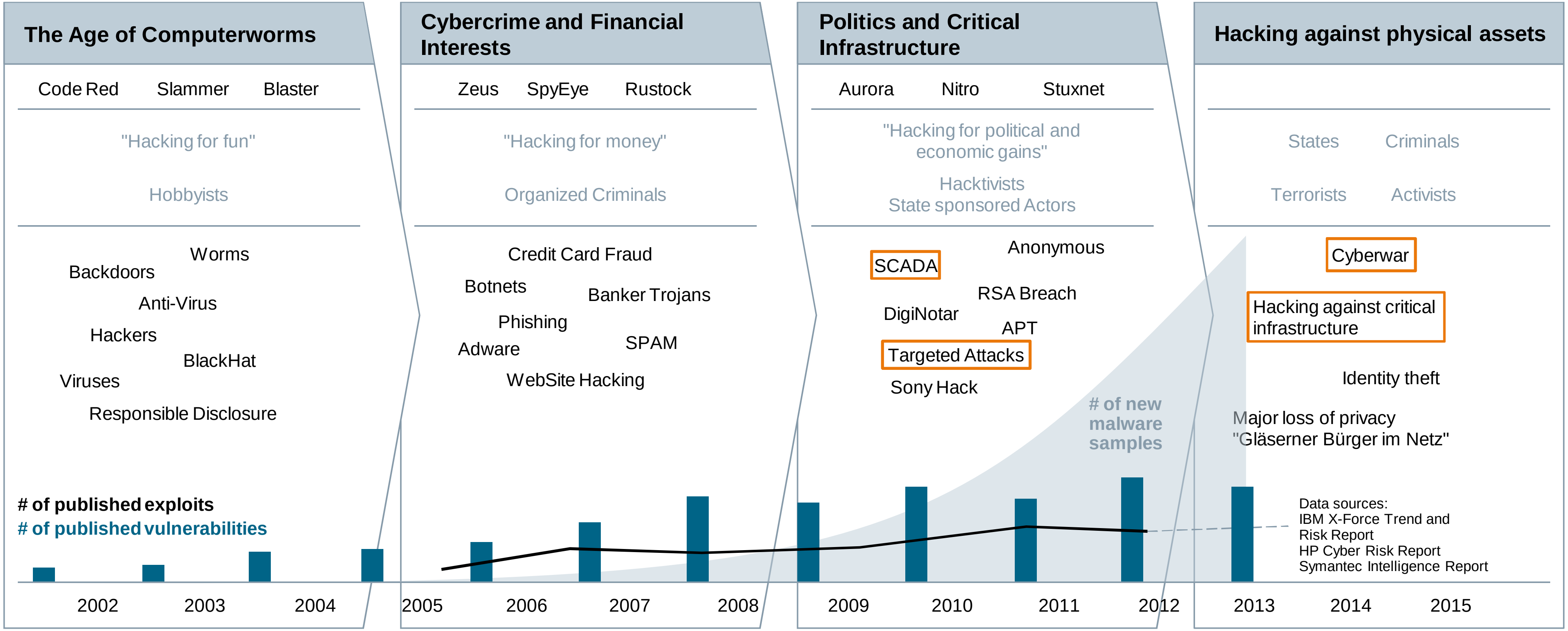
- Industry infrastructures changes (Digitalization)
- More networked embedded systems
- Increasing device-to-device communication
- Need to manage intellectual property

And

- Increasing international organized crime
- Privacy
- Compliance enforcement
- Cyber war fare
- Cloud/Virtualization
- PDAs, Smart Mobiles
- Social Networks / data mining concepts

The threat level is rising – attackers are targeting critical infrastructures

Evolution of attacker motives, vulnerabilities and exploits



The Age of Computerworms

Code Red Slammer Blaster

"Hacking for fun"

Hobbyists

Worms
Backdoors
Anti-Virus
Hackers
BlackHat
Viruses
Responsible Disclosure

Cybercrime and Financial Interests

Zeus SpyEye Rustock

"Hacking for money"

Organized Criminals

Credit Card Fraud
Botnets
Banker Trojans
Phishing
Adware
SPAM
WebSite Hacking

Politics and Critical Infrastructure

Aurora Nitro Stuxnet

"Hacking for political and economic gains"

Hacktivists
State sponsored Actors

SCADA
Anonymous
RSA Breach
DigiNotar
APT
Targeted Attacks
Sony Hack

Hacking against physical assets

States Criminals

Terrorists Activists

Cyberwar
Hacking against critical infrastructure
Identity theft
Major loss of privacy
"Gläserner Bürger im Netz"

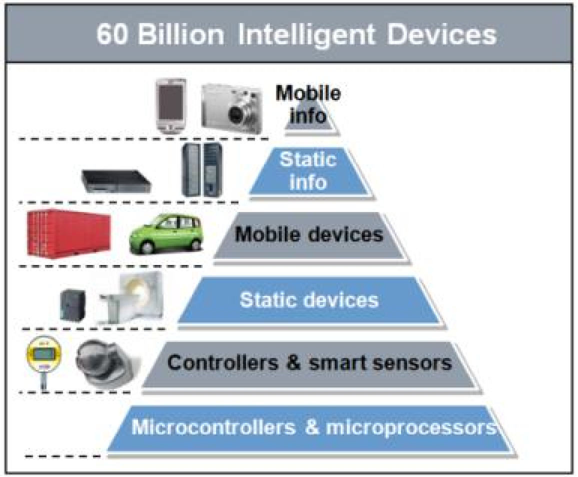
Data sources:
IBM X-Force Trend and Risk Report
HP Cyber Risk Report
Symantec Intelligence Report

Different factors are driving the research demand for IT Security

New Functionality and Architectures

Examples

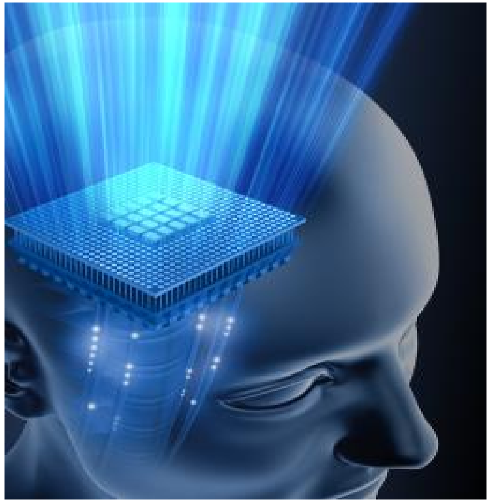
- Connectivity of devices and systems to public networks
- IP to the field
- Use of mobile devices


60 Billion Intelligent Devices
Mobile info
Static info
Mobile devices
Static devices
Controllers & smart sensors
Microcontrollers & microprocessors

Security Use Case

Examples

- Know-how protection
- Licensing



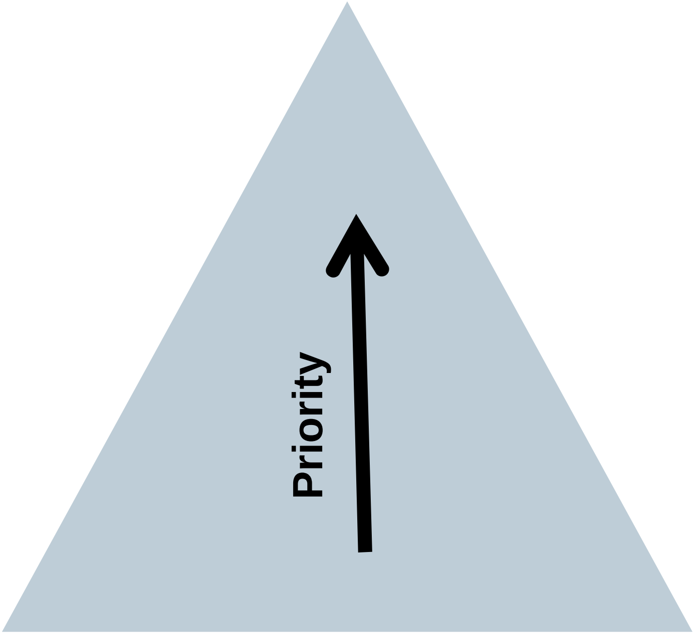
Quality of Security

Examples

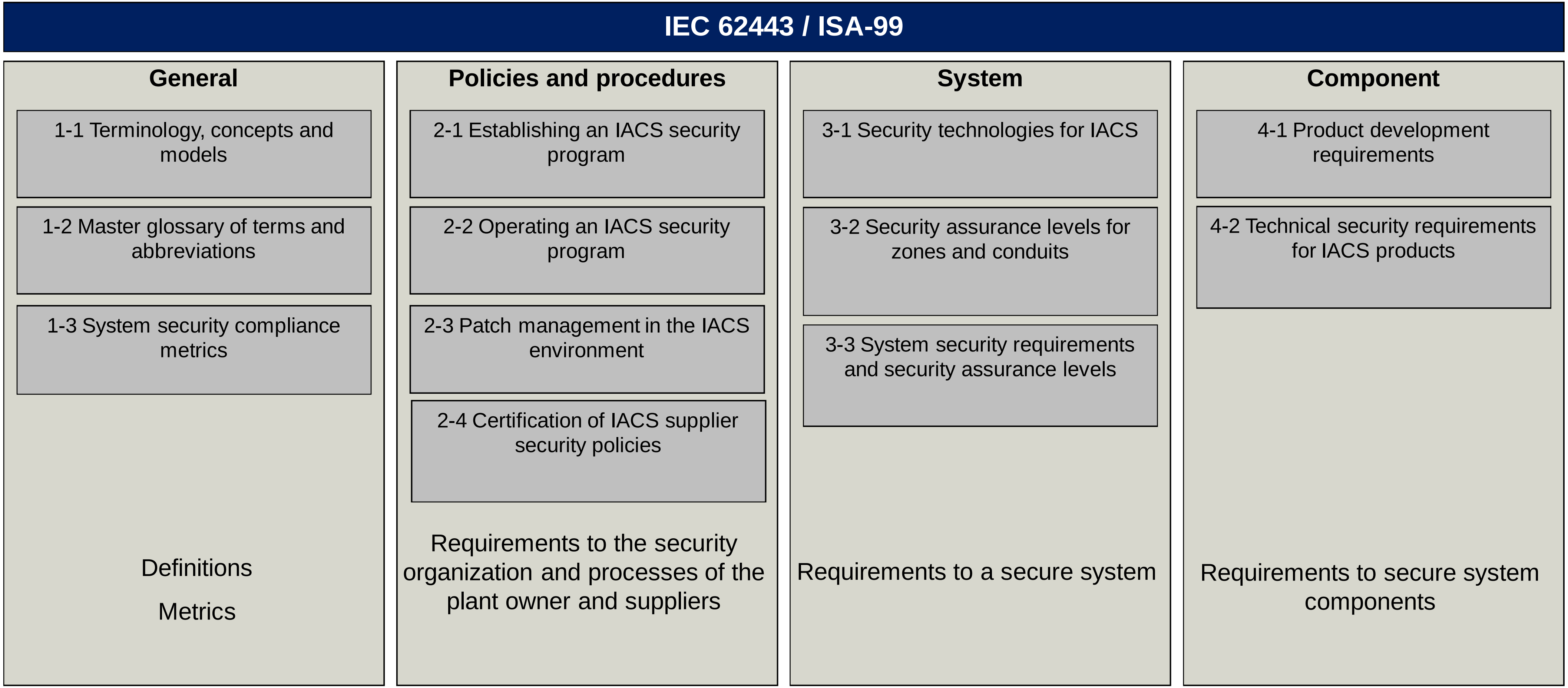
- Robust
- Easy to use
- Long term security

The CIA pyramid is turned upside down in industrial automation and control systems

Industrial Automation and Control Systems	Office IT Systems
Availability	Confidentiality
Integrity	Integrity
Confidentiality	Availability



ISO/IEC 62443 Covers Security Management, System and Component Level for Industrial Automation Control Systems (IACS)

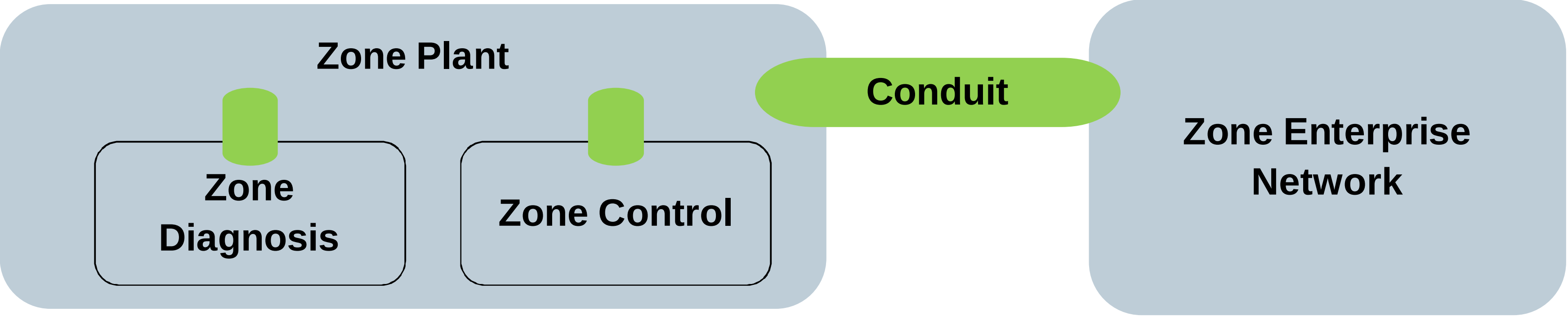


IEC 62443 / ISA-99

General	Policies and procedures	System	Component
1-1 Terminology, concepts and models	2-1 Establishing an IACS security program	3-1 Security technologies for IACS	4-1 Product development requirements
1-2 Master glossary of terms and abbreviations	2-2 Operating an IACS security program	3-2 Security assurance levels for zones and conduits	4-2 Technical security requirements for IACS products
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security assurance levels	
	2-4 Certification of IACS supplier security policies		
Definitions Metrics	Requirements to the security organization and processes of the plant owner and suppliers	Requirements to a secure system	Requirements to secure system components

Security levels provide for protection against different attack levels

Zones and Conduits



Zone Plant

Zone Diagnosis

Zone Control

Conduit

Zone Enterprise Network

The targeted security level is determined by a threat and risk analysis

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, IACS specific skills, moderate motivation
SL4	Protection against intentional violation using sophisticated means, extended resources, IACS specific skills, high motivation

Security Standard ISO/IEC 62443-3.3 defines security requirements for industrial control systems

SIEMENS

7 Foundational Requirements

FR 1 – Identification and authentication control

FR 2 – Use control

FR 3 – System integrity

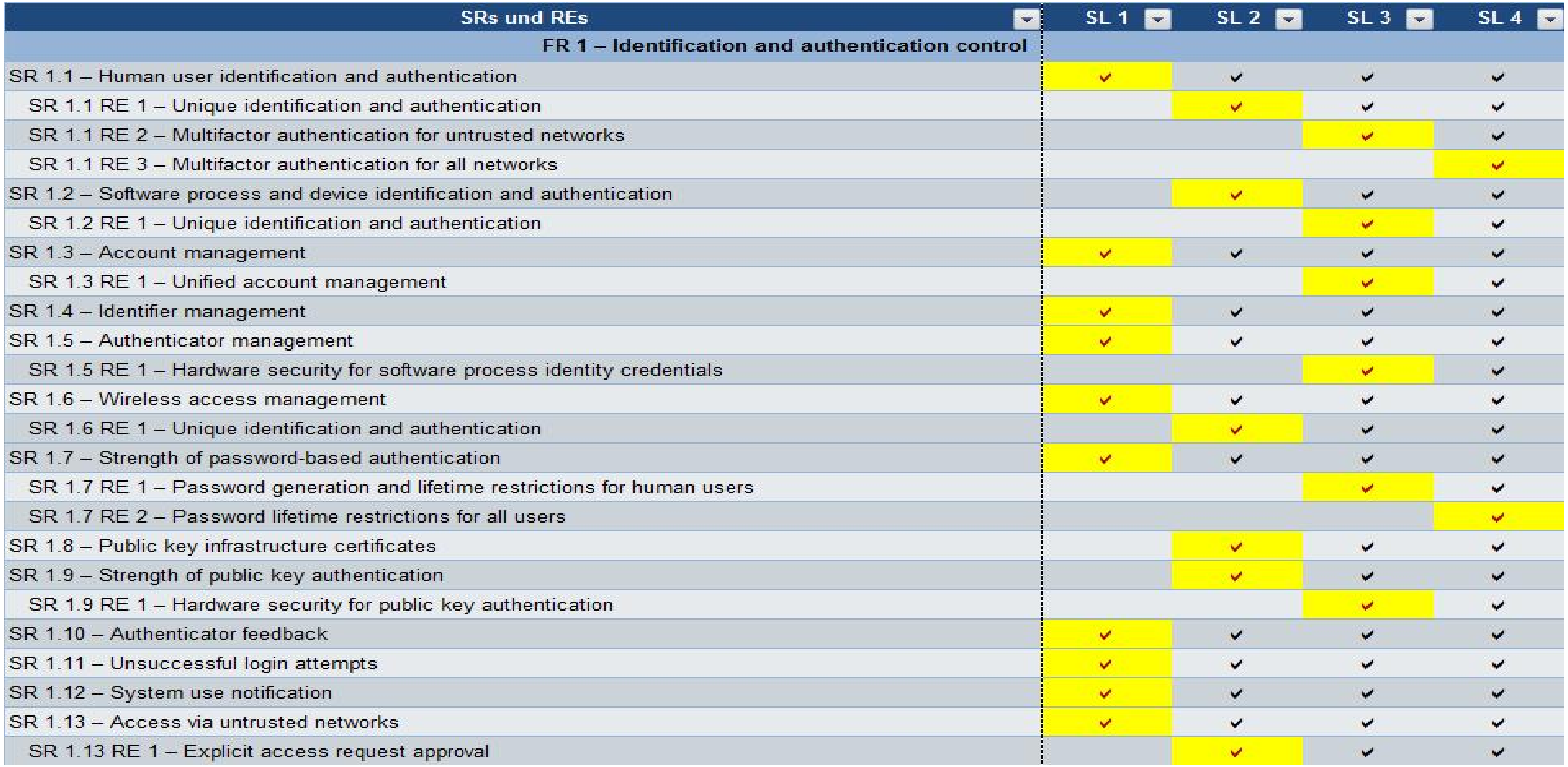
FR 4 – Data confidentiality

FR 5 – Restricted data flow

FR 6 – Timely response to events

FR 7 – Resource availability

Example: System requirements (SR) and requirement extensions (RE) for foundational requirement FR1 “Identification and authentication control”

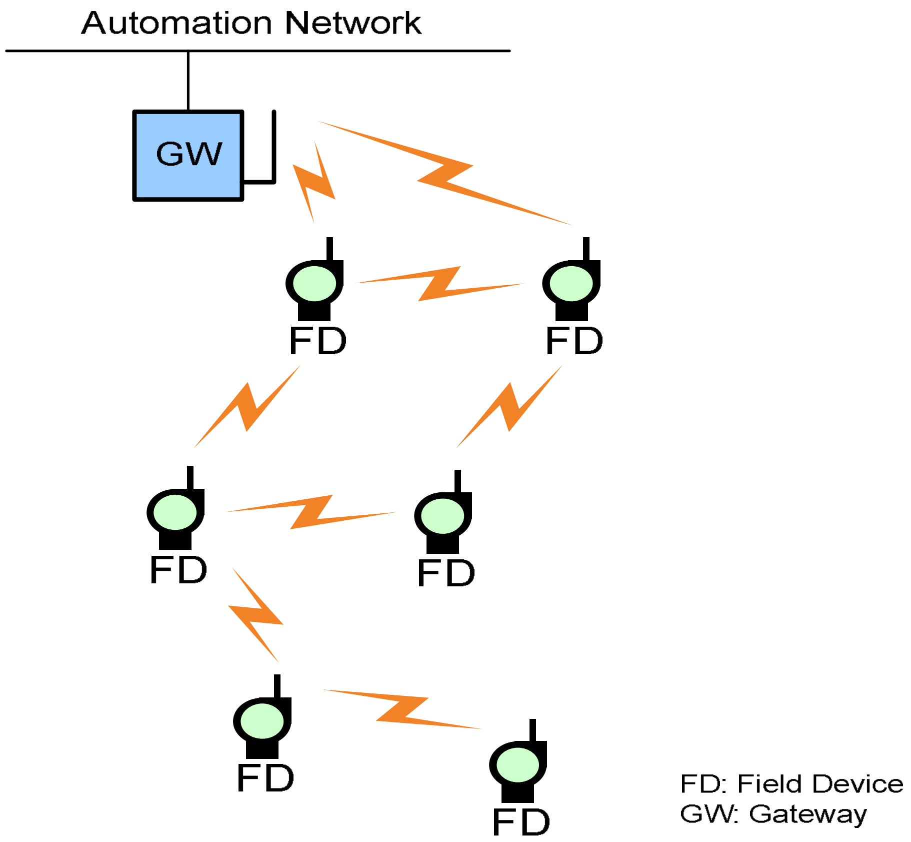


SRs und REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentication		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentication for untrusted networks			✓	✓
SR 1.1 RE 3 – Multifactor authentication for all networks				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
SR 1.2 RE 1 – Unique identification and authentication			✓	✓
SR 1.3 – Account management	✓	✓	✓	✓
SR 1.3 RE 1 – Unified account management			✓	✓
SR 1.4 – Identifier management	✓	✓	✓	✓
SR 1.5 – Authenticator management	✓	✓	✓	✓
SR 1.5 RE 1 – Hardware security for software process identity credentials			✓	✓
SR 1.6 – Wireless access management	✓	✓	✓	✓
SR 1.6 RE 1 – Unique identification and authentication		✓	✓	✓
SR 1.7 – Strength of password-based authentication	✓	✓	✓	✓
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users			✓	✓
SR 1.7 RE 2 – Password lifetime restrictions for all users				✓
SR 1.8 – Public key infrastructure certificates		✓	✓	✓
SR 1.9 – Strength of public key authentication		✓	✓	✓
SR 1.9 RE 1 – Hardware security for public key authentication			✓	✓
SR 1.10 – Authenticator feedback	✓	✓	✓	✓
SR 1.11 – Unsuccessful login attempts	✓	✓	✓	✓
SR 1.12 – System use notification	✓	✓	✓	✓
SR 1.13 – Access via untrusted networks	✓	✓	✓	✓
SR 1.13 RE 1 – Explicit access request approval		✓	✓	✓

Example: Wireless sensor network

Purpose: Obtain accurate sensing information (not data communication)

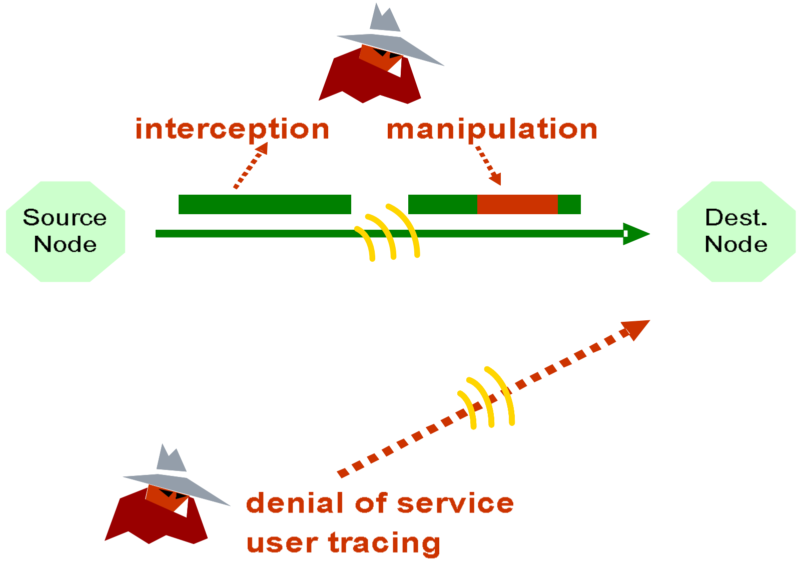
- nodes often battery powered or energy harvesting
- wireless communication (low bandwidth)
- nodes may be static or mobile
- small to large number of nodes
- often severely limited resources: processing, memory, bandwidth



Security threats for wireless sensor networks

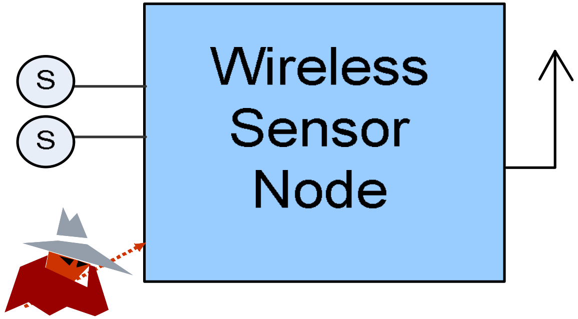
Attacks against wireless communication:

- manipulation, interception, replay, user privacy, repudiation
- DoS, sleep deprivation, routing security
- traffic flow analysis

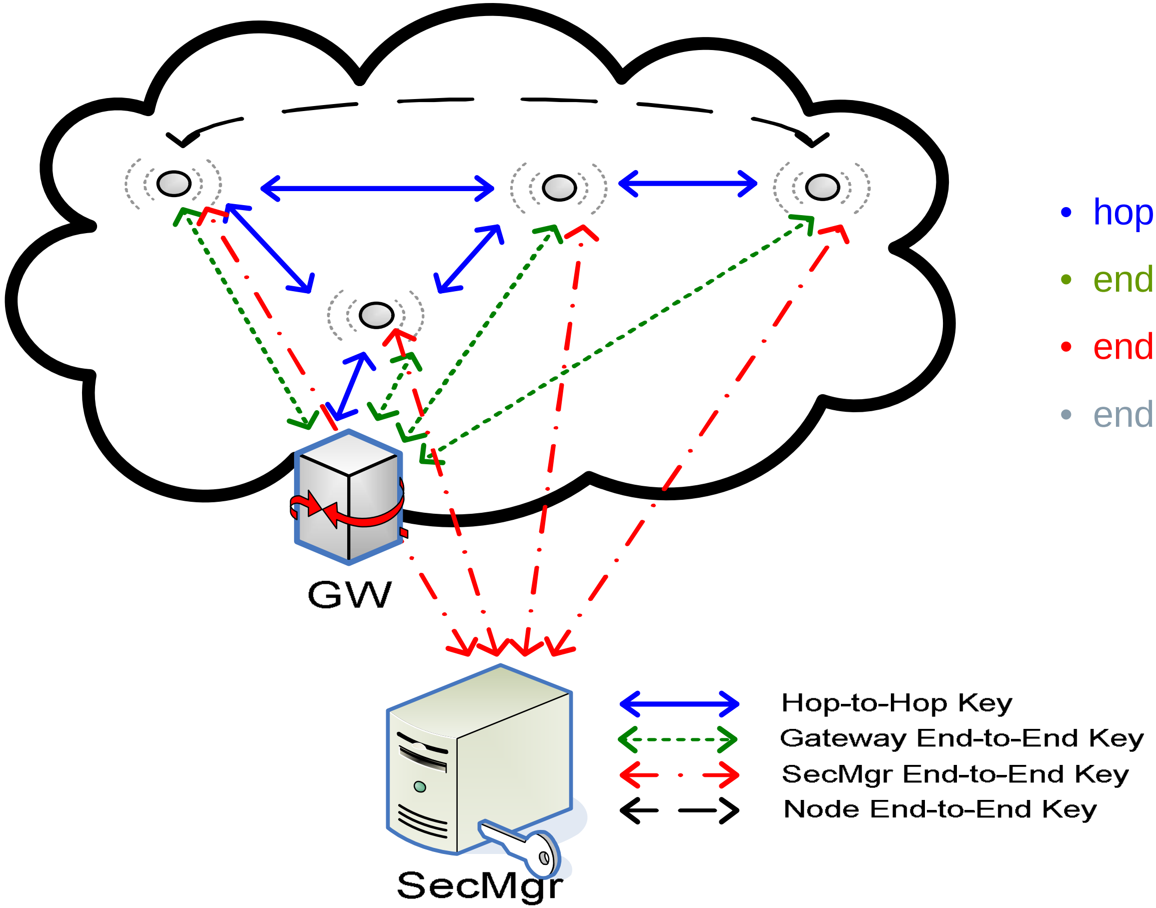


Attacks against sensor node

- tampering (physical attacks)
- Reverse engineering
- node capture, node theft, node relocation

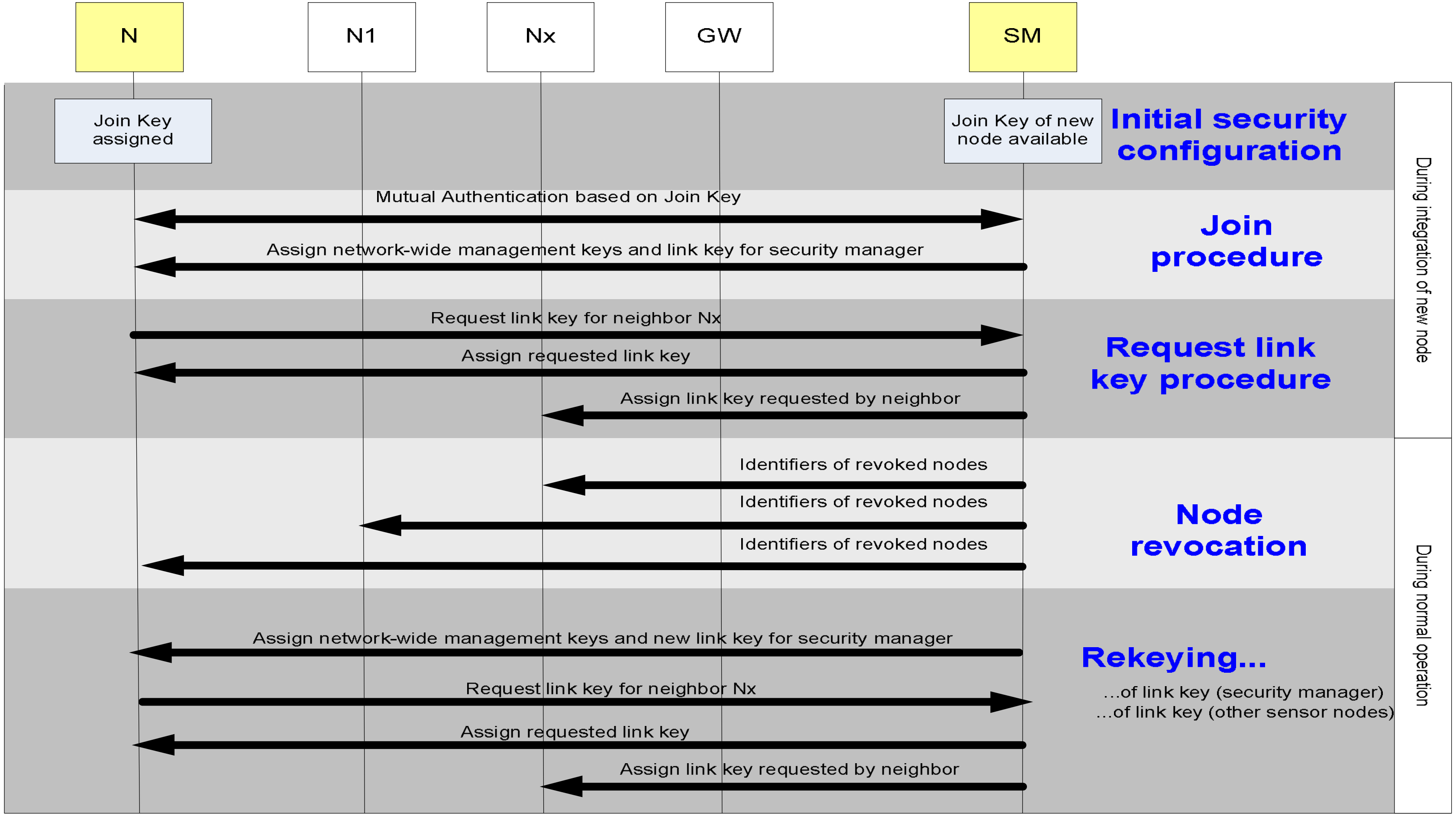


Several session keys are established by the security manager based on a single join key



- hop-to-hop key (network key)
- end-to-end key with gateway(s)
- end-to-end key with security manager
- end-to-end keys with other nodes

Overview security-related signaling

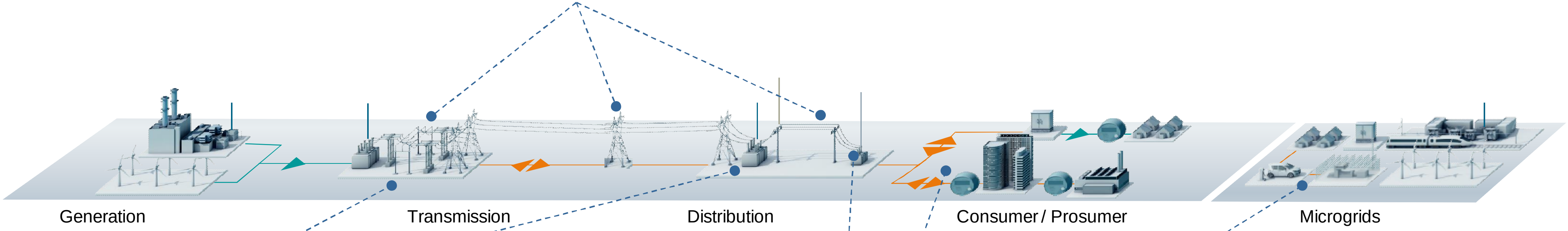

N
N1
Nx
GW
SM
Join Key assigned
Join Key of new node available
Initial security configuration
Mutual Authentication based on Join Key
Assign network-wide management keys and link key for security manager
Join procedure
Request link key for neighbor Nx
Assign requested link key
Assign link key requested by neighbor
Request link key procedure
During integration of new node
Identifiers of revoked nodes
Identifiers of revoked nodes
Identifiers of revoked nodes
Node revocation
Assign network-wide management keys and new link key for security manager
Rekeying...
...of link key (security manager)
...of link key (other sensor nodes)
Request link key for neighbor Nx
Assign requested link key
Assign link key requested by neighbor
During normal operation

Example: Smart Grid

Secure Communication supports reliable operation

2

- Power Quality Monitoring and Eventing (Transmission/Distribution, Substation)
- Communication Standards used: IEC 61850 (GOOSE)
- Security uses group- based security integrated in GOOSE (IEC 62351-6)



1

- Substation Automation (Telecontrol and Monitoring)
- Inter Control Center Communication
- Communication Standards used:
  IEC 60870-5-104, IEC 61850
- Remote Service
- Transport level security through TLS
  (IEC 62351-3/4/5)
- Application level security through X.509 based authentication + integrity. (IEC 62351-4)

4

- Connecting electric vehicles to the charging infrastructure
- Communication Standards used:
  ISO/IEC 15118, IEC 61850
- Transport level security: TLS
- Application level security: XML Dig.Sig.

3

- DER Integration (Metering & Control)
- Communication Standards used: IEC 61850, XMPP (future use)
- Transport level security through TLS (IEC 62351-3/4/5)

Example IEC 15118: eCar charging security

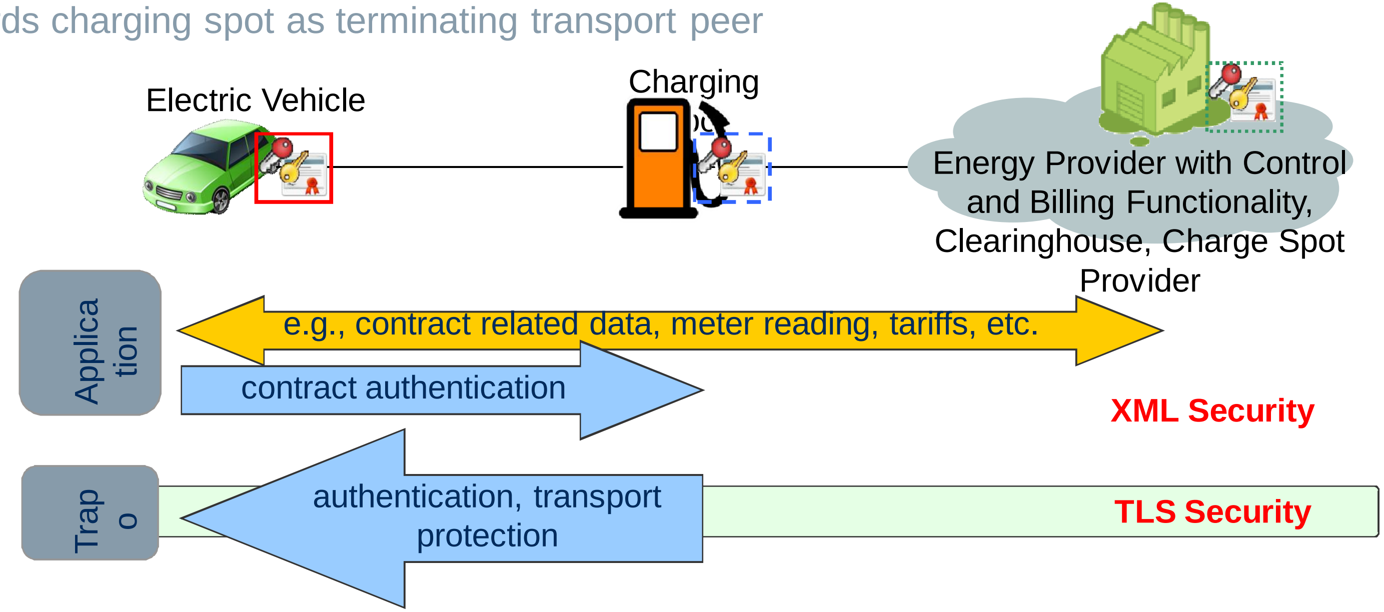
Securely connecting the vehicle to the smart grid

Standard for the interface between vehicle and charging station supporting

- Connection of vehicles to the power grid
- Billing of consumed energy (charging)
- Roaming of electric vehicles between different charging spot
- Value added services (e.g., software updates)

Trust Relations from the electric vehicle

- Towards backend (energy provider) for signed meter readings and encrypted information (e.g., tariff)
- Towards charging spot as terminating transport peer



Electric Vehicle

Charging

Energy Provider with Control and Billing Functionality, Clearinghouse, Charge Spot Provider

Applica tion

e.g., contract related data, meter reading, tariffs, etc.

contract authentication

XML Security

Trap o

authentication, transport protection

TLS Security

IEC 15118 – Approach based on certificates and corresponding private keys (PKI)

Approach

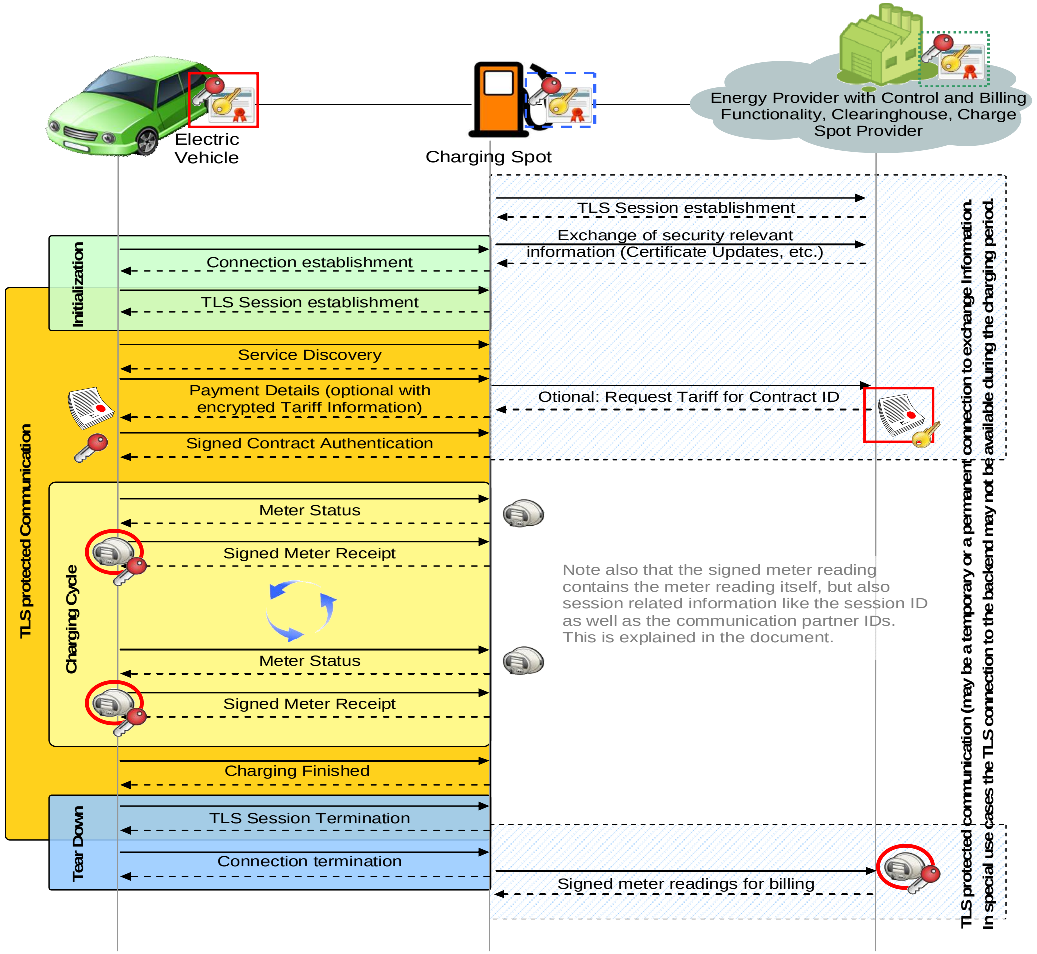
- Transport Layer Security to protect exchange between vehicle and EVSE
- Application layer security using XML security for data exchange with the backend

Credentials

- Public/private key pair incl. certificate

Connectivity

- Online and Semi-online to the backend
- Persistent connection between vehicle and EVSE during charging to exchange charging process relevant information, especially a cyclic exchange of metering data for provided energy



Electric Vehicle

Charging Spot

Energy Provider with Control and Billing Functionality, Clearinghouse, Charge Spot Provider

TLS protected Communication

Initialization

Connection establishment

TLS Session establishment

Service Discovery

Payment Details (optional with encrypted Tariff Information)

Signed Contract Authentication

Charging Cycle

Meter Status

Signed Meter Receipt

Meter Status

Signed Meter Receipt

Charging Finished

Tear Down

TLS Session Termination

Connection termination

TLS Session establishment

Exchange of security relevant information (Certificate Updates, etc.)

Otional: Request Tariff for Contract ID

Note also that the signed meter reading contains the meter reading itself, but also session related information like the session ID as well as the communication partner IDs. This is explained in the document.

Signed meter readings for billing

TLS protected communication (may be a temporary or a permanent connection to exchange information.

In special use cases the TLS connection to the backend may not be available during the charging period.

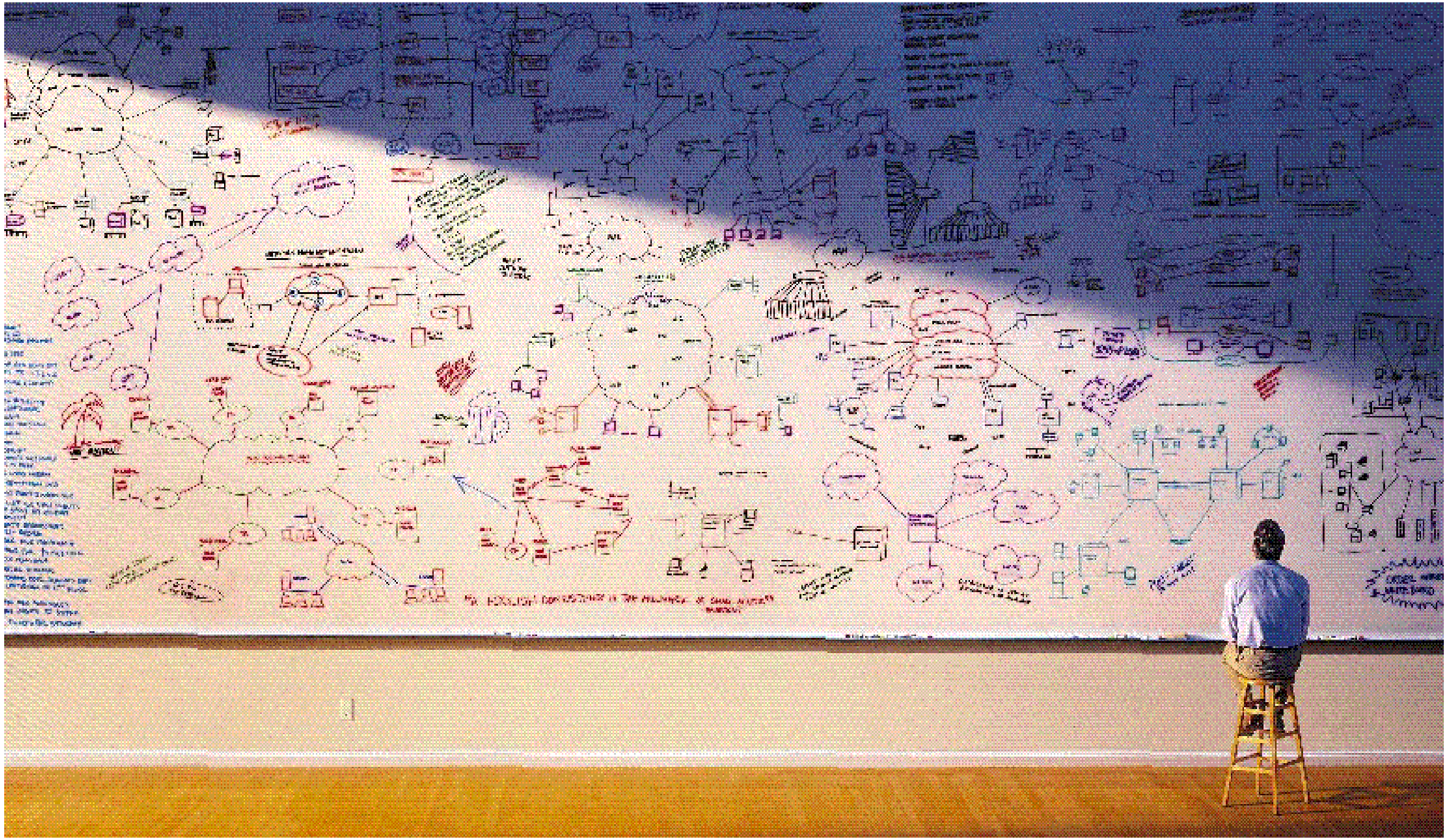
Security has to be suitable for the addressed environment

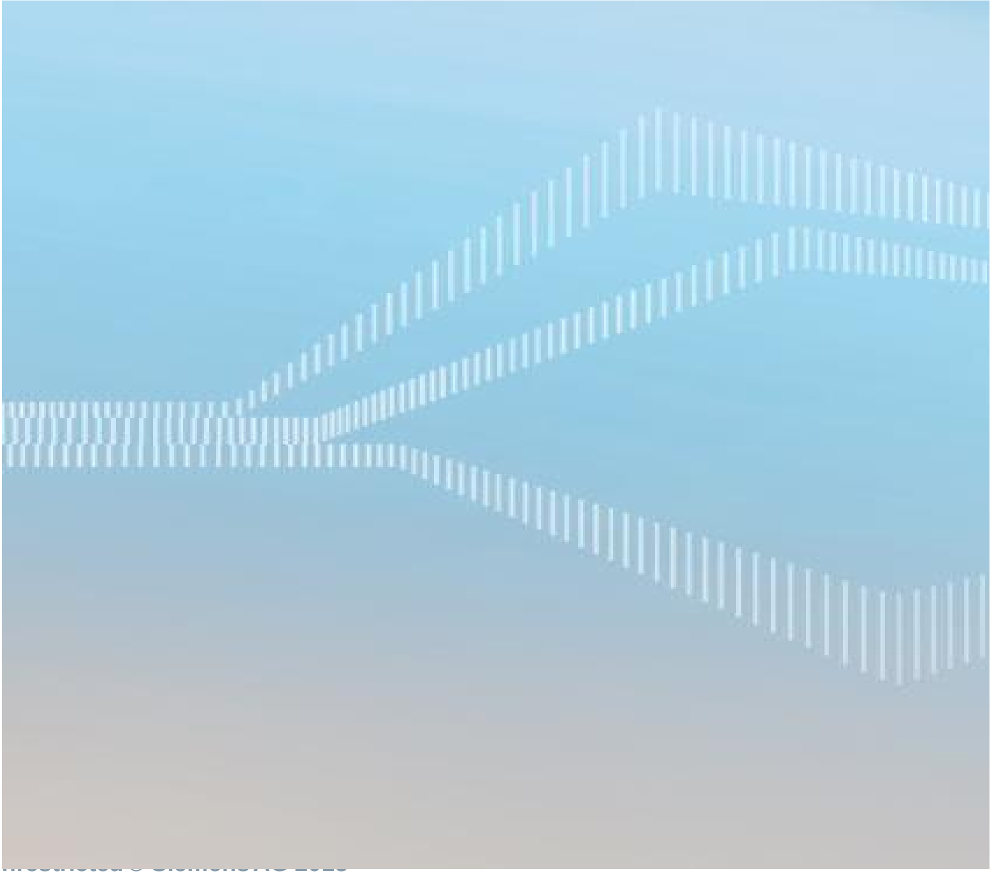
Awareness and Acceptance

Since security is not just a technical solution, which can be incorporated transparently, we need to consider how humans can get along with this issue. This needs actions for:

- awareness trainings
- help people to understand security measures and processes
- provide user friendly interfaces and processes

Thank you for your attention!





Dr.
Rainer Falk
Principal Key Expert

Siemens AG
Corporate Technology
IT Security
CT RTC ITS
Otto-Hahn-Ring 6
D-81200 Munich
Germany

rainer.falk@siemens.com