Automation Systems in Buildings

Evolution and Cybersecurity Regulation Landscape

AMCA European Fan Symposium 2024

Emmanuel Val

Head of Product Management
Edge BMS

Siemens Smart Infrastructure

Francesco Negosanti

Business Cybersecurity Manager
Building Automation and Connected Devices

Siemens Smart Infrastructure

Presentation Outline

01

The democratization of the automation systems in buildings: its evolution, the trend and its outlook

02

IT/OT convergence and cybersecurity threat landscape: impact on building automation and IOT

03

New EU cybersecurity regulation landscape: addressing the need for cybersecurity in products and infrastructures

04

Q&A

The democratization of the automation systems in buildings

Emmanuel Val
Siemens Smart Infrastructure

AMCA European Fan Symposium 2024

Current megatrends

#ClimateChange #Digitalization #Glocalization

#DemographicChange #Urbanization

#ResourceScarcity

People Challenges

9.7bn

people will populate
our planet by 2050.[1]

90%

of lifetime spent in buildings.[1]

68%

of the world population projected
to live in urban areas by 2050.[2]

Sources: **1** United Nations **2** Alliance To Save Energy (ASE)

Environmental Challenges

40% of all energy is used by buildings[1] whose operation causes 27% of global CO_2 emissions.[2]

75% of all buildings are energy **in**efficient.[1]

2x the global building floor area by 2060.[2]

More cooling than heating by 2050.

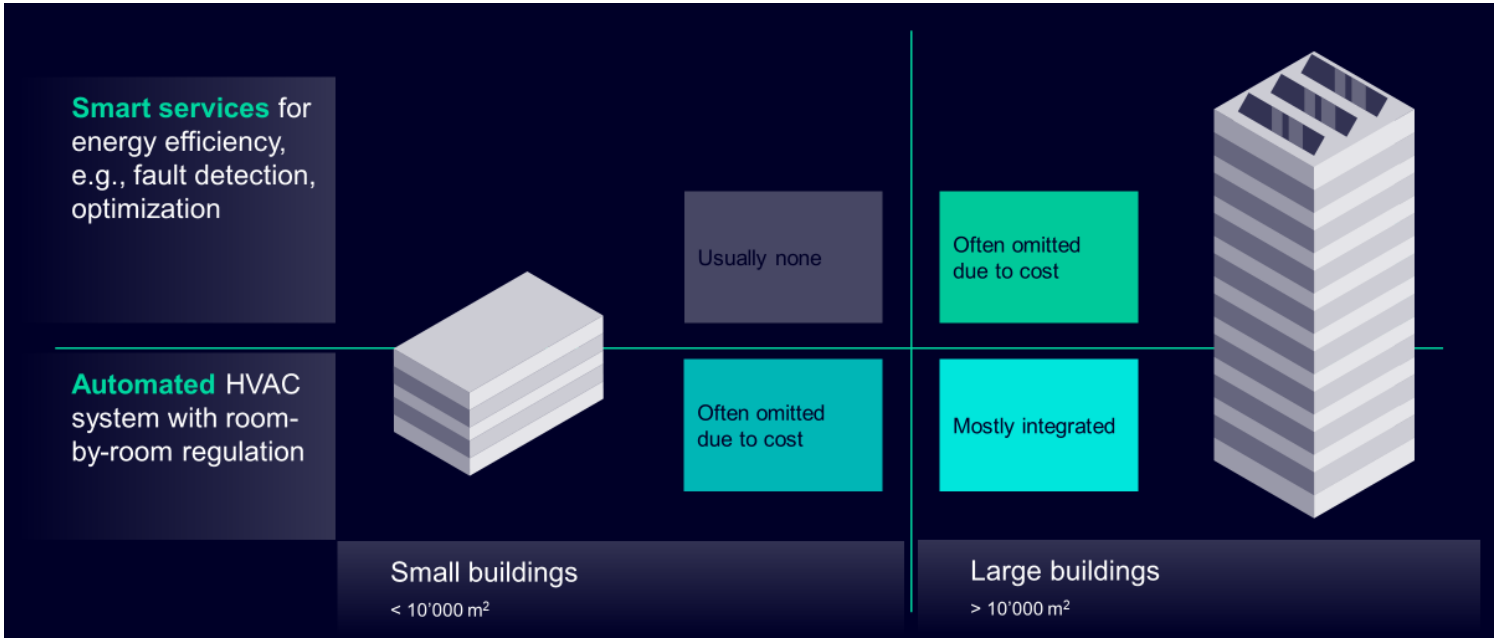
Sources:
1 Alliance To Save Energy (ASE), EU, UNEP, EPA
2 architecture 2030

Sustainability Challenges

- **Sustainability goals and regulations** need to be met
- Stricter policies from the **Paris Agreement**
- Greater **pressure for action** with high potential in the construction industry as demand of products can decline and CO_2 emission costs may rise
- Businesses can only be **competitive when sustainable**

Let’s focus on the floor area in commercial buildings

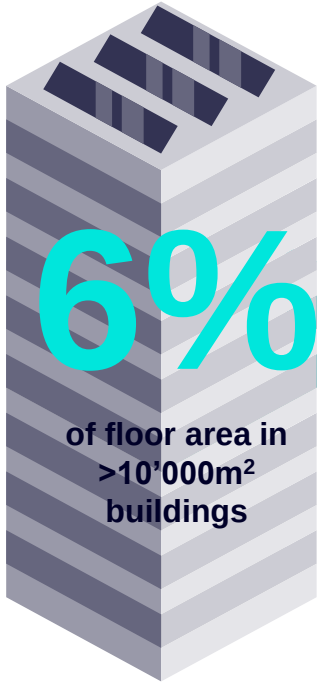
When it comes to commercial buildings, there is a wide range of building types



The global stock of commercial buildings – vast majority of buildings is smaller than 10’000m²

94%

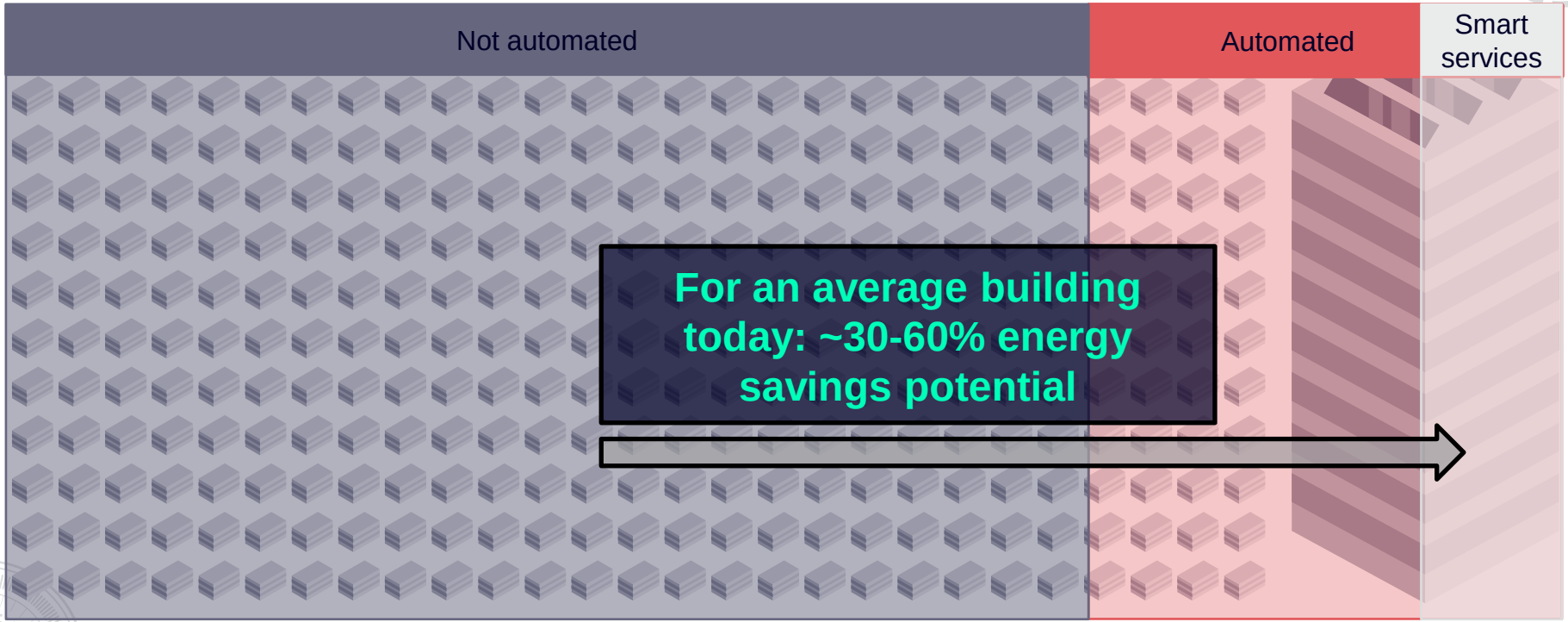
of floor area in <10’000m² buildings



6%

of floor area in >10’000m² buildings

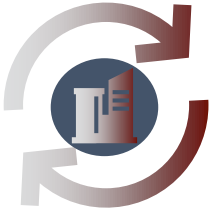
Most buildings are not automated and have big energy savings potential



Key takeaways

Regulation – compliance and certification

- Increasing pressure on companies to be compliant
- Stronger regulation at a global, regional and country level
- Expectations on sustainability from tenants and employees grows



Retrofit wave for existing buildings

- 75% of all current buildings are inefficient
- We need to expand the application of automation in new, and existing buildings
- Fast and simple retrofit to add automation is a key enabler

Broader engagement required in industry and beyond

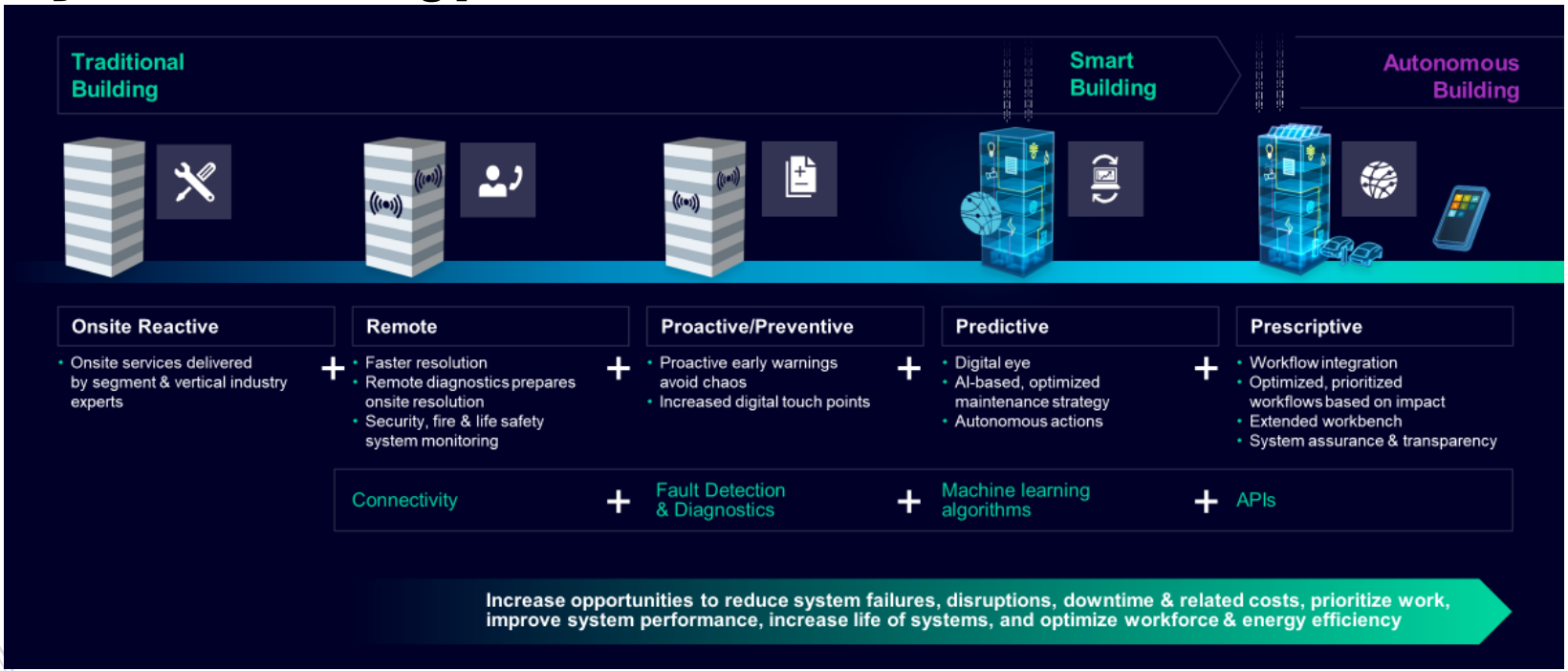
- Retrofit wave broadens the scope of buildings to equipe
- Mobilization of an expanded workforce to deliver automation is crucial
- Solutions that require less experience and skills for simpler buildings are core

Technology alone won’t do the trick, but

75% of companies see digitalization as key driver

of change processes in buildings

The journey from a traditional to a smart building and beyond
Pathway to better building performance

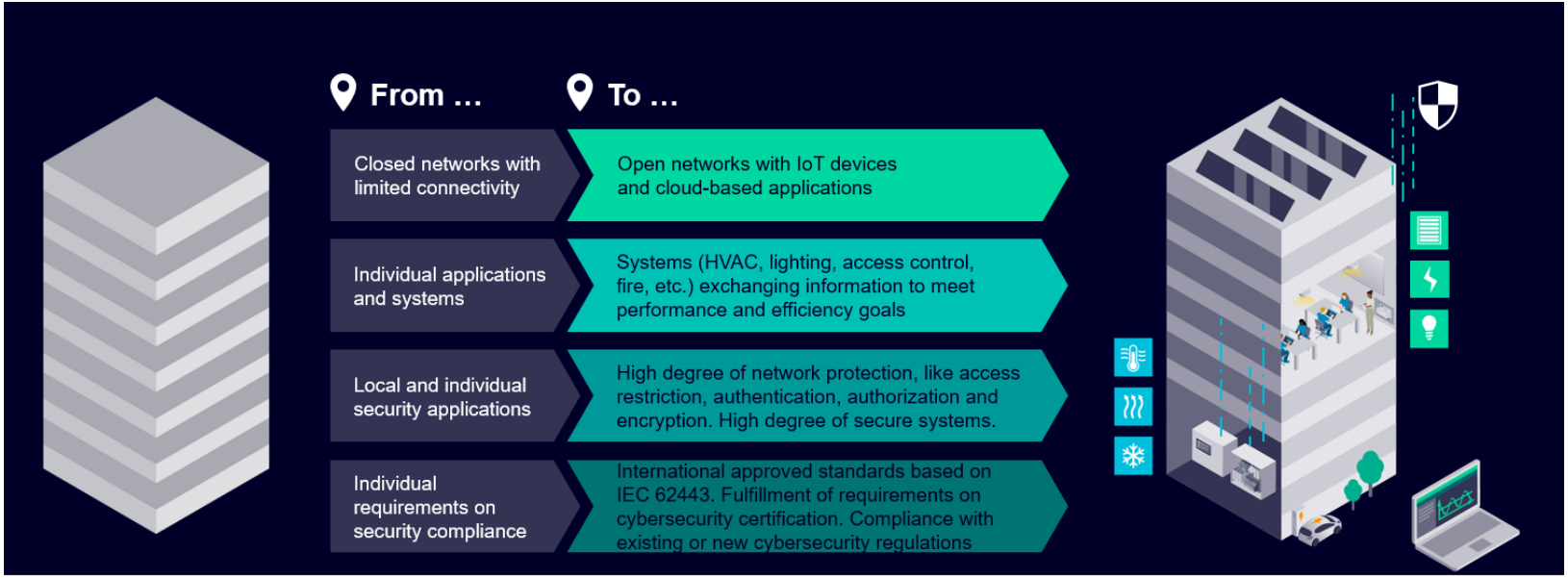


IT/OT convergenge and cybersecurity threat landscape: impact on building automation and IOT

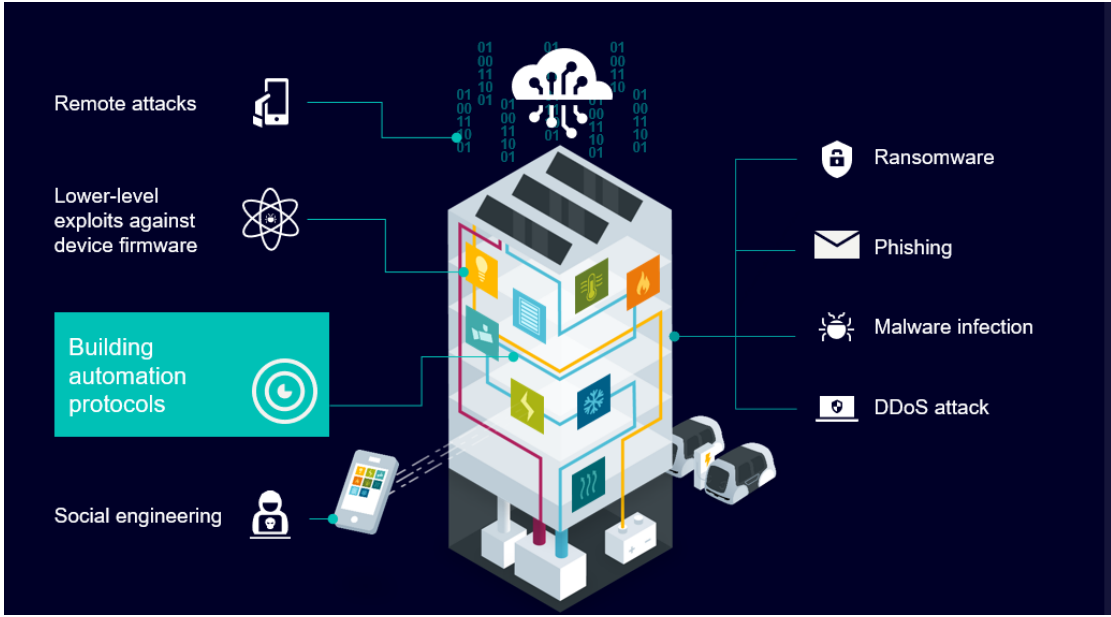
Francesco Negosanti
Siemens Smart Infrastructure

AMCA European Fan Symposium 2024

Increased connectivity and digitalization in building systems bring new cybersecurity requirements



Buildings are getting smarter and more connected....
The attack surface is growing

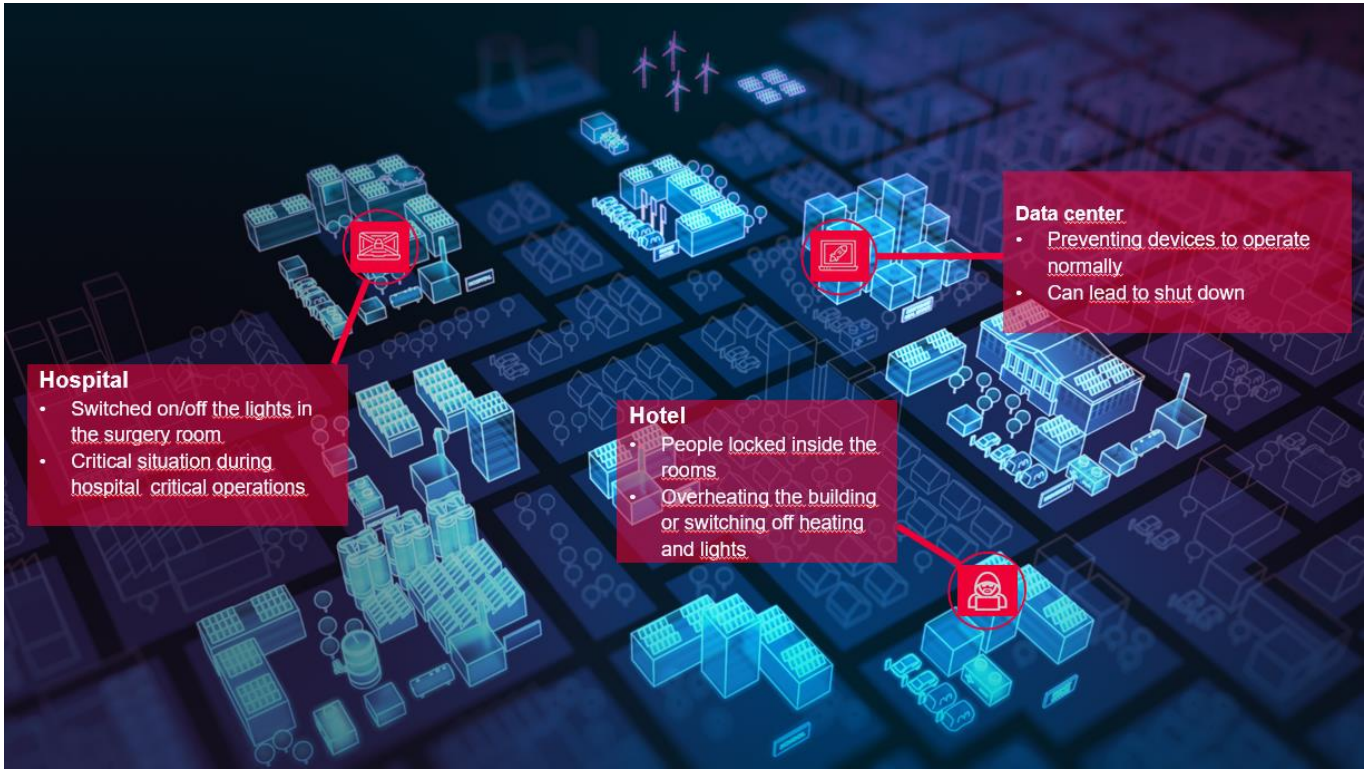


Increased number of connected devices

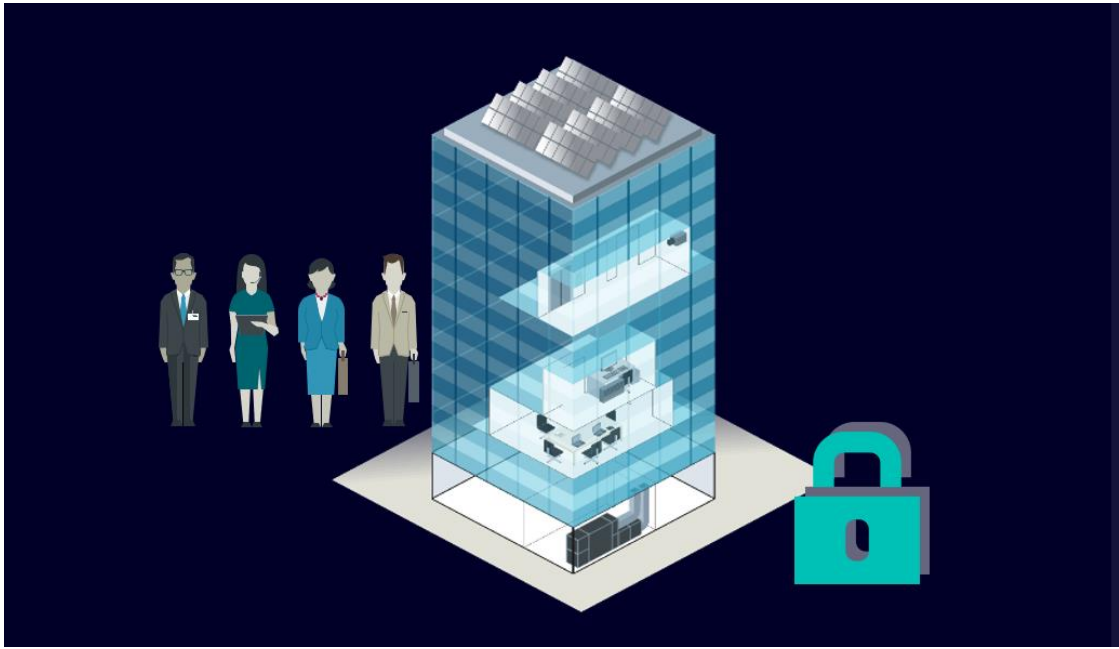
More devices are remotely accessible

Interconnectivity of different systems

What could happen in case a building is facing a cyberattack?



Organizations - (small or large) – have a lot at stake if faced with a cyber attack



Financial impact

Loss of intellectual property

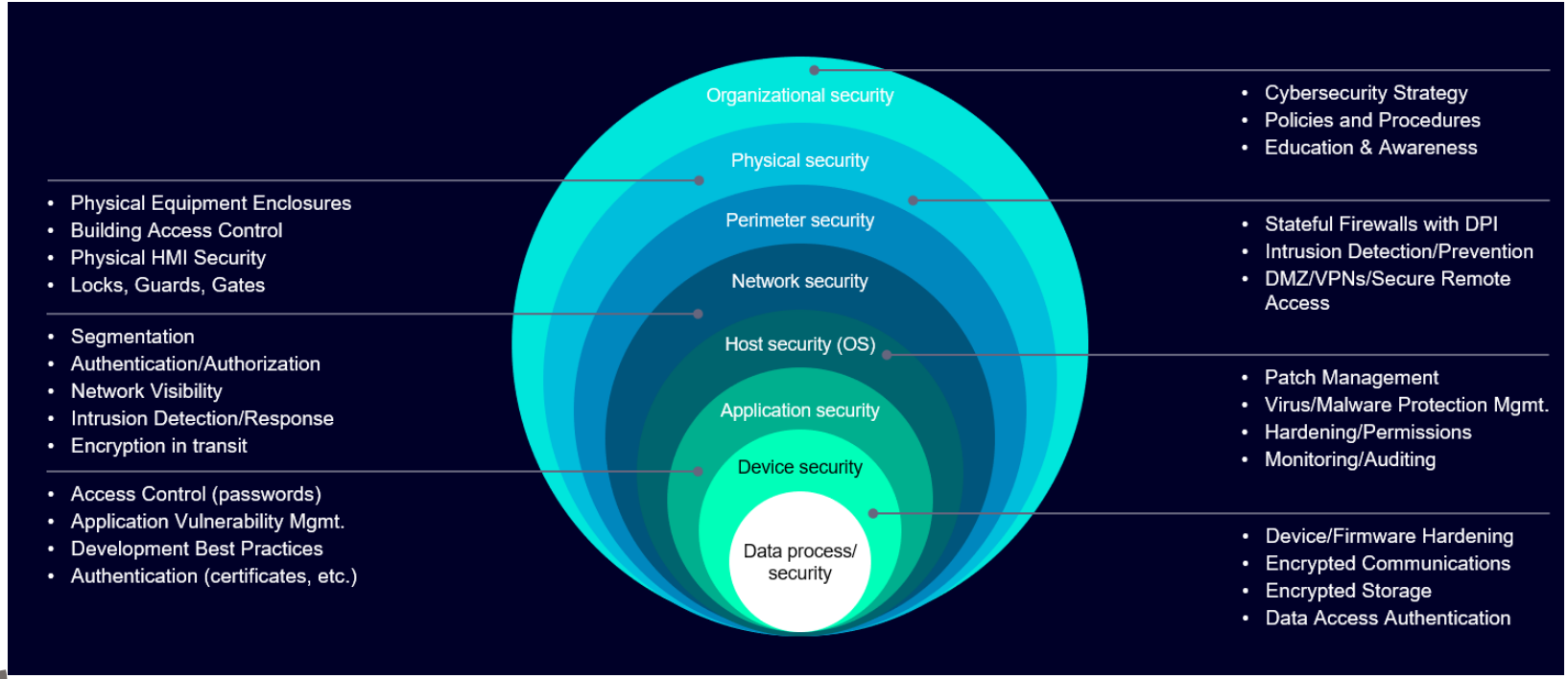
Loss of valuable data

Critical operations halted

Compromised reputation

Customers lose confidence

Organizations need a defense-in-depth model to protect themselves from cybersecurity risks



New EU cybersecurity regulation landscape: addressing the need for cybersecurity in products and infrastructures

Francesco Negosanti
Siemens Smart Infrastructure

AMCA European Fan Symposium 2024

NIS-2 Directive:
Large part of public and private sector is impacted

Essential and Important Entities

Annex I: Sectors of high criticality

SECTOR	SUB-SECTOR	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
ENERGY	Electricity; district heating & cooling; gas; hydrogen; oil. Including providers of recharging services to end users.	ESSENTIAL	IMPORTANT	NOT IN SCOPE
TRANSPORT	Air (commercial carriers; airports; Air traffic control [ATC]); rail (infra and undertakings); water (transport companies; ports; Vessel traffic services [VTS]); road (ITS)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: public transport: only if identified as CER (see notes on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
BANKING	Credit institutions (**attention: DORA lex specialis – see note on page 2**)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
FINANCIAL MARKET INFRASTRUCTURE	Trading venues, central counterparties (**attention: DORA lex specialis – see note on page 2**)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
HEALTH	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: entities holding a distribution authorization for medicinal products: only if identified as CER (see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DRINKING WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
WASTE WATER	(only if it is an essential part of their general activity)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DIGITAL INFRASTRUCTURE	Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
	DNS service providers (excluding root name servers)	ESSENTIAL	ESSENTIAL	ESSENTIAL
	TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
	Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
	Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
ICT-SERVICE MANAGEMENT (B2B)	Managed service providers, managed security service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
PUBLIC ADMINISTRATION ENTITIES	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Of regional governments: risk based (Optional for Member States: of local governments)	IMPORTANT	IMPORTANT	IMPORTANT
SPACE	Operators of ground-based infrastructure (by Member State)	ESSENTIAL	IMPORTANT	NOT IN SCOPE

Annex II: other critical sectors

SECTOR	SUB-SECTOR	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10 million revenue)	SMALL & MICRO ENTITIES
POSTAL AND COURIER SERVICES		IMPORTANT	IMPORTANT	NOT IN SCOPE
WASTE MANAGEMENT	(only if principal economic activity)	IMPORTANT	IMPORTANT	NOT IN SCOPE
CHEMICALS	Manufacture, production, distribution	IMPORTANT	IMPORTANT	NOT IN SCOPE
FOOD	Wholesale production and industrial production and processing	IMPORTANT	IMPORTANT	NOT IN SCOPE
MANUFACTURING	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)	IMPORTANT	IMPORTANT	NOT IN SCOPE
DIGITAL PROVIDERS	online marketplaces, search engines, social networking platforms	IMPORTANT	IMPORTANT	NOT IN SCOPE
RESEARCH	Research organisations (excluding education institutions) (Optional for Member States: education institutions)	IMPORTANT	IMPORTANT	NOT IN SCOPE
ENTITIES PROVIDING DOMAIN NAME REGISTRATION SERVICES	All sizes, but only subject to Article 3(3) and Article 28			

NIS-2 Directive: a stricter cybersecurity regulation for EU public and private sector

“Minimum” Cyber Risk Management measures…

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication

Cybersecurity incidents reporting obligation

24h — EARLY WARNING
Is it a suspected malicious act with potential cross-border impacts?

72h — OFFICIAL INCIDENT NOTIFICATION
Assessment of the incident, severity and impact, plus indicators of compromise.

as requested — INTERMEDIATE STATUS REPORT
At the request of CSIRT or relevant competent authority.

1 month — FINAL REPORT
Or if incident ongoing at time of final report a progress report and final report 1 month after end

Each member state will define NIS 2 requirements by 17.10.2024

EU CRA (Cyber Resilience Act)
The new EU cybersecurity regulation for products with digital elements

Cybersecurity is taken into account in **planning, design, development, production, delivery** and **maintenance** phase;

All **cybersecurity risks** are documented;

Manufacturers will have to **report actively exploited vulnerabilities and incidents**;

Once sold, manufacturers must ensure that for the **duration of the support period**, **vulnerabilities are handled effectively**;

Clear and understandable instructions for the use of prod with digital elements;

Security updates to be made **available to users for the time the product is expected to be in use**.

Harmonised rules for the placing on the market of connected hardware and software products;

Essential cybersecurity requirements for the design and development of products with digital elements as well as obligations for all economic operators in the value chain;

Harmonised rules for the duty of care for the whole life cycle of products with digital elements.

Entry into force in late 2024 with applicability 36 months after for product requirements and 21 months after for reporting obligations

Any Question?

Thank you!