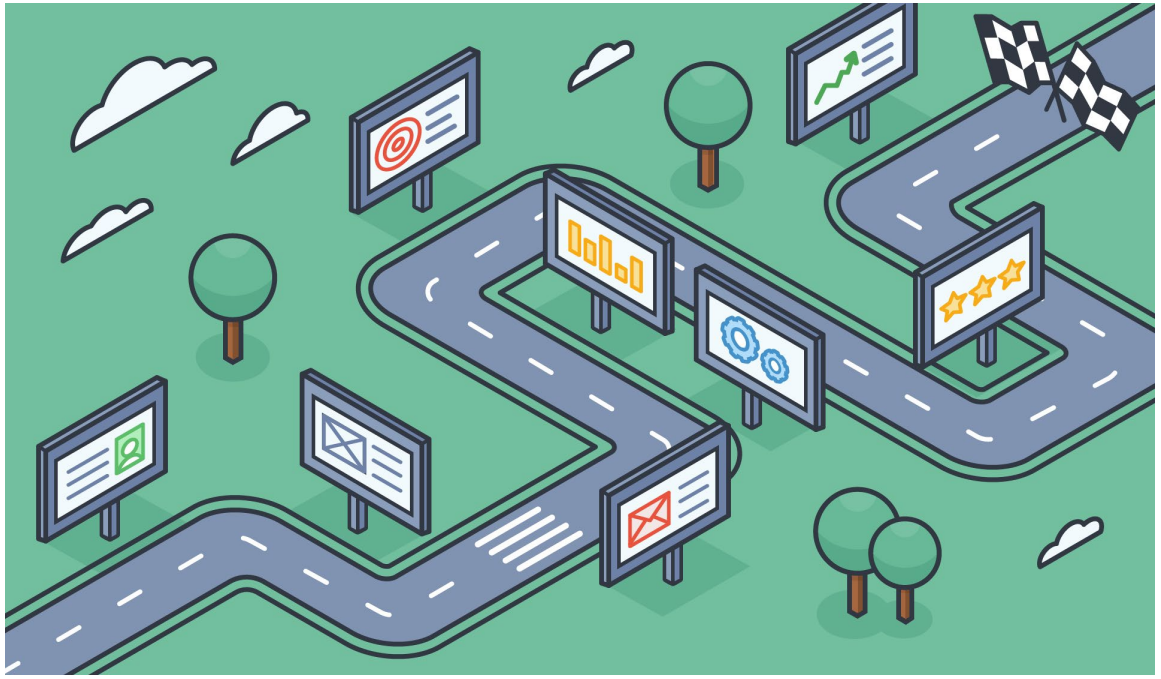
Smart Buildings
Understanding the Value of Intelligent Infrastructures

Agenda

SIEMENS
Ingenuity for life

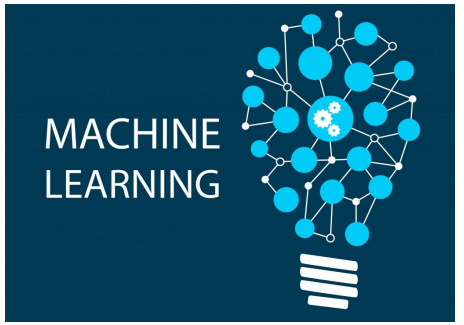


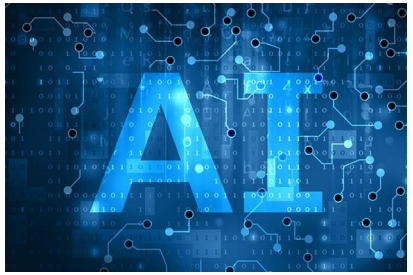
- Definition, Buzz Words
- Why are we talking about it?
- Where are we now?
- Where are we going?
- Security Concerns
- Value add for stakeholders

Definitions and Buzz Words

SIEMENS
Ingenuity for life

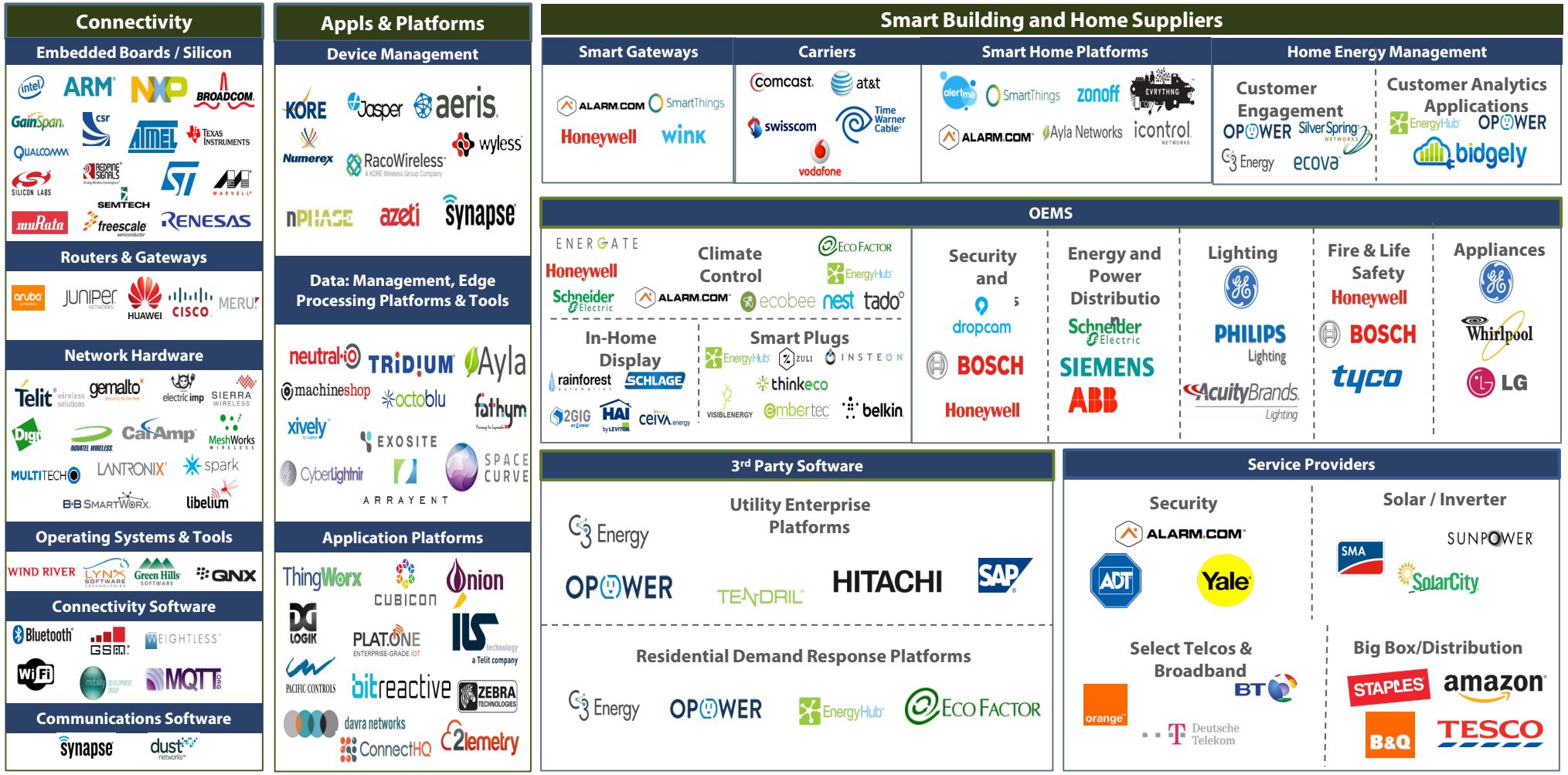
A definition, coined by the **Intelligent Buildings Institute**, defines an **intelligent building** as "*one which provides a productive and cost-effective environment through optimization of four basic elements: structure, systems, services and management, and the interrelationship between them*."





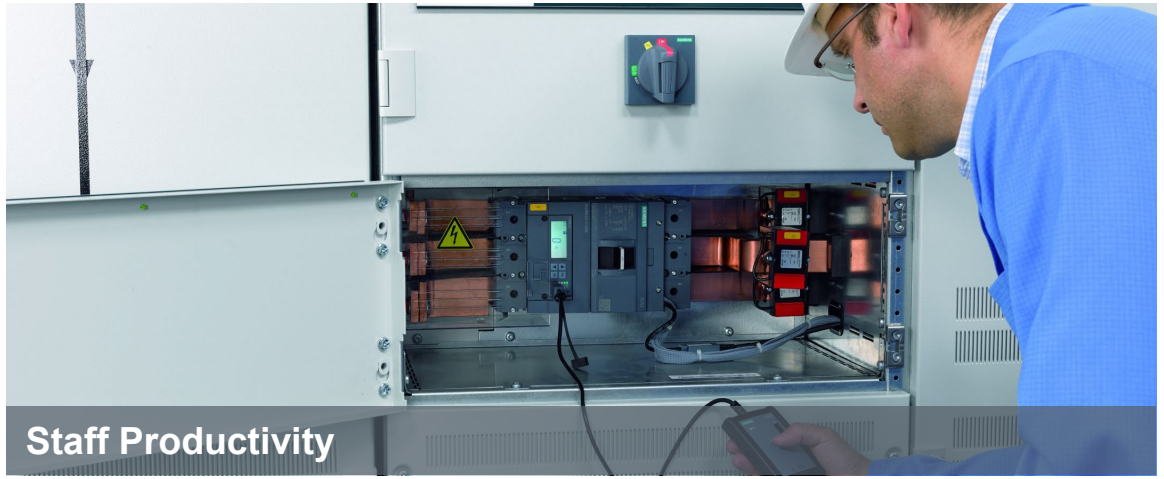
What's out there?

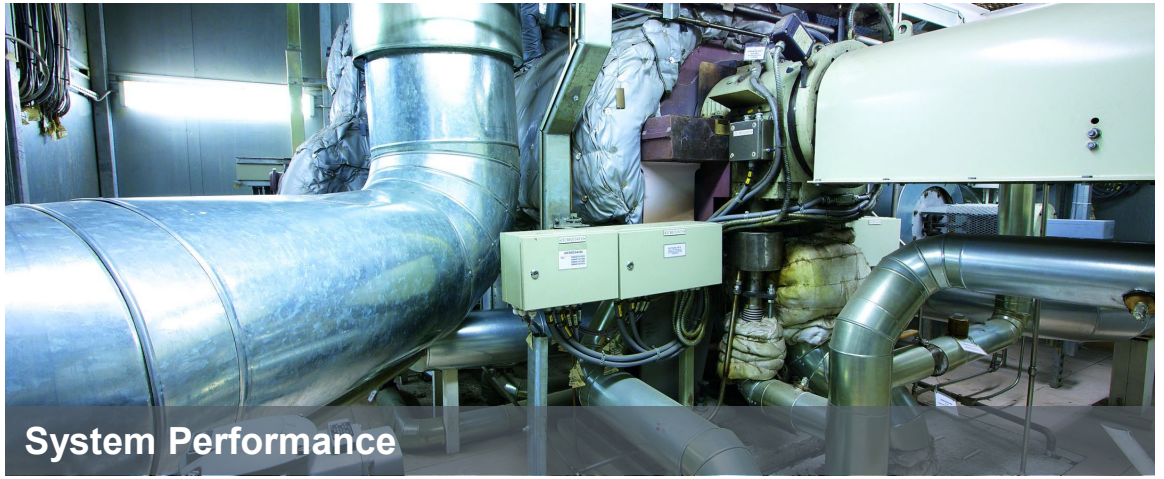
SIEMENS
Ingenuity for life



Today's Challenges

SIEMENS
Ingenuity for life

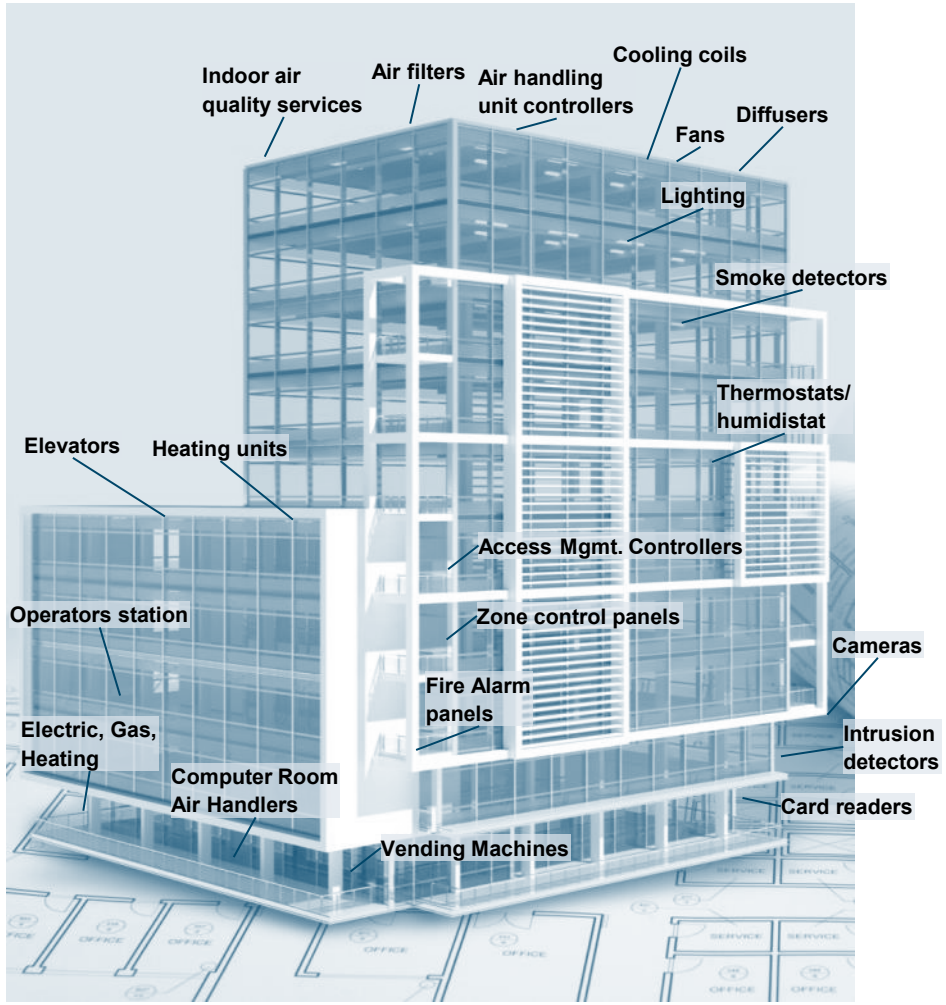




The interests of building stakeholders

The growing digital infrastructure of buildings needs a firm foundation

SIEMENS
Ingenuity for life



The number and complexity of building systems we have to manage keeps growing.

My team needs a common interface that communicates off-normal conditions, consistently, from all building systems

We are anticipating the retirement of our most experienced team members. I need to get new employees up to speed quickly, with reduced complexity of many systems

I'm excited about the promise of analytics. I want to consolidate all the building systems data and get the right stuff analyzed because the pool of local expertise is shrinking

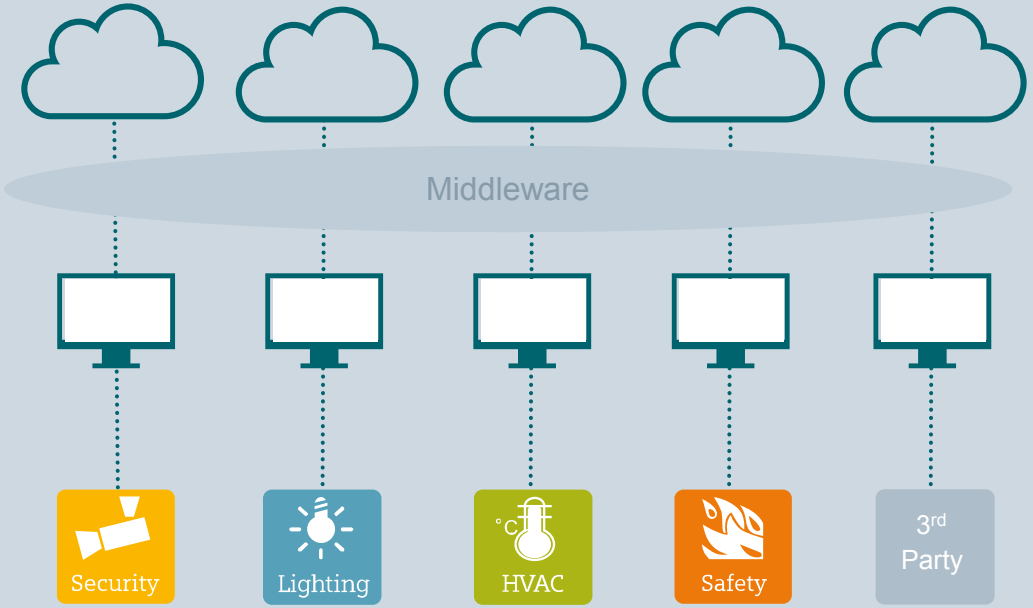
Open, integrated ecosystem leverages the power of data

SIEMENS
Ingenuity for life

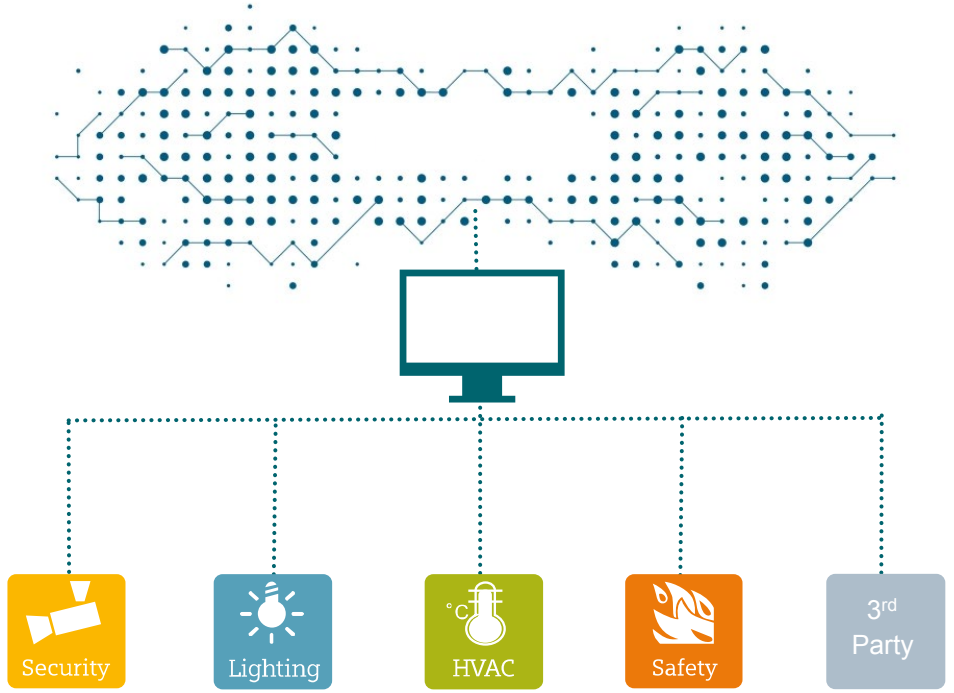
Today
Separate system control increases installation and operating costs and limits connectivity and use of data.

Tomorrow
An open, integrated ecosystem with all systems connected via an integrated building management system, fully leveraging the power of data to drive business outcomes . Results in **lower capital and operating expenditures** and **enhanced capabilities**.

Closed, multi-system architecture



Open, integrated ecosystem



Putting Data to Work

SIEMENS
Ingenuity for life

Use Cases…Meat and Potatoes

SIEMENS
Ingenuity for life

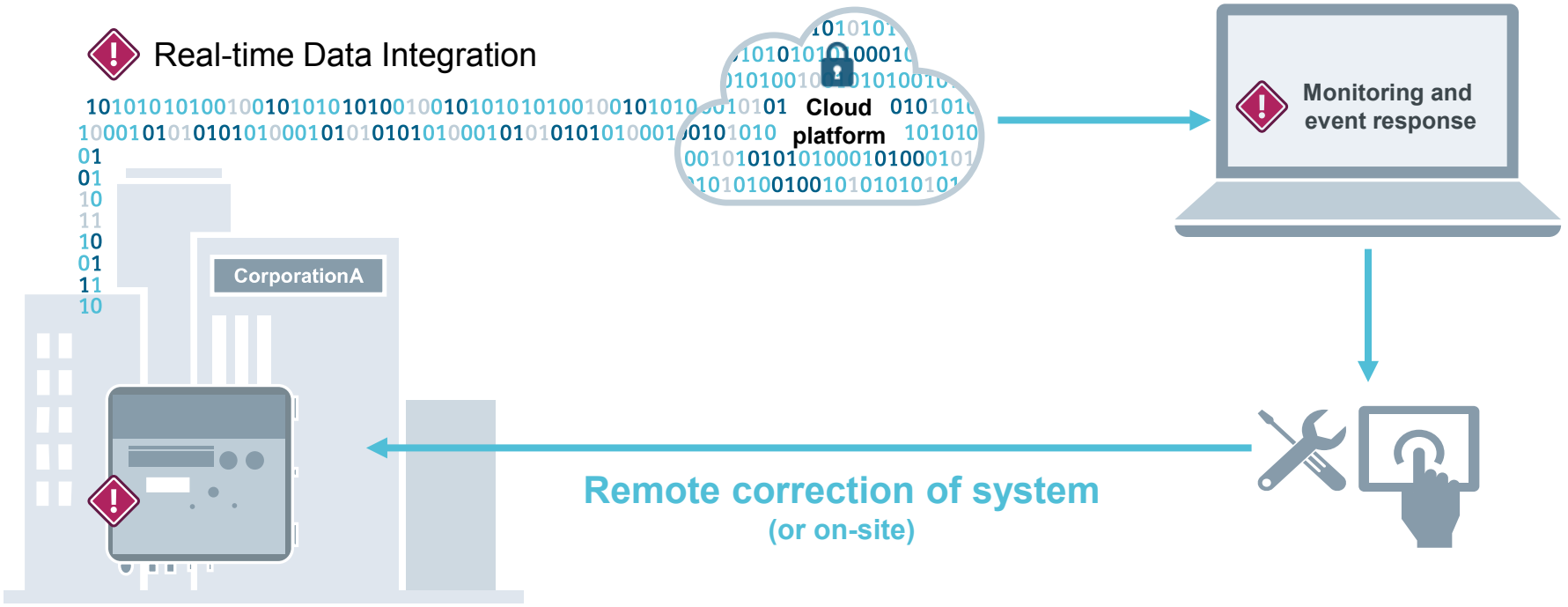
- Lighting/HVAC Occupancy Based
- Life Safety and Mass Notification, Smoke Control
- Video Surveillance and Intrusion Detection
- Asset Tracking and Parking Spaces, Desk Assignments, Conference Room Scheduling.
- Fire Systems and Elevator Recall
- Heat Mapping and Lighting/HVAC Operation
- Analytics and Predictive Maintenance
- Power over Ethernet
- What Else????

Optimal building performance through data analytics

SIEMENS
Ingenuity for life

Today
Faults are only identified during maintenance visits or when equipment fails, resulting in wasted energy and/or system downtime.

Tomorrow
With an advanced analytics platform, systems can be continuously monitored and facility improvement measurements can be implemented before failures occur, resulting in **energy savings, improved uptime** and **extended equipment life**.



Digital Service Center

- Data analysis
- Energy reports
- Identification of abnormal energy consumption
- Information is sent to local service organization

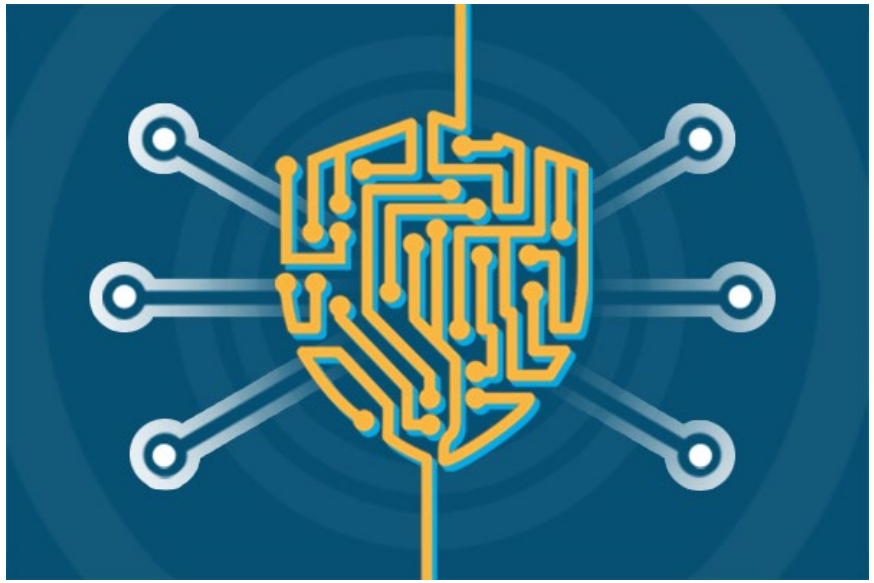
Remote Resolution & Facility Manager Issue Communication

- Remote analysis
- Options identified/communicated for resolution

Definition

SIEMENS
Ingenuity for life

Industry Definition of Cyber Security:



Source: Cisco Security

cyber security

is the practice of protecting systems, networks, and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Types of cyber security threats

SIEMENS
Ingenuity for life

Ransomware	• A type of malicious software. • It is designed to extort money by blocking access to files or the computer system until the ransom is paid.
Malware	• A type of software designed to gain unauthorized access or to cause damage to a computer.
Social Engineering	• A tactic that adversaries use to trick you into revealing sensitive information. • Can solicit a monetary payment or gain access to your confidential data.
Phishing	• The practice of sending fraudulent emails that resemble emails from reputable sources. • Aim is to steal sensitive data like login information, credit card numbers, etc. The most common type of cyber attack.

Cyber Security – Who is involved?

SIEMENS
Ingenuity for life

Setting the Standard for Automation™

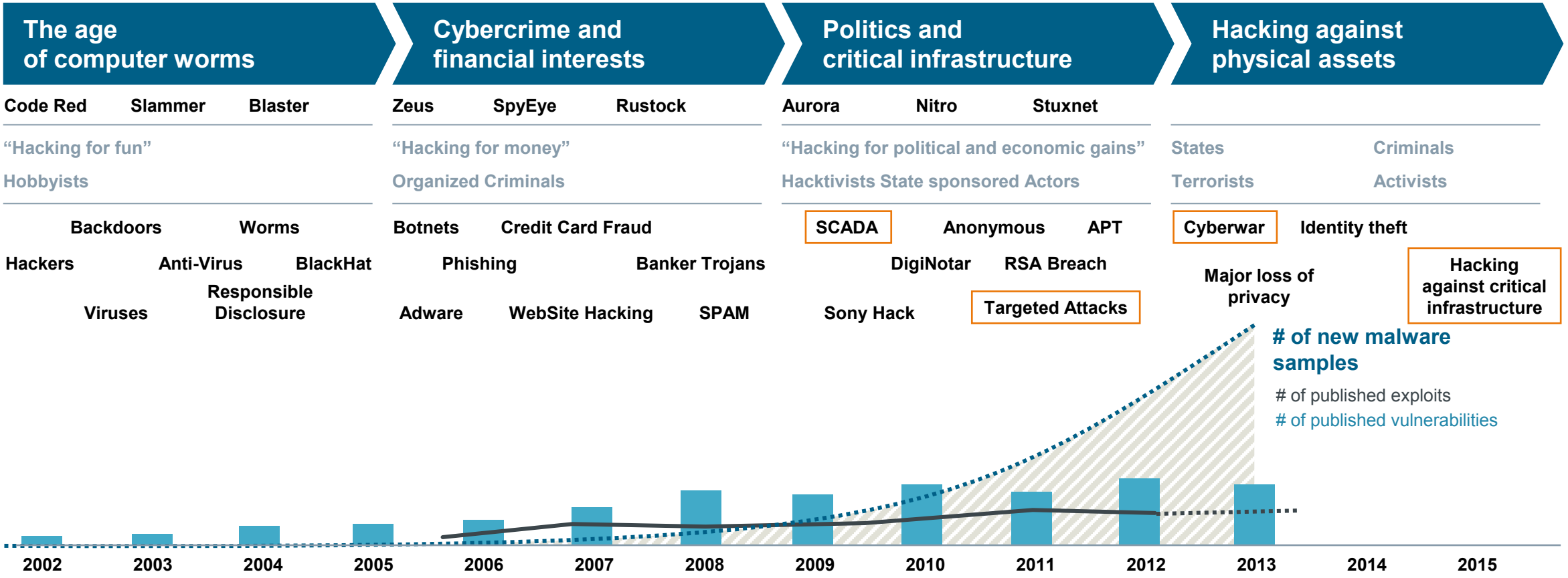
Key Involvement

- International Society of Automation (ISA)
- International Electrotechnical Commission (IEC)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- US Dept. of Energy (USDOE)
- Department of Homeland Security (DHS)
- Other Federal, states and private authorities.

The threat level is rising – Attackers are targeting critical infrastructures

SIEMENS
Ingenuity for life

Evolution of attacker motives, vulnerabilities and exploits



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

Implications –
What happens if technical vulnerabilities not known by asset owner?

SIEMENS
Ingenuity for life

Monetary and reputational damage

Loss of security goals:
Confidentiality/integrity/availability

Worst case scenarios triggered disrupting the business

Shut down of facility infrastructure

Customers break out of contained environments in datacenter targeting other customers or facility infrastructure

Physical and logical access control break

- **What happens if the remote access is not really secure?**
- **Do access control systems really prevent attackers from accessing the building?**
- **Is customer's IT really separated from facility IT?**

Essential to know own risks, threats and vulnerability for facility IT

Top 10 cyber security threats 2014 – Control system security

SIEMENS
Ingenuity for life

#	Top 10 security threats (2014)	Exposure	Detection
1	Malware Infection via Internet and Intranet	High	Difficult
2	Introduction of Malware on Removable Media and External Hardware	High	Difficult
3	**Social Engineering**	**High**	**Moderate**
4	Human Error and Sabotage	High	Difficult
5	Intrusion via Remote Access	Moderate	Difficult
6	**Control Components Connected to the Internet**	**High**	**Difficult**
7	Technical Malfunctions and Force Majeure	High	Easy
8	**Compromising of Smartphones in the Production Environment**	**Moderate**	**Difficult**
9	**Compromising of Extranet and Cloud Components**	**Moderate**	**Difficult**
10	(D)DoS Attacks	High	Easy

Source: Federal office for information security, Germany

New listed by 2014

Exposure

How easily can the vulnerability be located and reached?

Detection

How easily can a compromising action be detected?

Pentest: What is a penetration test? What are its goals?

SIEMENS
Ingenuity for life

A penetration test, or sometimes called pentest or "friendly hacking test", helps to reveal security weaknesses, that allow to gain access to the computer's and data, possibly disrupting the business

- Attacker perspective
- Simulate a skilled attacker
- Worst-Case-Scenario-driven (not control-driven)
- Cover complete attack surface

The goals of penetration tests are

- Determine **feasibility** of a particular set of attack vectors
- **Identify high-risk vulnerabilities** from a combination of lower-risk vulnerabilities exploited in a particular sequence
- **Identify vulnerabilities** that may be difficult or **impossible to detect with automated network or application vulnerability scanning** software
- **Assess** the **magnitude of** potential business and operational **impacts** of successful attacks
- **Test the ability of network defenders** to detect and respond to attacks
- **Provide evidence** to support increased investments in security personnel and technology

Source: https://en.wikipedia.org/wiki/Penetration_test

What is not goal/part of a Pentest?

Root cause analysis, vulnerability fixing/remediation support

Overall business threat and risk analysis

Complete software security tests (e.g. not including binary reversing, protocol fuzzing, source code analysis)

Assessment of IS processes (e.g. ISO, PCI DSS)

Social engineering attack

Penetration test – Benefits

SIEMENS
Ingenuity for life

Limit the chance that worst case scenarios can be triggered by a malicious attacker

Efficiently finding vulnerabilities that really matter and must be addressed first

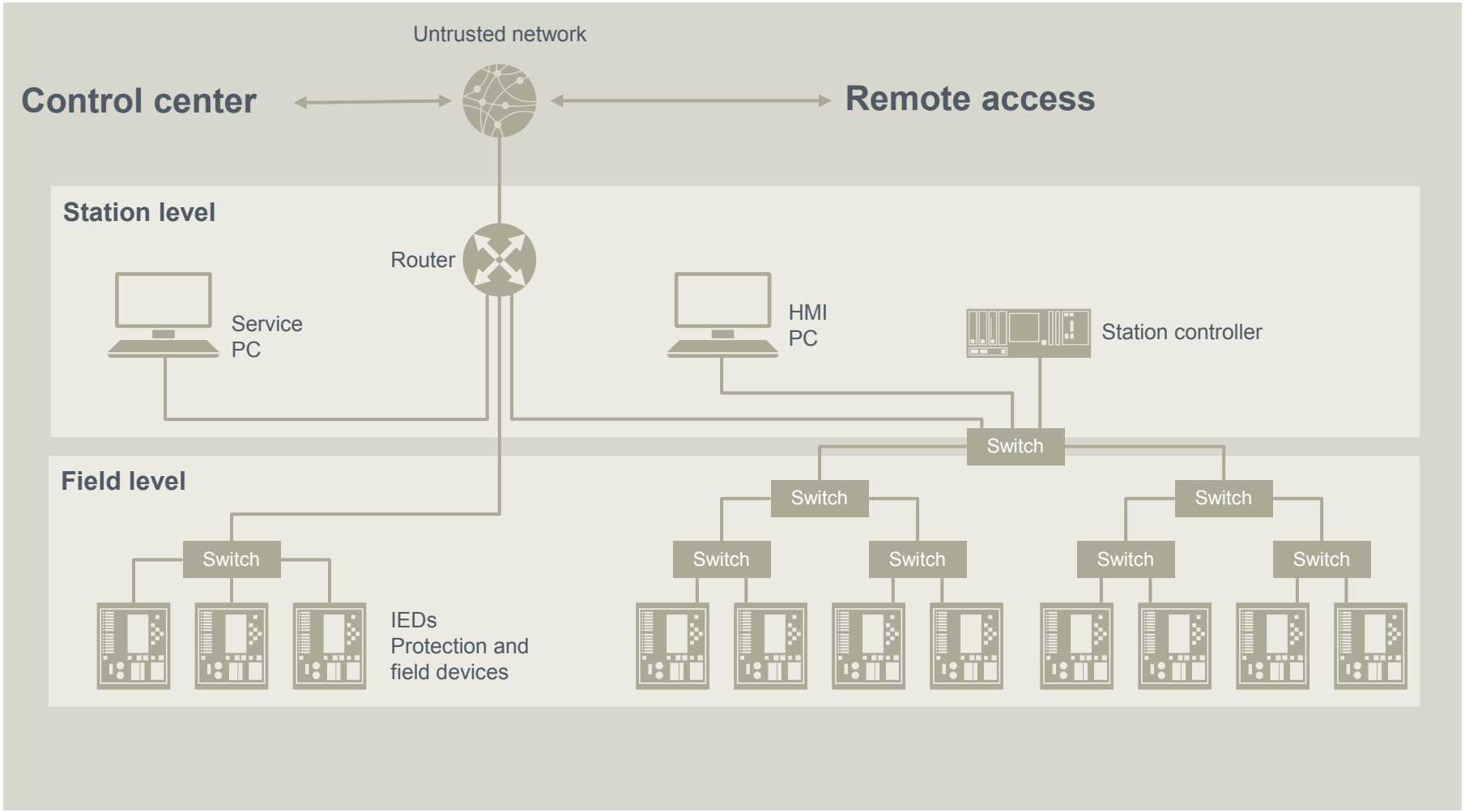
Highly customizable to simulate different attacker types (script kiddie up to professional attacker)

Simulation of insider attackers, attackers from the Internet, attacks originating from data center customer's IT infrastructures

Starting point for further security activities

Example: Digital Substations are vulnerable to Cyber Attacks Conditions

SIEMENS
Ingenuity for life

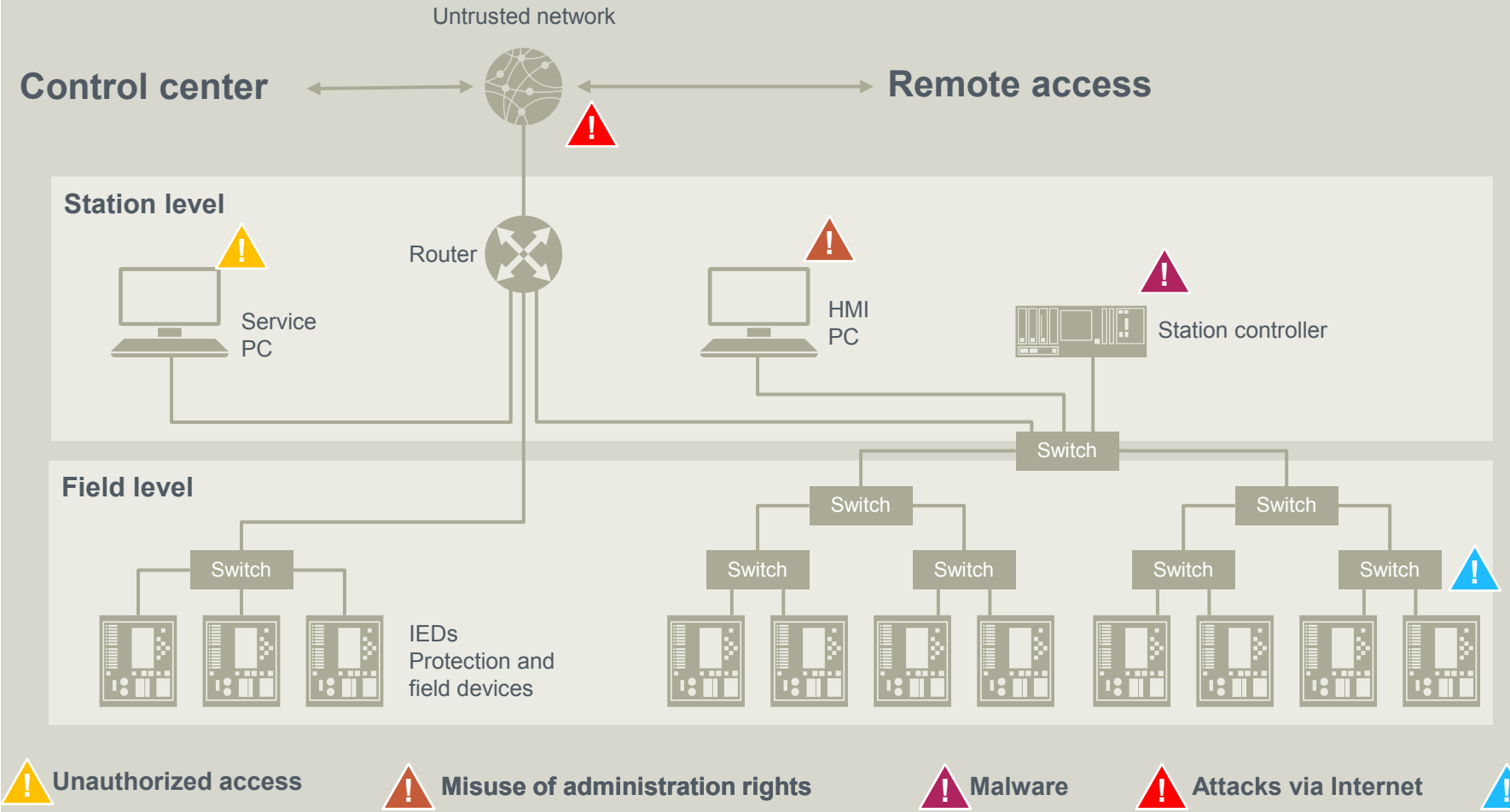


Conditions:

- Critical Infrastructure
- 24 h Operation
- Windows and Linux standard components
- Interfaces to unsecure networks
- Interfaces to office networks
- Legacy components
- Proprietary technology
- Mix of components from different vendors with different technologies

Example: Digital Substations are vulnerable to Cyber Attacks
Possible Threats and Attackers

SIEMENS
Ingenuity for life



Possible Attackers:

- States
- Criminal Organizations
- Script Kiddies
- Insider

Security is a must for Digital Substations Covers all Cyber Security Aspects

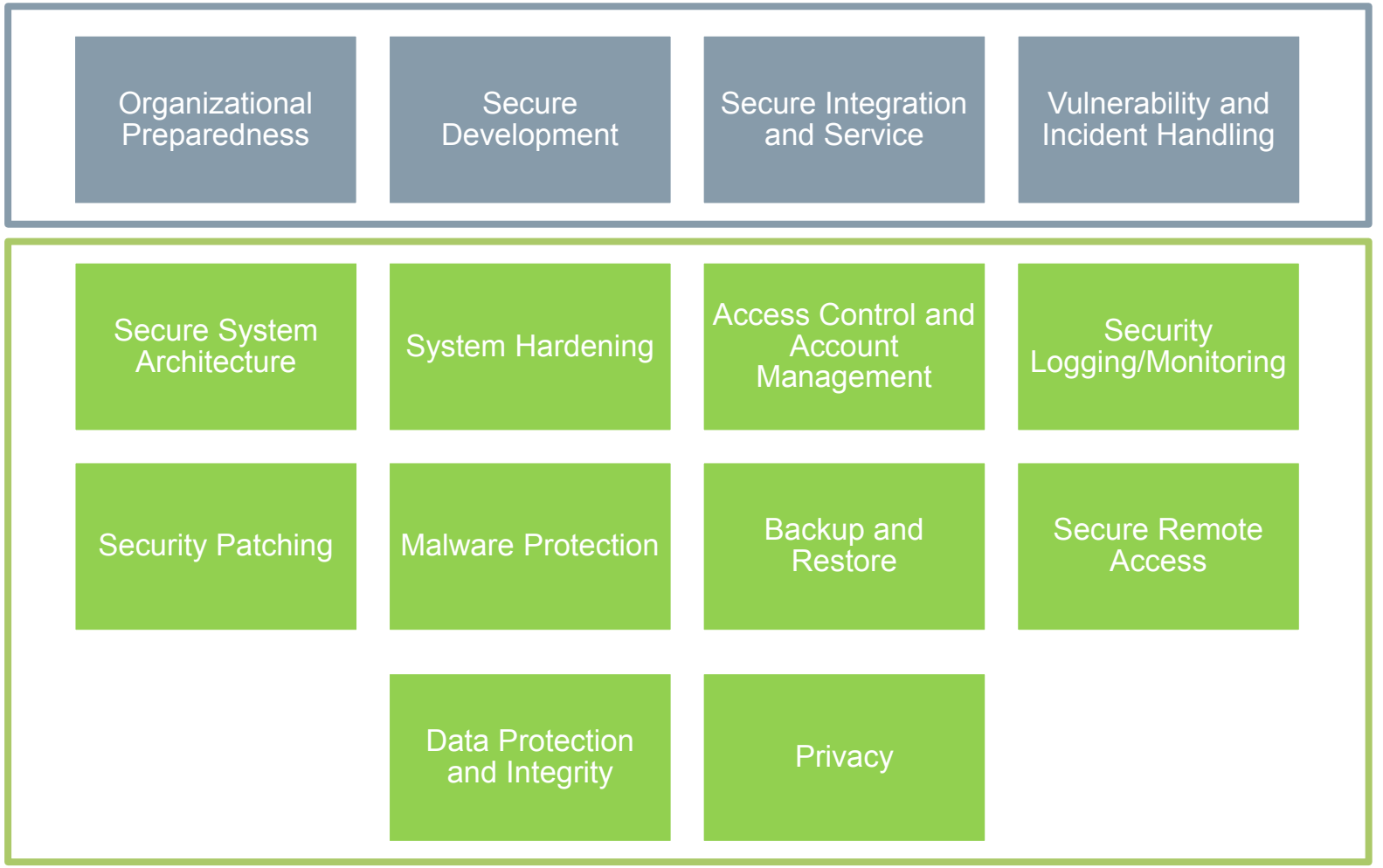
SIEMENS
Ingenuity for life

Policies, Processes and Procedures

- Organizational security, secure development and integration, vulnerability and incident handling

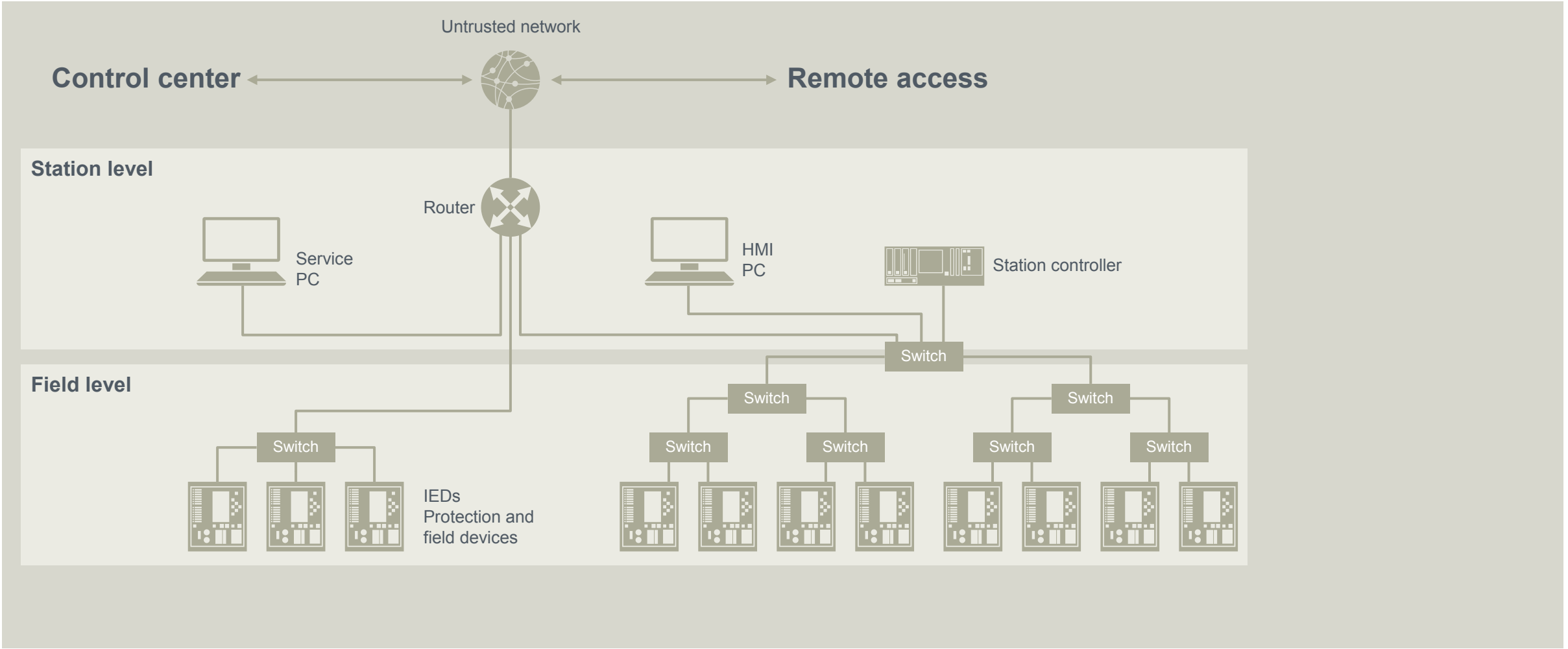
Security Technologies

- Common security technologies need to be implemented and contribute to the overall secure system architecture



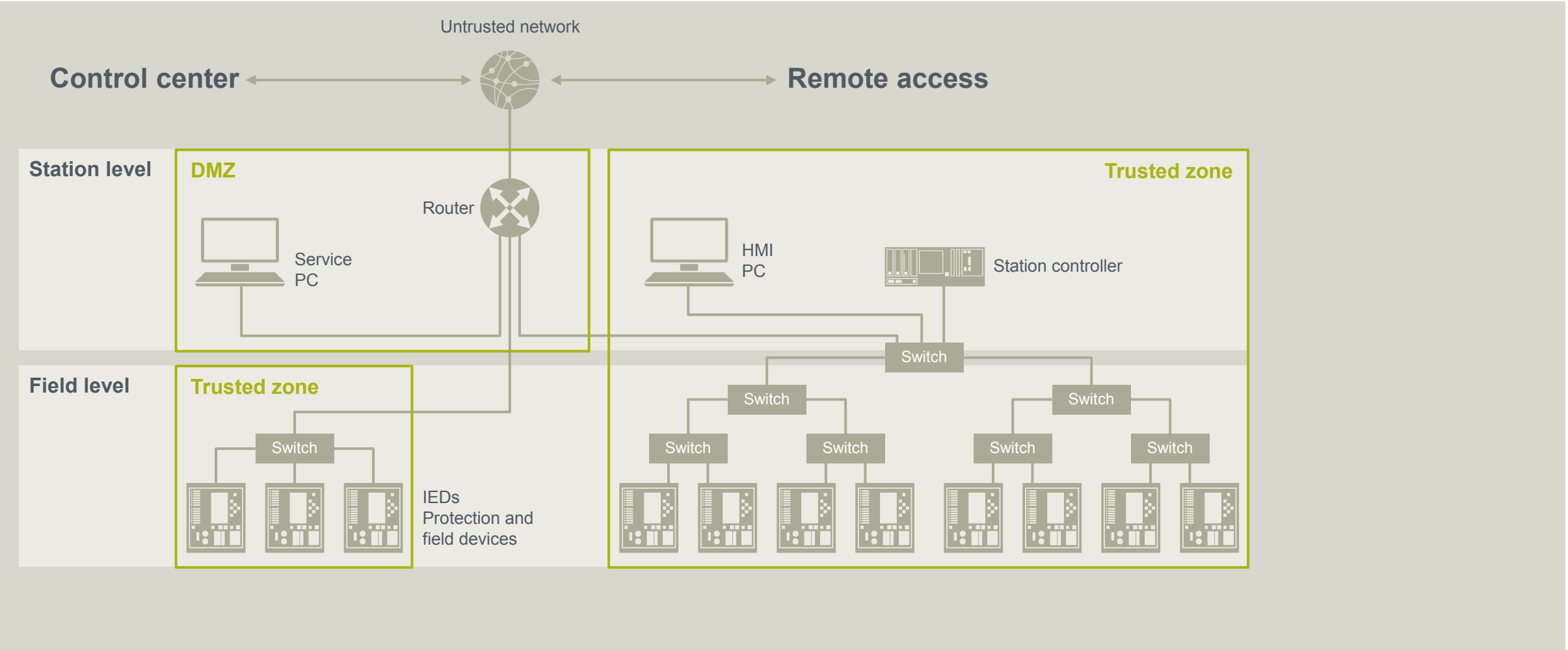
Example: Migration to Secure Substation
Current State

SIEMENS
Ingenuity for life



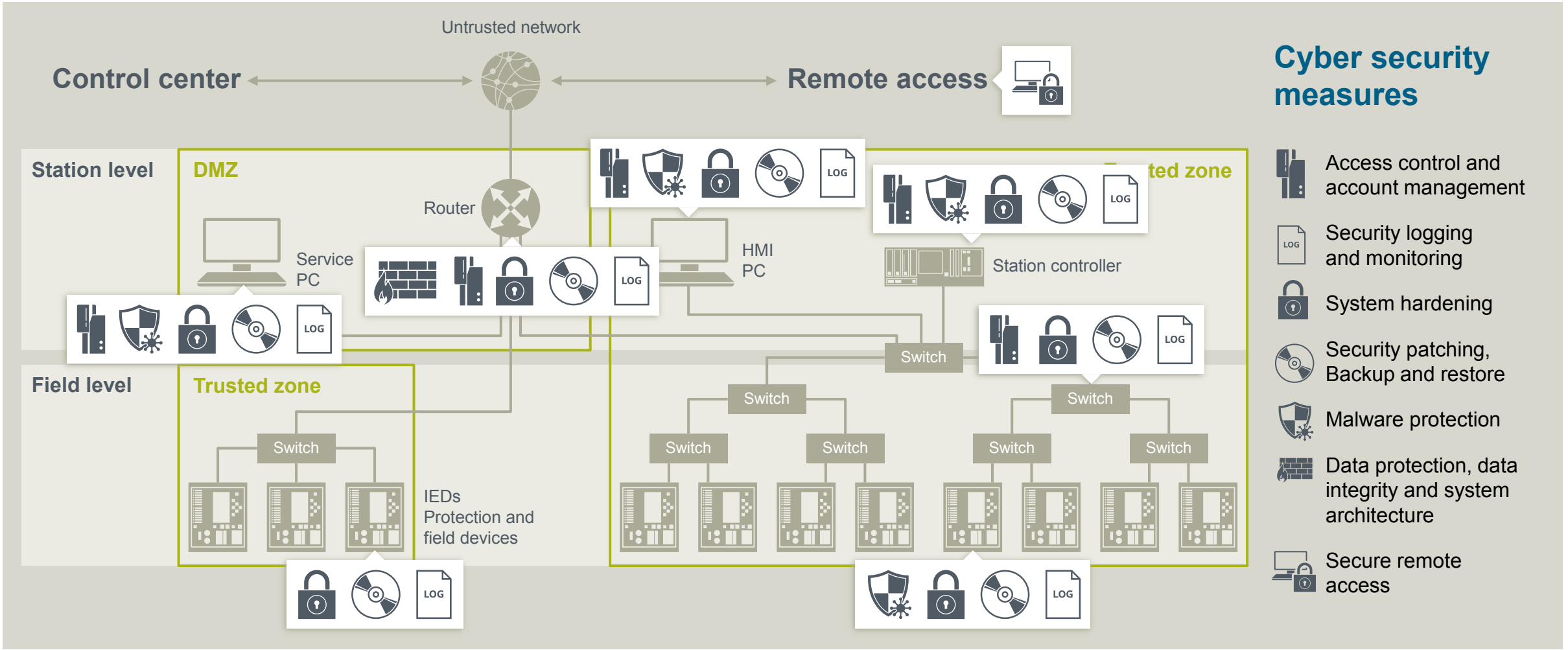
Example: Migration to Secure Substation Secure Architecture

SIEMENS
Ingenuity for life



Example: Migration to Secure Substation Security Controls

SIEMENS
Ingenuity for life

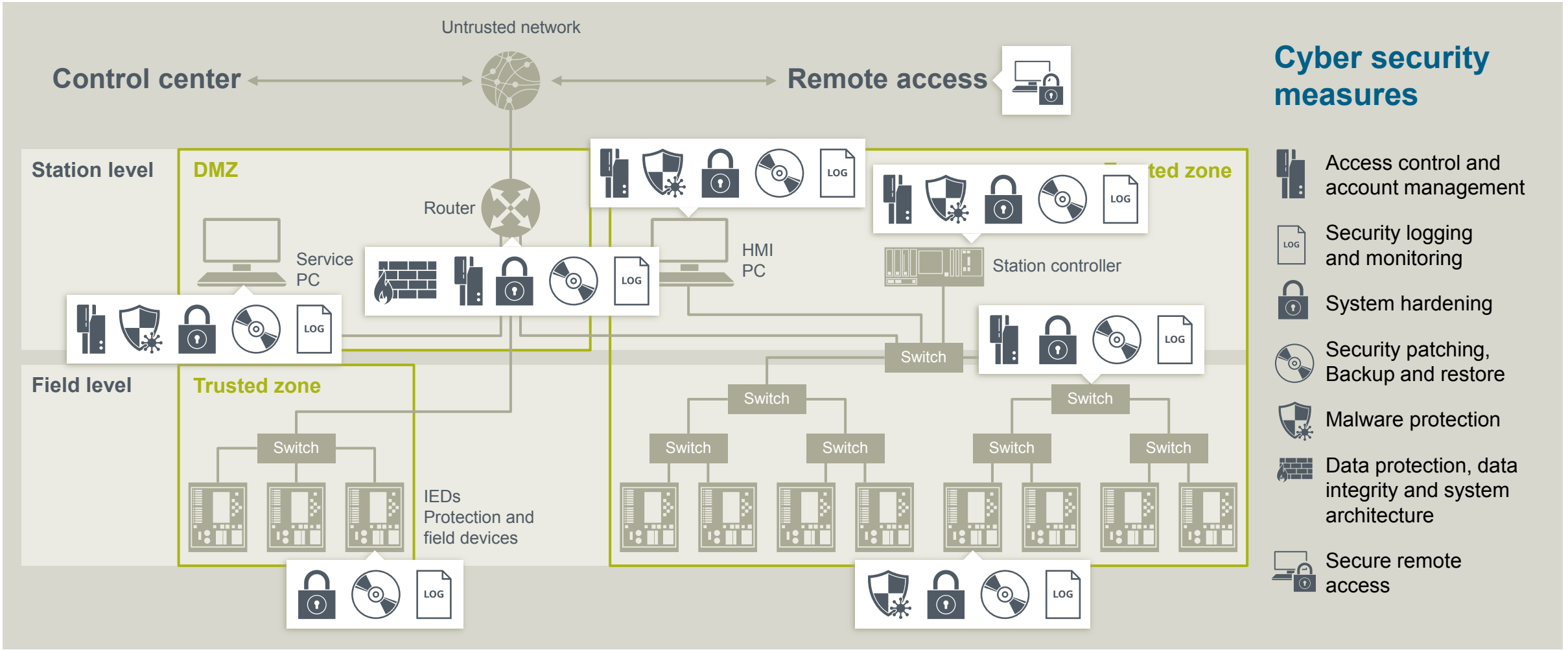


Cyber security measures

- Access control and account management
- Security logging and monitoring
- System hardening
- Security patching, Backup and restore
- Malware protection
- Data protection, data integrity and system architecture
- Secure remote access

Example: Migration to Secure Substation
Secure Substation

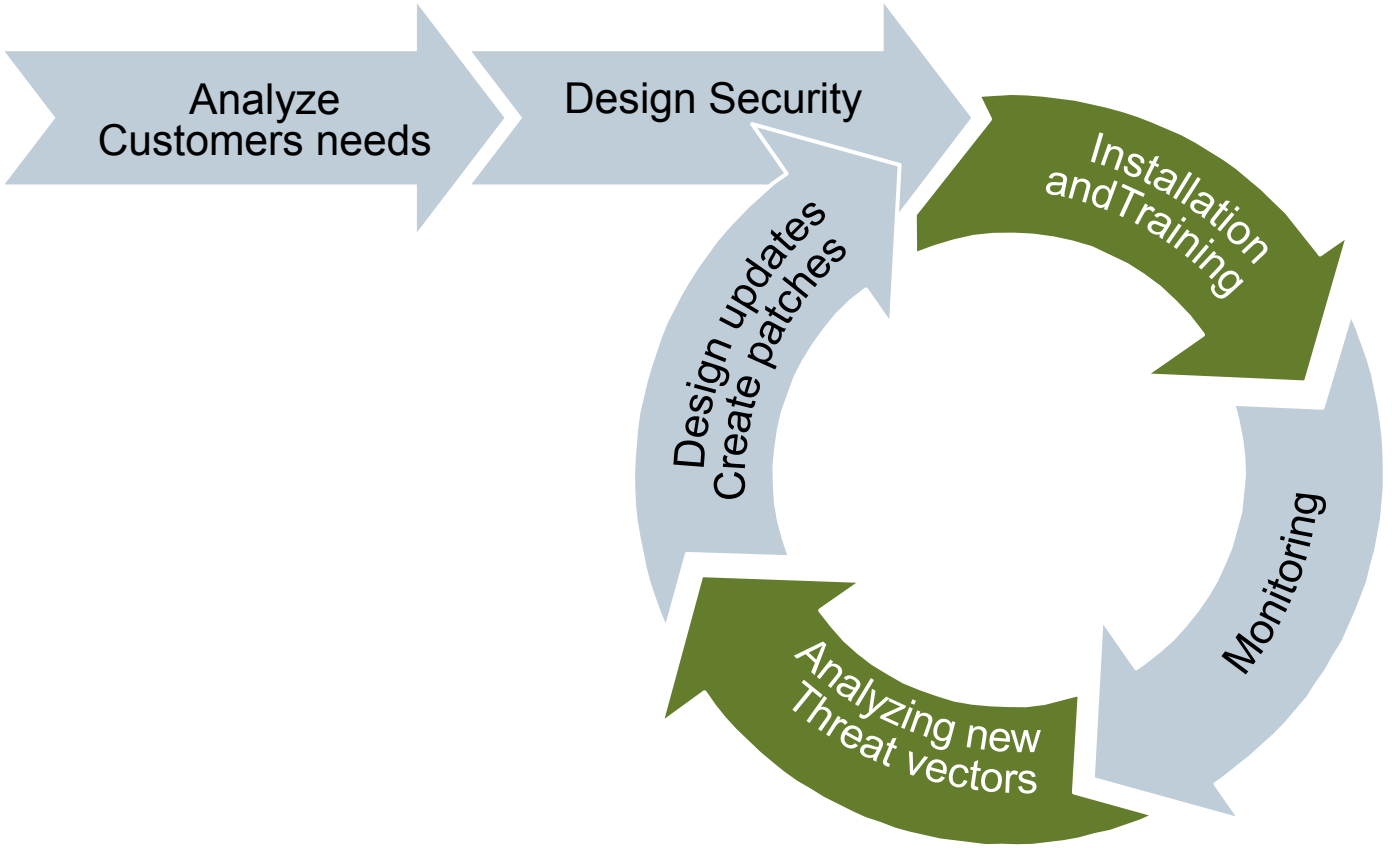
SIEMENS
Ingenuity for life



Cyber security measures

- Access control and account management
- Security logging and monitoring
- System hardening
- Security patching, Backup and restore
- Malware protection
- Data protection, data integrity and system architecture
- Secure remote access

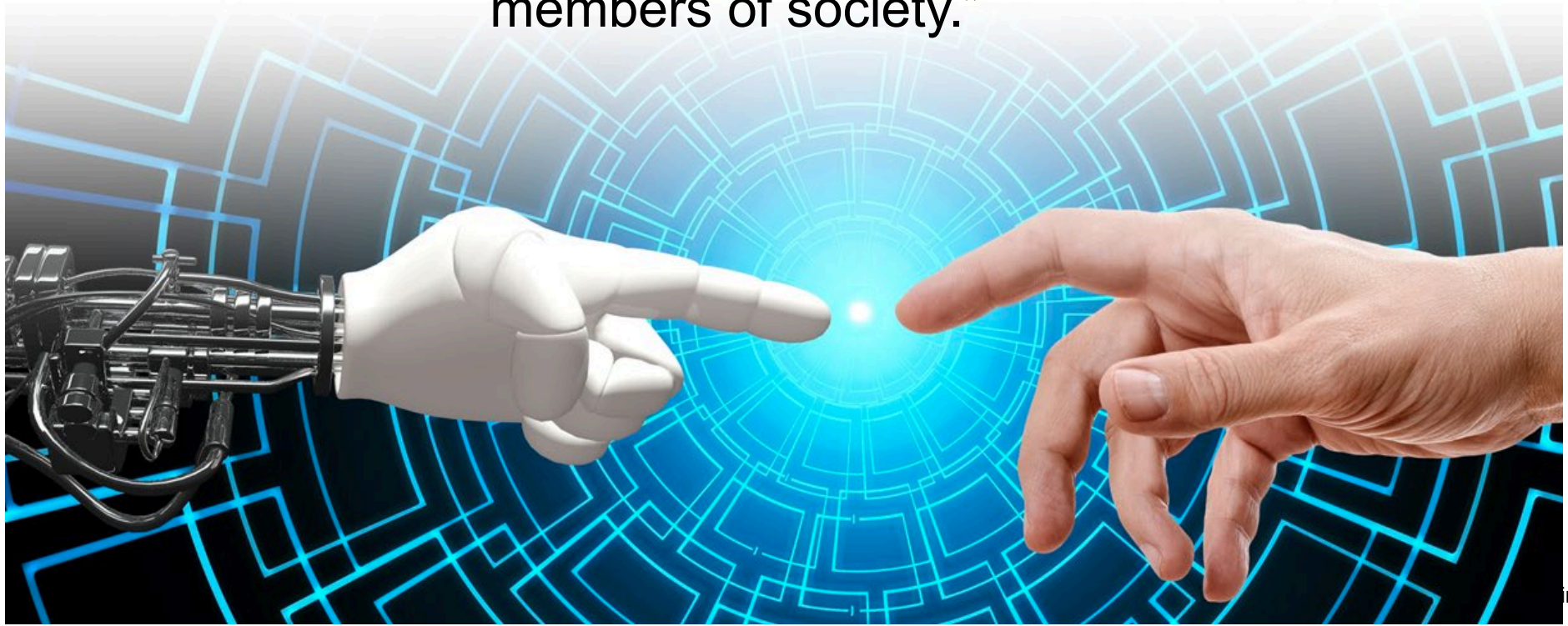
Cyber Security Lifecycle



SIEMENS
Ingenuity for life

Artificial Intelligence (AI)

As artificial intelligence grows in its capabilities - and its impact on people's lives - businesses must move to "raise" their AIs to act as responsible, productive members of society."



SIEMENS
Ingenuity for life

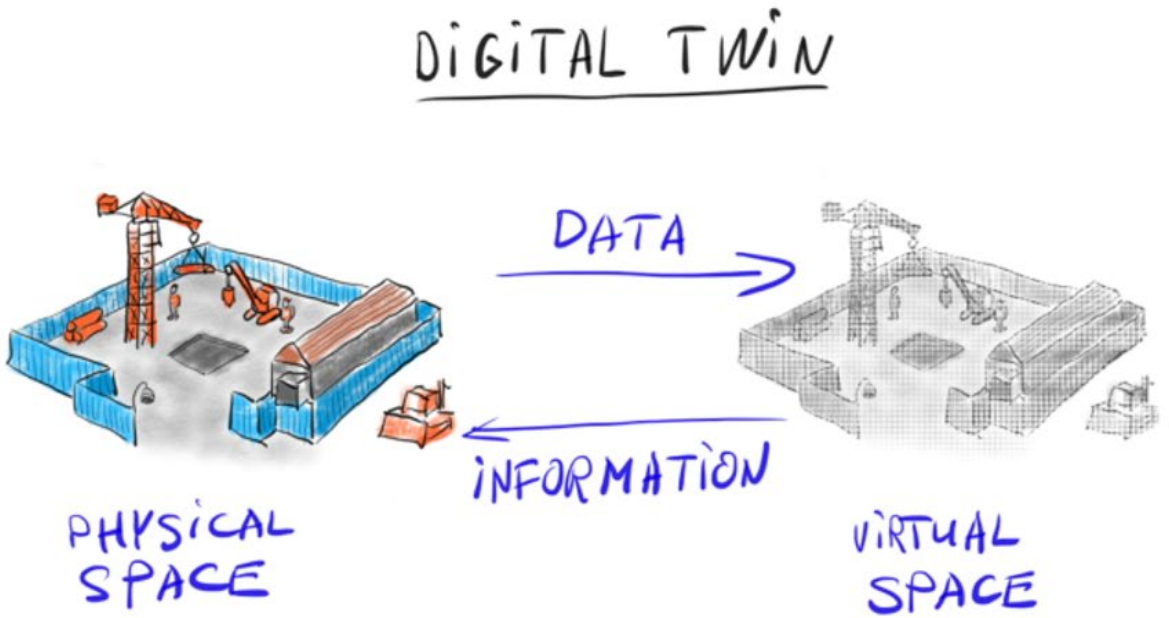
Data Veracity – The Importance of Trust

"By transforming themselves to run on data, businesses have created a new kind of vulnerability: inaccurate, manipulated,

and biased data that leads to corrupted business insights, and skewed decisions with a major impact on society."

Digital Twin

SIEMENS
Ingenuity for life



Technologies needed:

- Data Veracity
- Augmented Reality
- Blockchain
- Deep Machine Learning

How does this benefit me?

SIEMENS
Ingenuity for life

Owner
- Lower cost infrastructure
- Higher valued assets
- Life cycle savings
- Higher rent
- Ongoing partnership

Architect/Engineer
- Design a more efficient, more modern facility
- Ease of operability between systems

Facility/Property Manager
- Data based preventative maintenance
- Reduced nuisance calls
- Remote monitoring
- One system to learn, one service provider to call

Broker
- Higher price per ft^2
- Longer term leases
- Higher end clientele.

General Contractor
- Collaborative design lowers risk
- Lower first cost install
- Reduces RFIs
- Reduces scope gaps

Tenant
- Increased productivity
- People like nice things
- Reduced utilities
- Ability to influence environment

OTHERS???

Q & A

William Coyle
Siemens Industry Inc.
Manager National Business Development
william.coyle@siemens.com

Chris Smith
Siemens Industry Inc.
Business Development
Christopher.e.smith@siemens.com

Maria Marks
Siemens Industry Inc.
Manager National Business Development
Maria.marks@siemens.com