

28.10.2021 / 11.00-11.45

How to design a cybersecurity strategy for IoT?

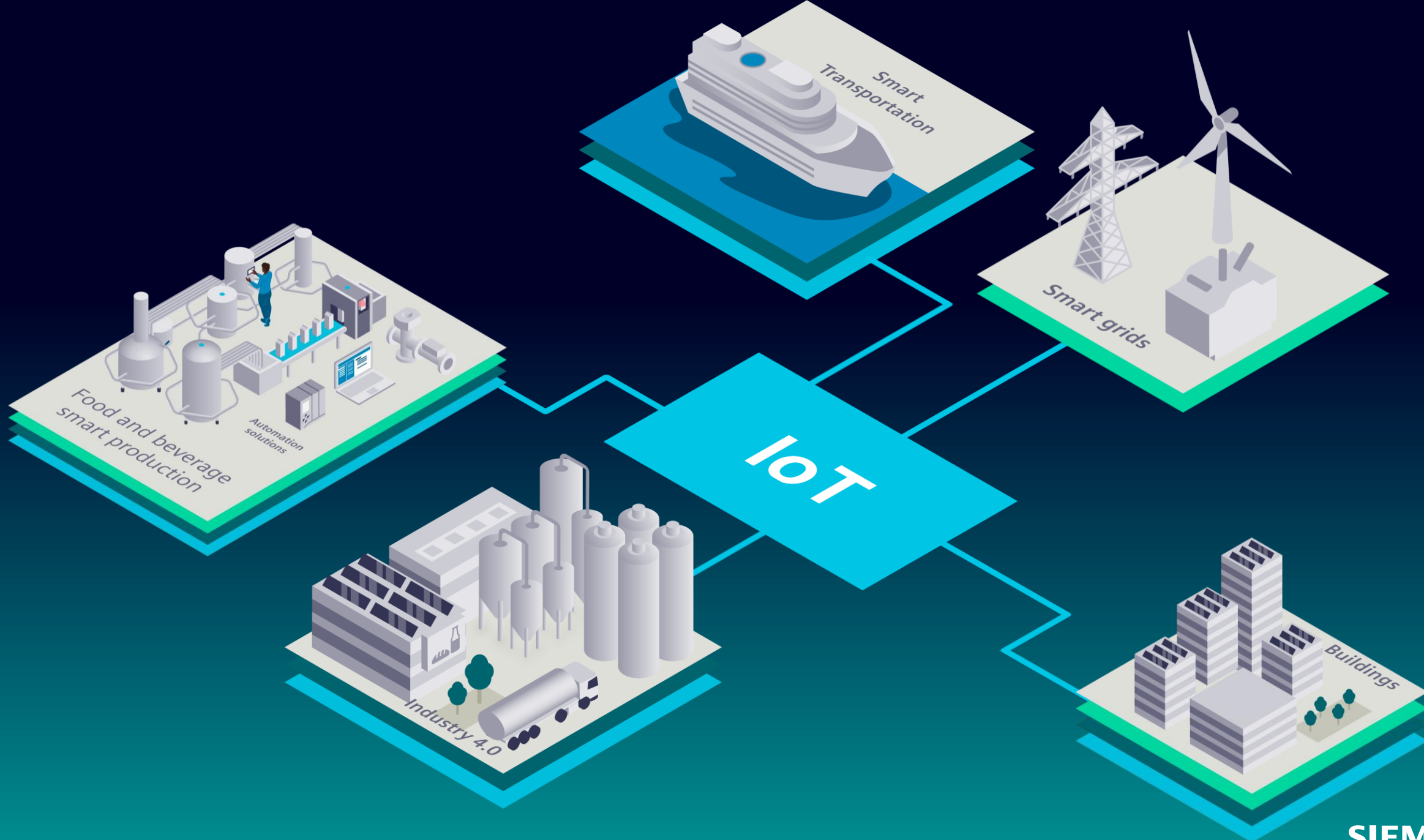
by Dr. Alina Matyukhina



SIEMENS

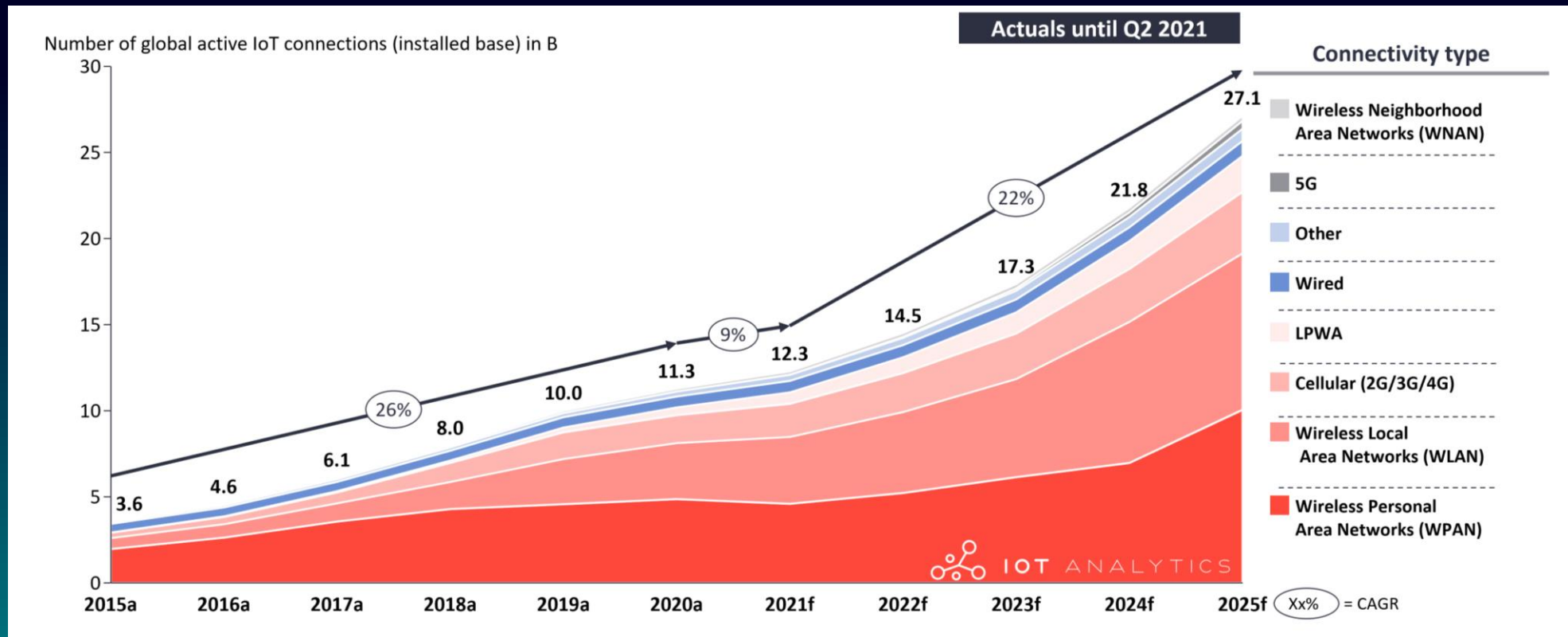
digitalswitzerland
Swiss Digital Day





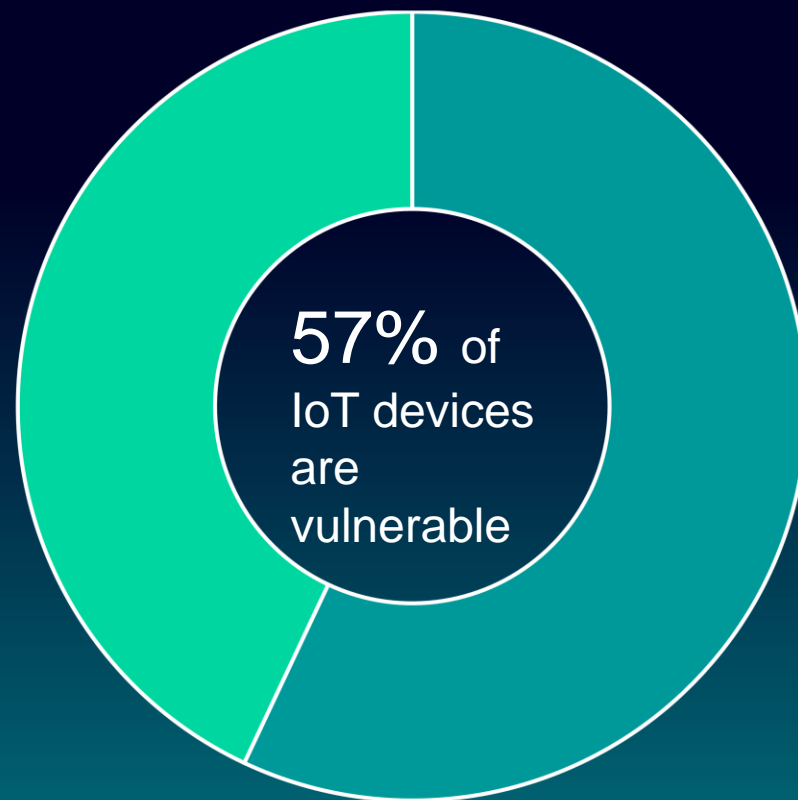
IoT Global Market

The global market for installed based IoT devices is expected to grow due to digital transformation and need of remote maintenance extremely pushed by COVID pandemic



Source: <https://iot-analytics.com/wp/wp-content/uploads/2021/09/Global-IoT-market-forecast-in-billion-connected-iot-devices-min.png>

But sometimes IoT fails...



Source: <https://unit42.paloaltonetworks.com/iot-threat-report-2020/>

Principle 1. Governance

Identification of responsibilities will ensure fast handling and business continuity.



Principle 2. Secure supply chain

Supply chain is critical for a company's cybersecurity

60% of cyberattacks originate from entities within the supply chain

Small organizations are accounted for 92% of cyber incidents

Top cybersecurity issues name supply chain as weakest link in risk management

1,500 SolarWinds Customers Are Exposing Themselves To Hackers...



Source: <https://www.forbes.com/sites/thomasbrewster/2021/01/06/1500-solarwinds-customers-are-exposing-themselves-to-hackers-as-russian-espionage-continues/?sh=7f404c554329>

How to find a right supplier and select a secure component?

Companies should require critical supply chain partners to meet reasonable levels of security before establishing business agreements.

Does your supplier comply with security standards (IEC, ISO, etc.)?

Did the component go through security testing?

How suppliers prevent unauthorized manipulation of deliveries along the chain?



How will potential vulnerabilities be fixed in the future?

Are security features and secure configuration sufficiently documented?

What kind of security activities suppliers have in their development process?

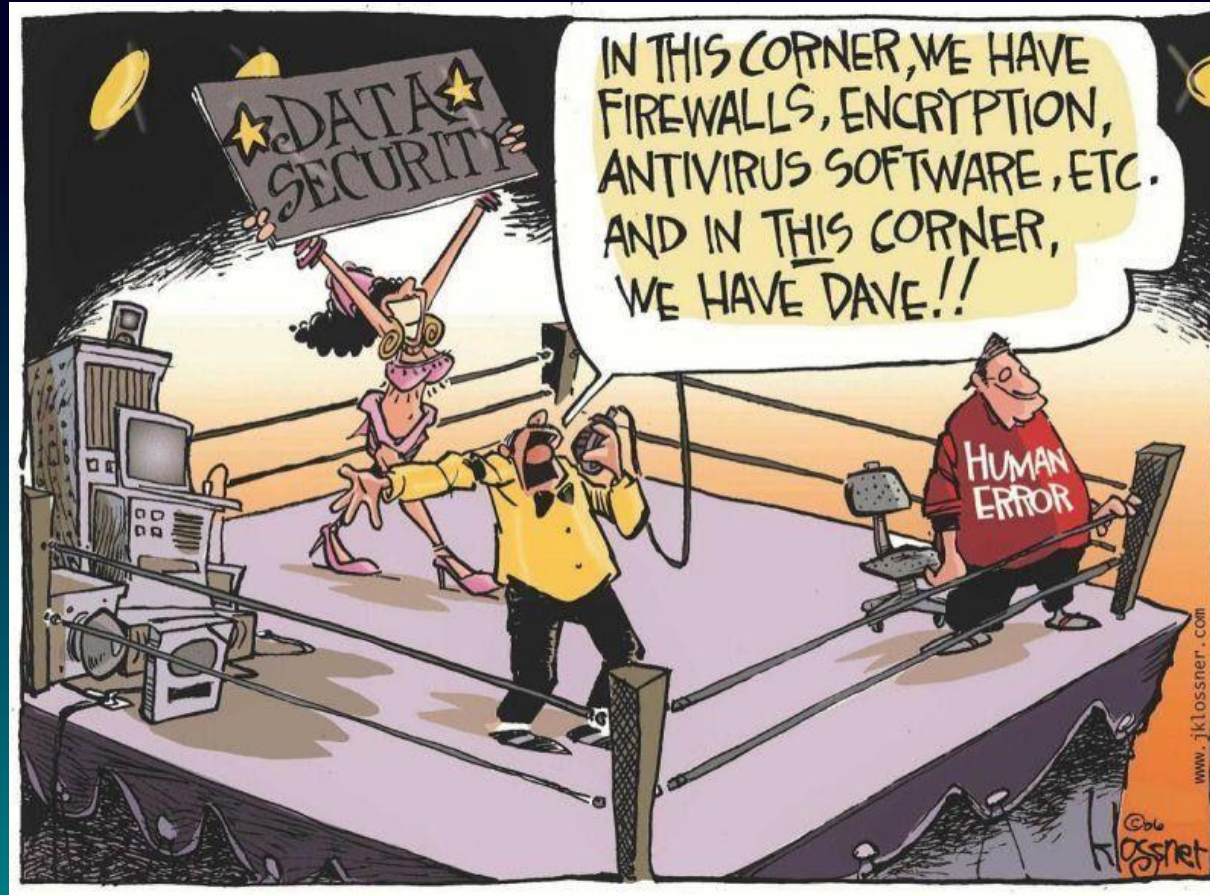
Principle 3. Cybersecurity in product development

Agile development shall include all necessary security measures



Principle 4. Internal and external cybersecurity awareness

People are at the heart of cybersecurity...



Source: <https://community.spiceworks.com/topic/497931-and-in-this-corner-we-have-dave-funny-cartoon>

Knowledge shared = knowledge²


WORLD ECONOMIC FORUM

Agenda Events Reports Platforms

Join us

Future of Energy | Cybersecurity

7 ways to boost cyber resilience in the smart building industry



Siemens' campus in Zug, Switzerland, evaluates the information from 12,000 sensor-generated datapoints to reduce its energy consumption. Image: Siemens Schweiz AG

27 Jul 2021

Henning Sandfort
Chief Executive Officer, Building Products, Smart Infrastructure, Siemens AG

Alina Matyukhina
Cybersecurity Manager, Smart Infrastructure, Siemens AG

AUDIO: LISTEN TO THE ARTICLE

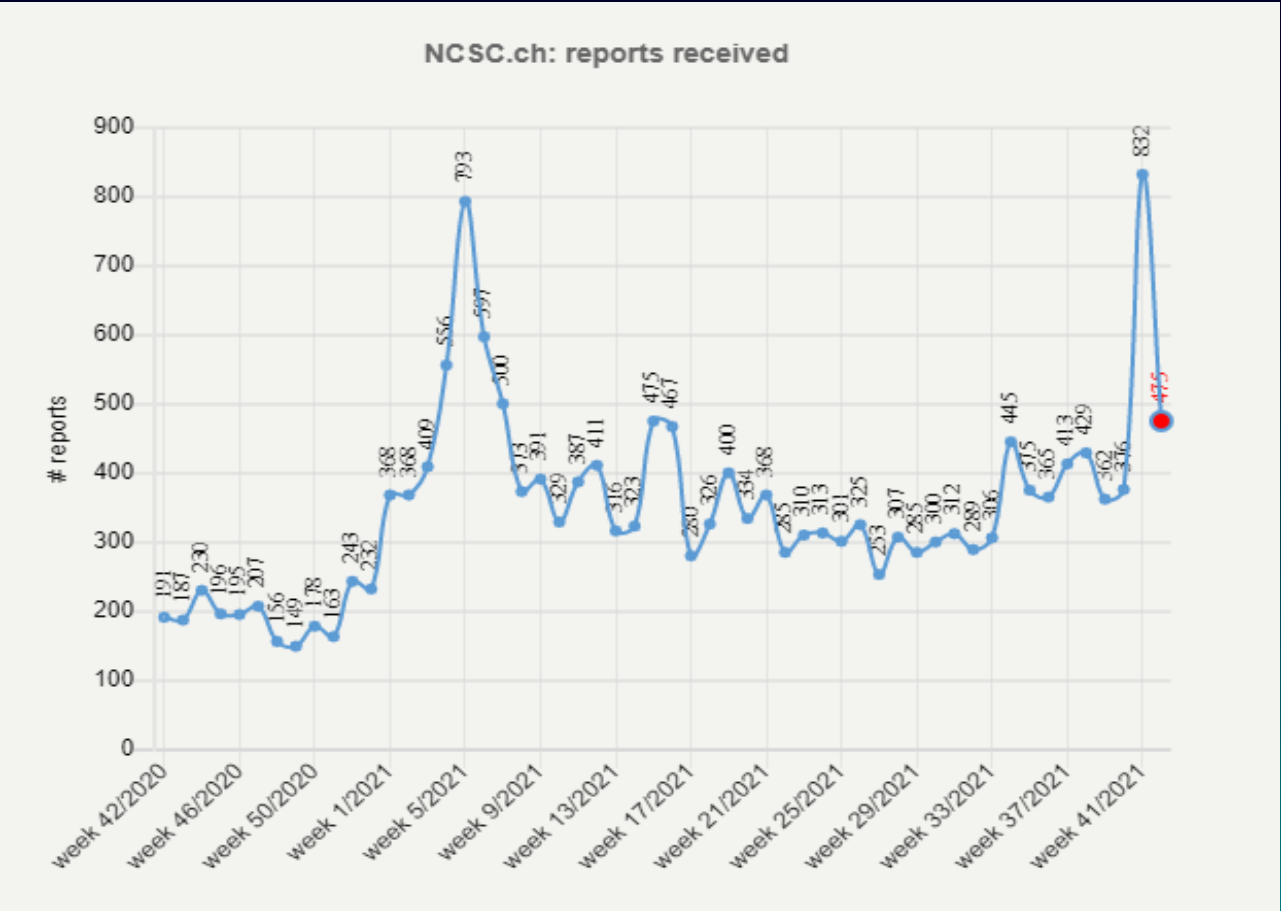
08:51

This is an experimental feature. Some words or names may be mispronounced. Does it sound good? Yes / No

- Smart buildings can significantly reduce buildings' energy consumption.

Source: <https://www.weforum.org/agenda/2021/07/7-ways-to-boost-cyber-resilience-in-the-smart-building-industry/>

Principle 5. Vulnerability and incident handling



~400 cyberincidents/week reported by the public and SMEs to the National Cybersecurity Centre (NCSC) in Switzerland.

Source: <https://www.ncsc.admin.ch/ncsc/en/home/aktuell/aktuelle-zahlen.html>

What is the process of Incident and vulnerability handling?

Any suspected incident should be treated as real incident until you have proved that it was a false alarm



Report

Analysis

Handling

Disclosure



Siemens ProductCERT and Siemens CERT- the central expert teams for immediate response to security threats and issues affecting Siemens products, solutions, services, or infrastructure.

<https://new.siemens.com/global/en/products/services/cert.html>

Report Security Issue

Siemens Security Advisories

Hall of Thanks

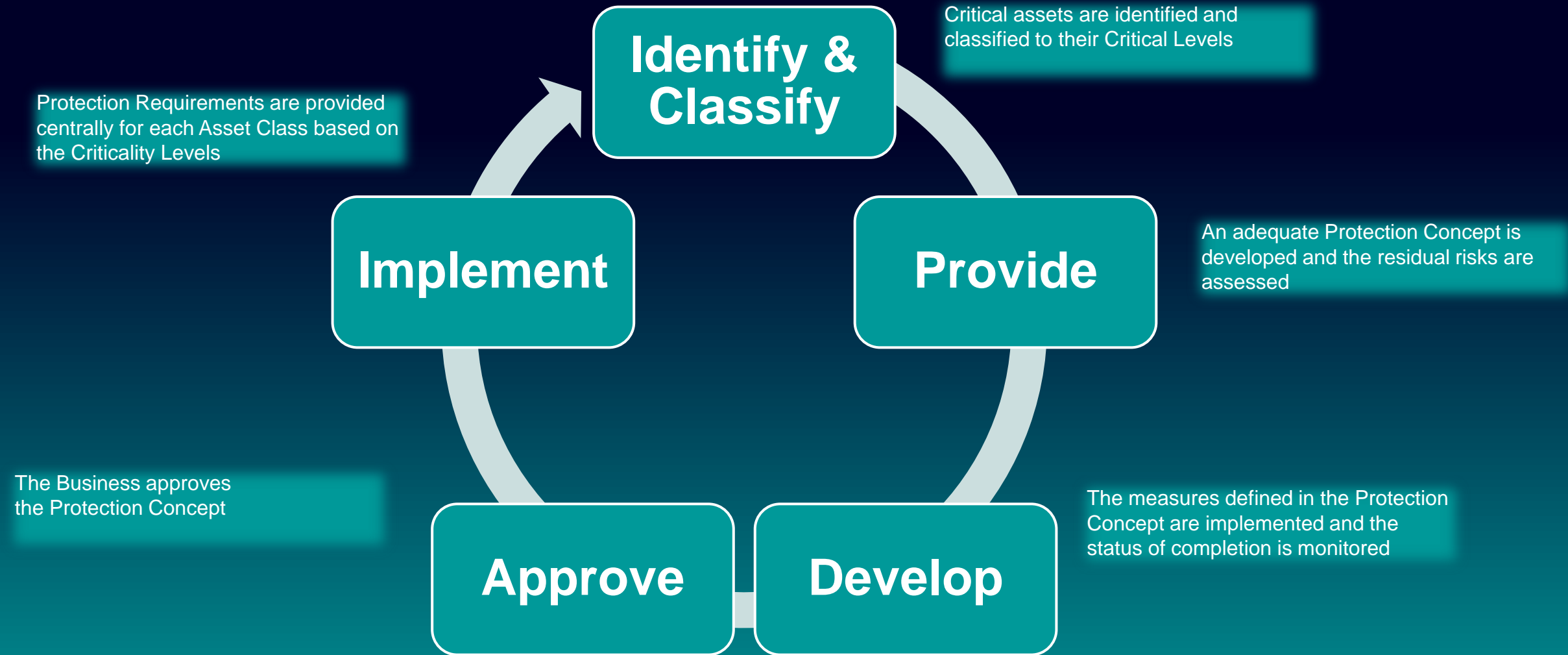
Principle 6. Risk-based asset management







- Do you know which assets are critical to your business?
- How your assets are secured with regard to:
 - Confidentiality?
 - Integrity?
 - Availability?



How does asset classification and protection (ACP) work?



Principle 7. Compliance with cybersecurity standards

Industry		IEC62443	<p>Industrial communication networks – Network and system security</p> <ul style="list-style-type: none"> • International standard • Focus: Applications of Industrial Automation and Control Systems • Content: Organization, system and component security • Endorsed by industry and local authorities in EU, AP, MA
		UL2900	<p>Software Cybersecurity for Network-Connectable Products</p> <ul style="list-style-type: none"> • International standard • Focus: Network Connectable Products • Content: Industrial Control Systems (UL2900-2-2) • Endorsed by local authorities in US
IT		ISO270xx	<p>Information security management systems</p> <ul style="list-style-type: none"> • International standard • Focus: Classic IT Environments • Content: Base for IEC62443, e.g. ISO27033 Network Security • Endorsed by IT, software and cloud providers
		OWASP	<p>Open Web Application Security Project – OWASP Foundation</p> <ul style="list-style-type: none"> • International not-for-profit charitable organization • Focus: Safety and security of Software applications and services • Content: Penetration test and process evaluation • Endorsed by software and cloud providers

Example: IEC62443 certification

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ CERTIFICADO ◆ CERTIFIKAT



CERTIFICATE

No. IITS1 113879 0001 Rev. 00

Holder of Certificate: **Siemens Schweiz AG**
SI BP
Theilerstrasse 1a
6300 Zug
SWITZERLAND

Site(s): Siemens Schweiz AG
SI BP
Theilerstrasse 1a, 6300 Zug, SWITZERLAND

Siemens AG
SI BP
Siemensallee 84, 76187 Karlsruhe, GERMANY

Certification Mark: 

Type: Industrial IT Security

Scope of Certificate: Secure Development Lifecycle Process

Applied Standard(s): IEC 62443-4-1:2018
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report.
See <http://www.tuvsud.com/ps-cert> for details.

Report No.: 21CR02S027

Valid until: 2024-08-29

Date, 2021-09-14 
(Enrico Seidel)

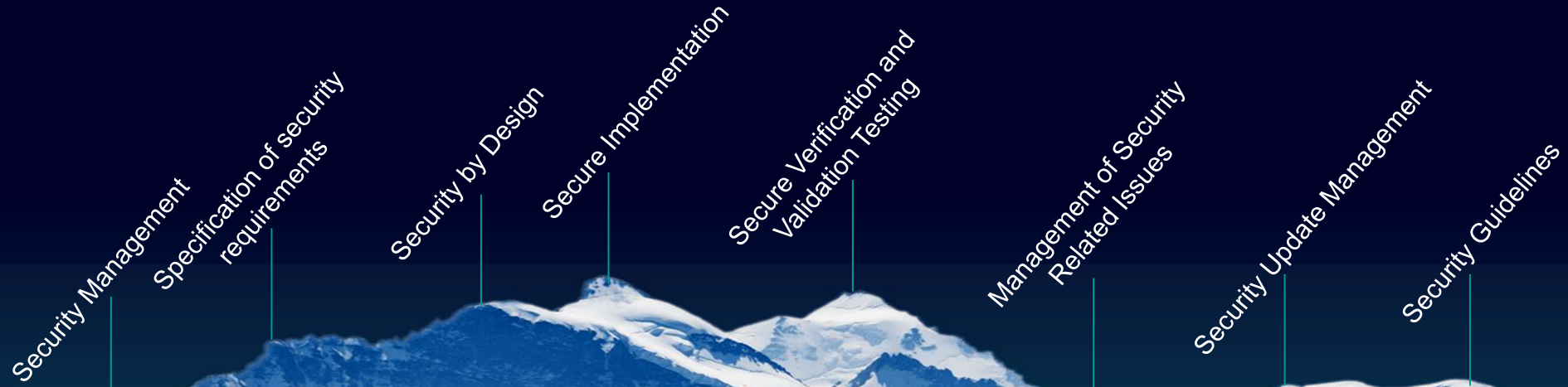
Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TUV[®]

- Siemens Smart Infrastructure Building Products was certified by TÜV Süd on IEC62443 4-1:
 - the process of our secure product development is fully compliant with international standard
 - achieved maturity level 3: the process is lived by existing projects
- The locations with certified process:
 - Zug (Switzerland)
 - Karlsruhe (Germany)
- IEC62443 4-1 (process certification) is a prerequisite to IEC62443 4-2 (product certification)

Achieving cybersecurity certification is like climbing a mountain....

The assessment was based on more than four dozen metrics:



Link to the article: <https://www.linkedin.com/pulse/achieving-cybersecurity-certification-like-climbing-matyukhina/>

| Contact

Dr. Alina Matyukhina
Cybersecurity Manager
Siemens Schweiz AG, Smart Infrastructure
Theilerstrasse 1A
6300 Zug
Switzerland

E-mail alina.matyukhina@siemens.com



<https://www.linkedin.com/in/alinamatyukhina/>



@alinamatyukhina

Feedback



Contest

Win a HomePod mini!

