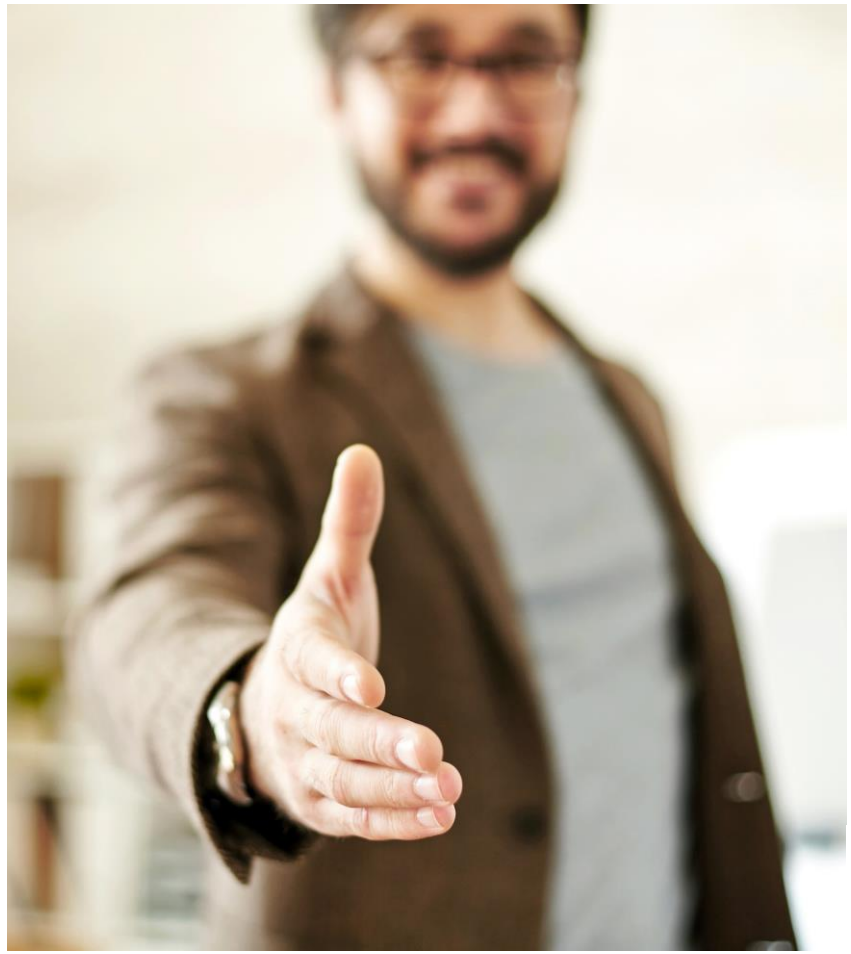
Data security, privacy and ethics in smart buildings

Elena Chochanova & Tousif Rahman | TNO | Feb 16, 2023

The project received funding from Dutch Ministry of Economic Affairs and Climate Policy and Ministry of the Interior and Kingdom Relations under the MOOI program

Contents

Welcome & introduction



Elena Chochanova

Consultant Digitalisation & Building Information

Contact info:

E-mail: elena.chochanova@tno.nl

Tel: +31 6 21 98 42 72

Tousif Rahman

Specialist in BIM, Data & Digitalisation

Contact info:

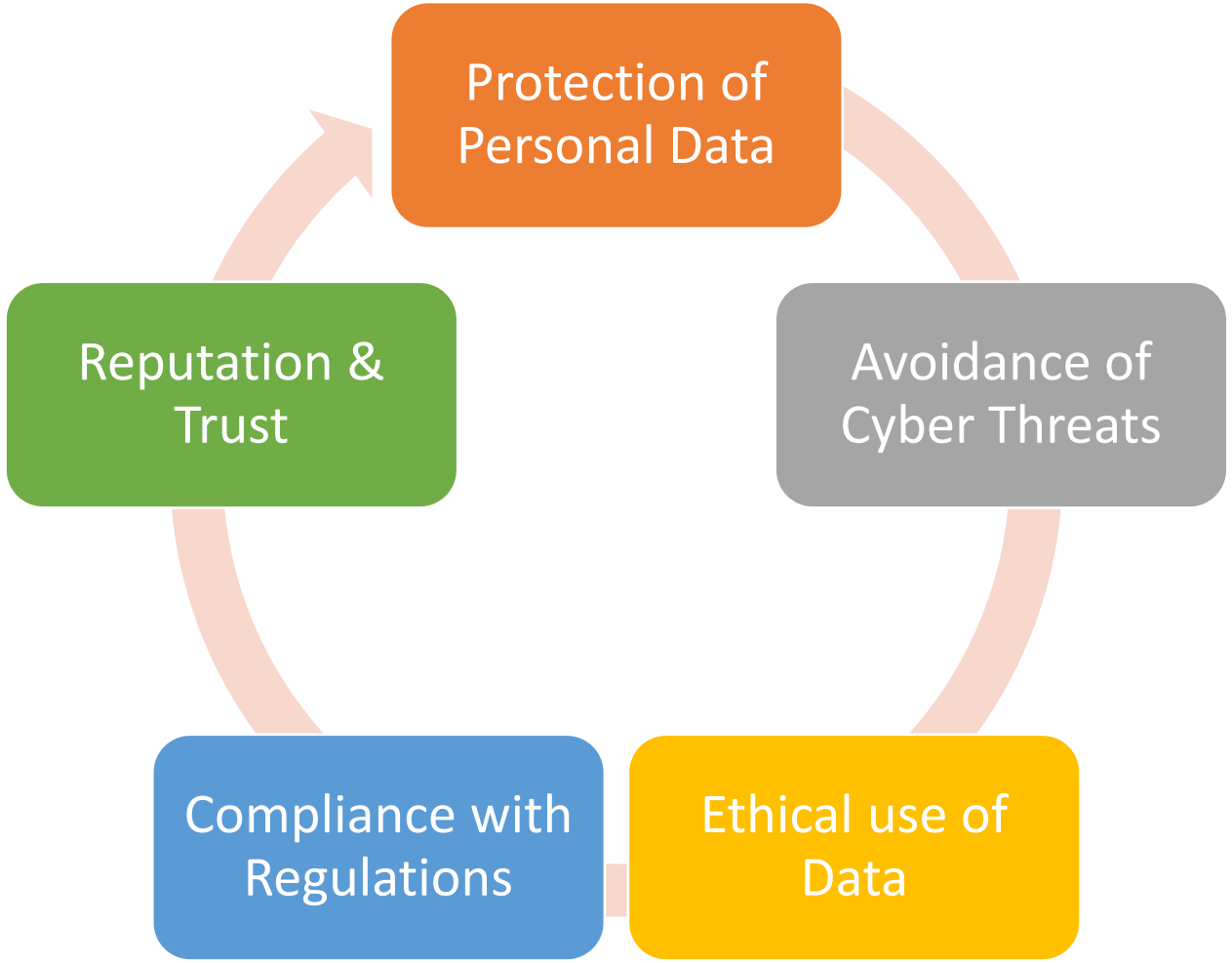
E-mail: tousif.rahman@tno.nl

Tel: +31 6 25 23 83 18

TNO innovation for life

info@tno.nl
www.tno.nl

Why data privacy security & ethics



It is crucial to ensure that this data is collected, stored, and processed in a way that protects the privacy of the occupants. Failure to do so could result in data breaches, unauthorized access, or even identity theft.

Hackers can exploit security vulnerabilities in the building's network and gain access to sensitive data, compromise building control systems, or even cause physical harm to occupants. It is important to implement robust cybersecurity measures to prevent such attacks.

It is important to ensure that this data is used ethically and with the consent of the occupants. For example, the data should not be used to discriminate against certain groups or individuals, or to violate their privacy rights

GDPR in the European Union, that require organizations to implement measures to protect personal data. Failure to comply with these regulations can result in fines, legal action, or damage to the organization's reputation

A smart building that prioritizes data privacy, security, and ethics will earn the trust of its occupants and stakeholders. This can lead to increased occupancy rates, higher rental rates, and improved financial performance.

Smart buildings and Industry 4.0

Industry 4.0, based on concepts and technologies that include cyber-physical systems, the Internet of Things (IoT), and the internet of services. It is also based on the **perpetual communication of technology and people via the internet** that allows a continuous interaction and exchange of information between:

- Humans and other humans
- Humans and machines
- Machines and other machines

Image source: Industry 4.0, What does it involve? (ATRIA Innovation)

Source: Chen, Y.; Huang, D.; Liu, Z.; Osmani, M.; Demian, P. Construction 4.0, Industry 4.0, and Building Information Modeling (BIM) for Sustainable Building Development within the Smart City. Sustainability 2022, 14, 10028. https://doi.org/ 10.3390/su141610028

Smart buildings and Industry 4.0

1st industrial revolution

Mechanization

Steam & water power.

2nd industrial revolution

Electrification

Mass production

3rd industrial revolution

Automation

Electronic & IT systems

4th industrial revolution

Digitalization

Cyber physical systems, IoT

1784

1870

1969

2014

“Smart” things are everywhere

Image source: Ikea Tradfri slimme verlichting (elektrozine.be)

Image source: Ezewarm Pro Wifi Thermostat (Ezewarm)

Image source: Samsung Family Hub Refrigerator (Samsung US Newsroom)

Image source: Choosing The Best Voice Assistant For Your Home (GeeksFL)

Data in smart buildings

- IoT
  - Numerous devices that produce data
  - Devices connected to the internet
- Interconenctivity
  - Multiple connections
  - Multiple access points
- Data sharing
  - Local data storage
  - Remote data storage
  - Data defragmentation
  - Limited data governance
- Flexibility
  - Changing protocols
  - Lack of oversight

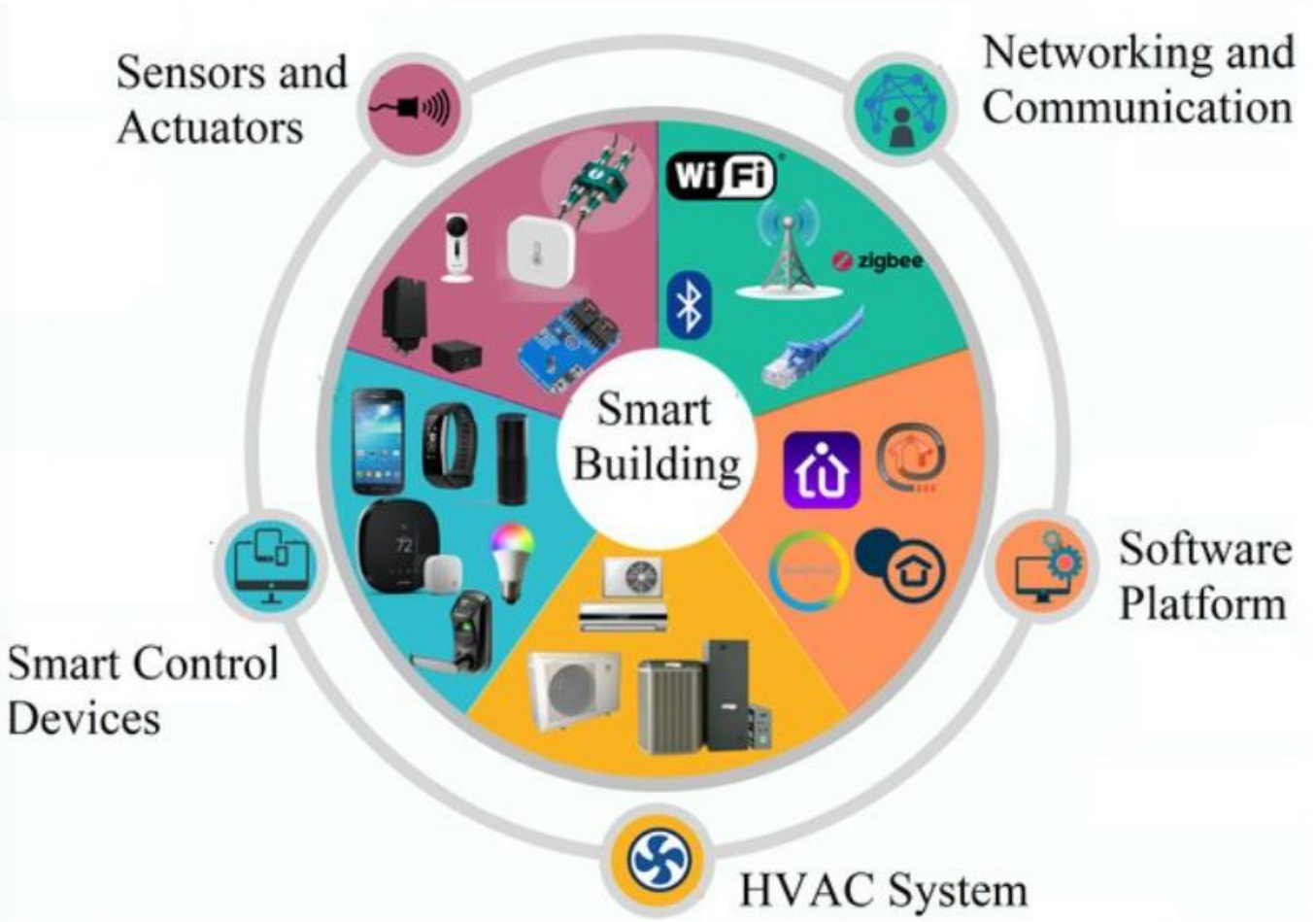


Image source: Leveraging Machine Learning and Big Data for Smart Buildings: A Comprehensive Survey (researchgate.net)

Data security

The act of **protecting digital assets** from attacks that aim to:

- Obtain, alter or damage (sensitive) data,
- Extract money from users (e.g. by applying ransomware)
- Hinder regular business or industrial processes
- Place human life or wellbeing in danger (directly or indirectly)

Data security - scope

It encompasses every aspect of information security, including:

- physical security of hardware and storage devices,
- administrative and access controls,
- logical security of software applications,
- organizational policies and procedures.

Data Security - key dimensions

- **Confidentiality**

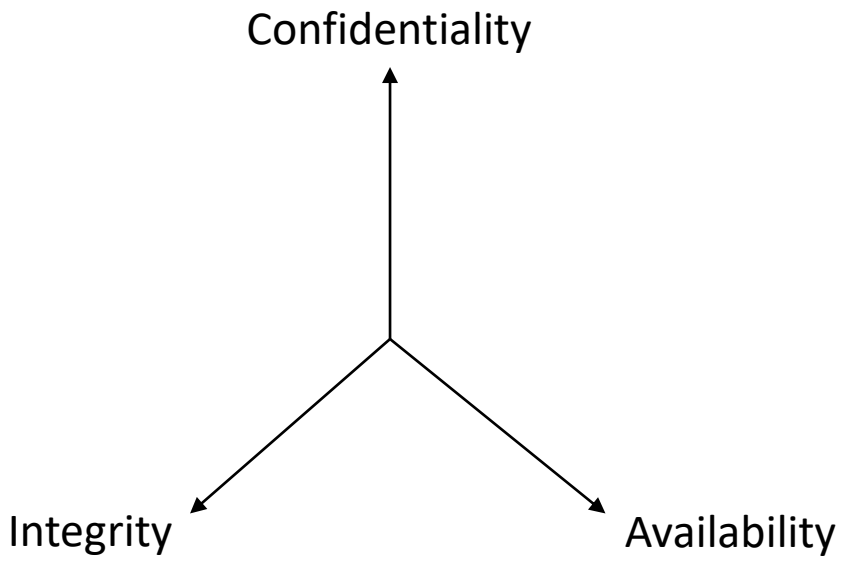
Ensures that data is accessed only by authorized users with the proper credentials.

- **Integrity**

Ensure that all data stored is reliable, accurate, and not subject to unwarranted changes.

- **Availability**

Ensures that data is readily — and safely — accessible and available for ongoing business needs.



Data Privacy

Image source: CCPA: What is Personal Information? (truevault.com)

Giving individuals the power to control their personal data is internationally recognized as a **basic human right**.

Personal data includes things like:

- name,
- contact data,
- location,
- any data describing a natural person's physical, physiological, mental, economic, cultural, or social identity (e.g. age, sex, religion, etc.)

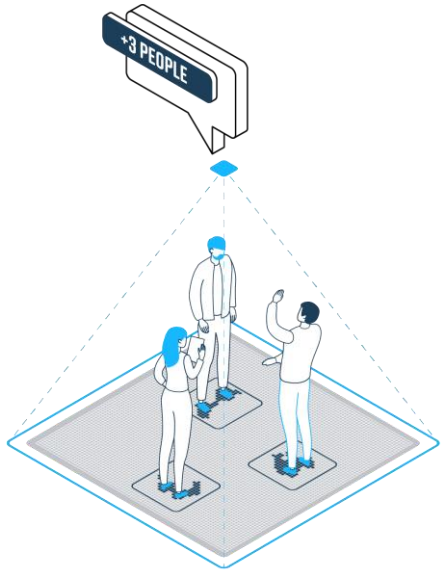
The General Data Protection Regulation (GDPR) is enforced since **May 25th, 2018**

Data privacy

Summarized in six data protection principles of the GDPR.

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

Data privacy in Smart Buildings



When do we collect personal data in smart buildings?

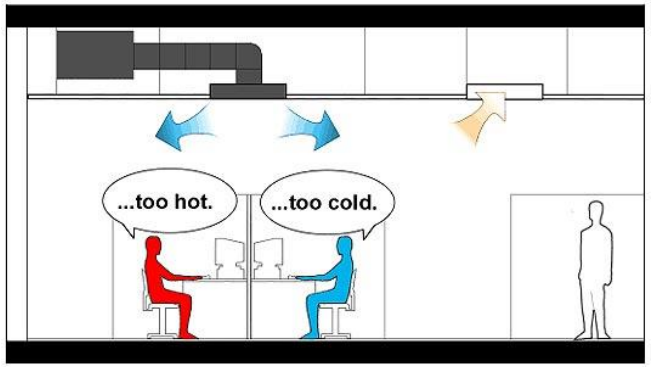
1. Occupancy

- anonymous information is collected

  ➔ no privacy concerns

- information crossed referenced with other data can be traced back to individuals

  ➔ subject to GDPR



2. Occupants' behaviors and comfort requirements

- stored personal preferences, e.g. for optimizing energy use

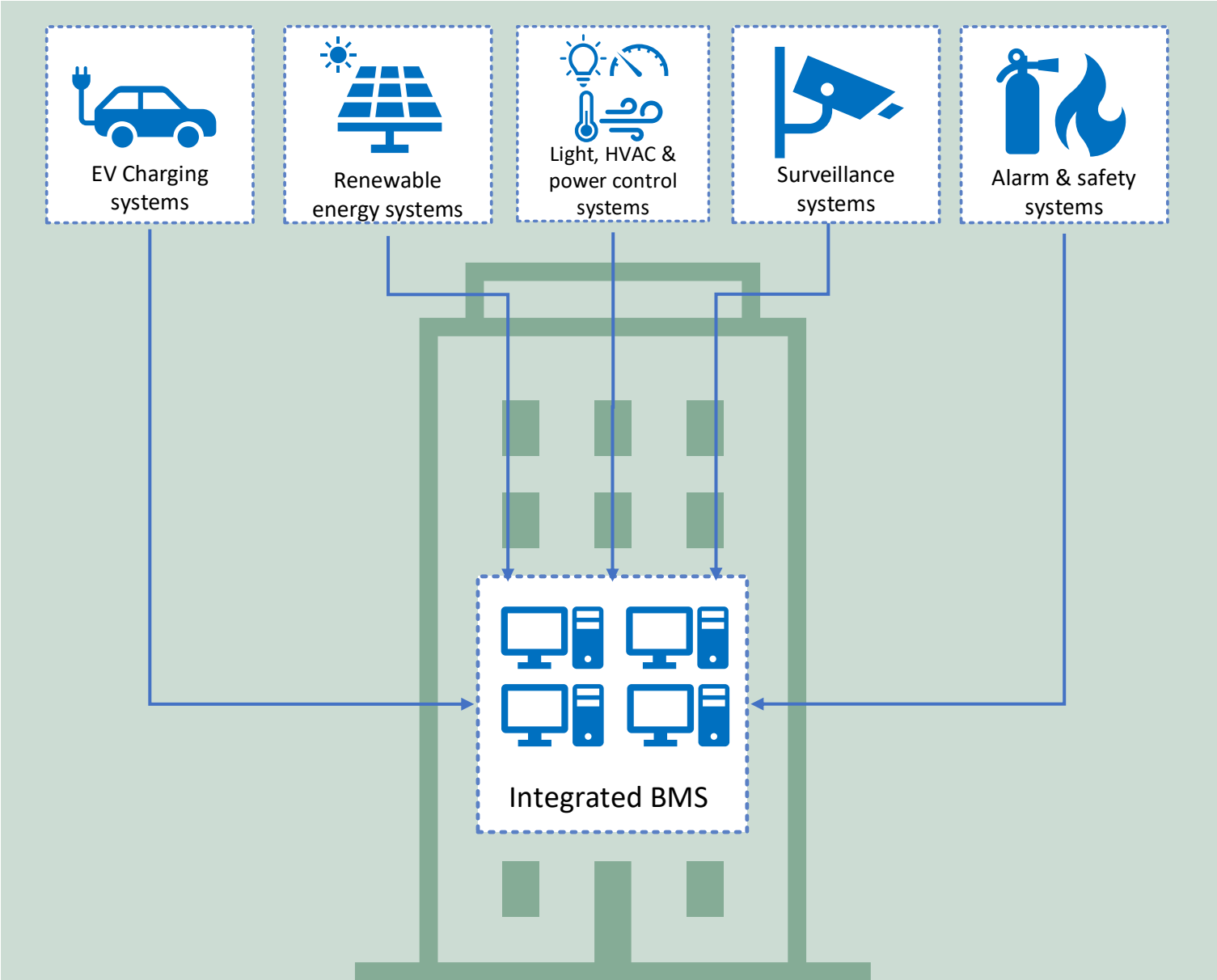
  ➔ subject to GDPR

Image sources: Explaining the Types of Anonymous Occupancy Sensors (CoWorkr); Underfloor Technology Thermal Comfort (berkeley.edu)

Data Ethics

- Data ethics involves applying ethical principles, such as fairness, transparency, and respect for privacy, to the collection, analysis, and use of data.
- In smart buildings, data ethics is particularly important to protect the safety and privacy of occupants, comply with regulations, and earn the trust of stakeholders.
- Key issues in data ethics in smart buildings include informed consent, privacy, bias and discrimination, transparency, and accountability.
- By prioritizing data ethics in smart buildings, we can ensure that data is used in a responsible and ethical manner, and that the potential benefits of data use are balanced with the potential risks and consequences.

Buildings systems & OT in Smart Buildings



A building system is a control system for managing and operating a building. It is usually comprised of individual sub-systems

Some misconceptions

<u>Building systems…</u>

× …are unlikely to become targets of cyberattacks

‼ Cyberattacks targeting building systems have been reported globally

× …are isolated from the Internet

‼ Ever more building systems are now connected to the Internet to improve their facilities

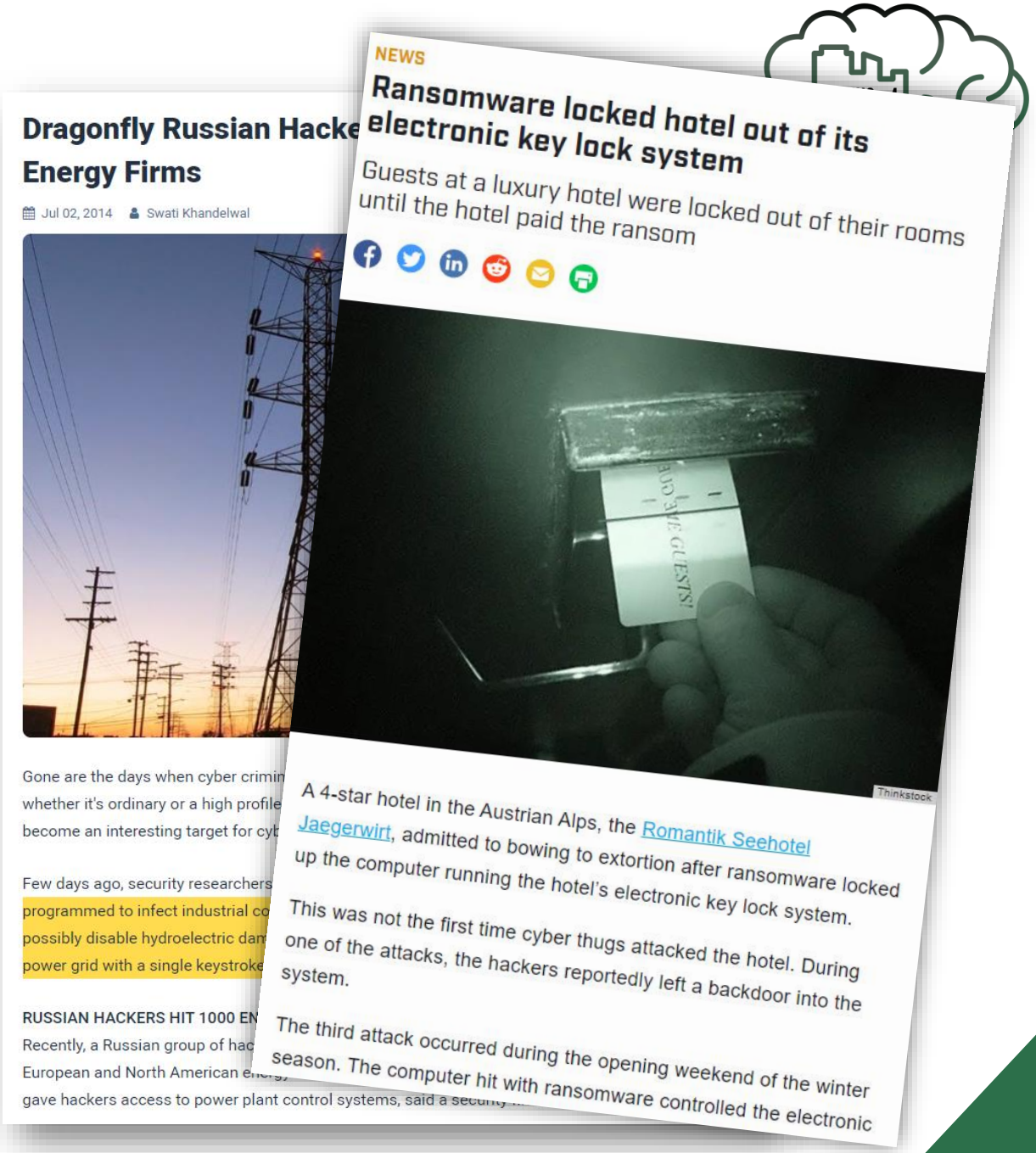
× …use special protocols to communicate with each other and therefore are exempt from cyber attacks

‼ This is no longer a guarantee as cyberattack techniques keep advancing

Examples of cyber attacks

A recent report indicated that in 2019 nearly 40 percent of 40,000 smart buildings were impacted by a cyberattack.[1]

- 70% of IoT devices are still using the factory-set default passwords.
- Most IoT devices are often too critical to stop operations for software updates
- BAS systems are not sufficiently protected

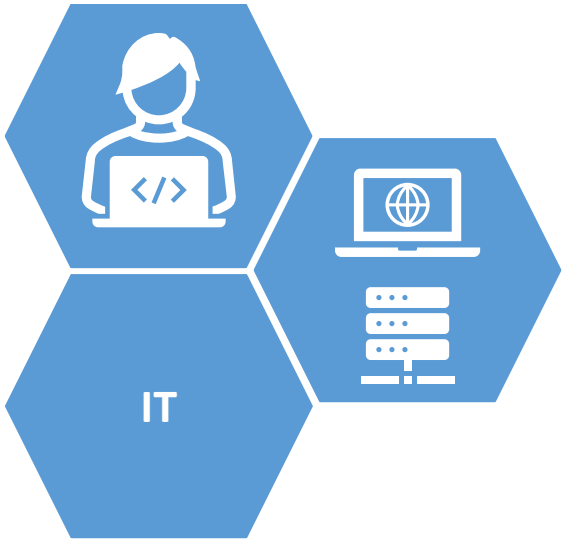


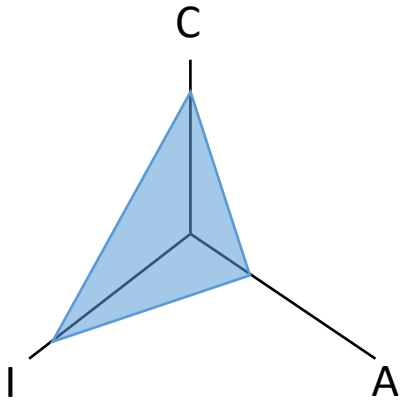
[1] Source: Nearly Four in Ten Smart Buildings Targeted by Malicious Attacks in H1 2019 | Kaspersky

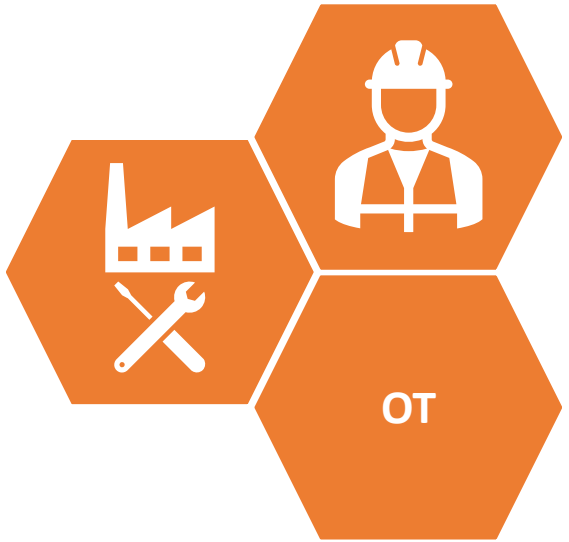
OT & IT in smart buildings

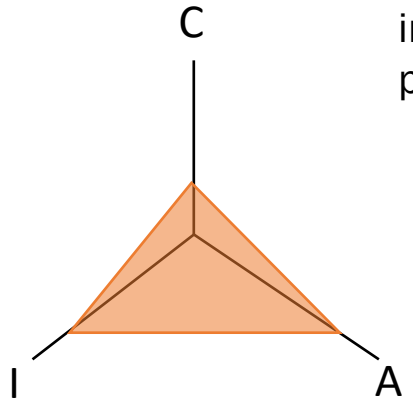
Information Technology (IT)

The entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services.





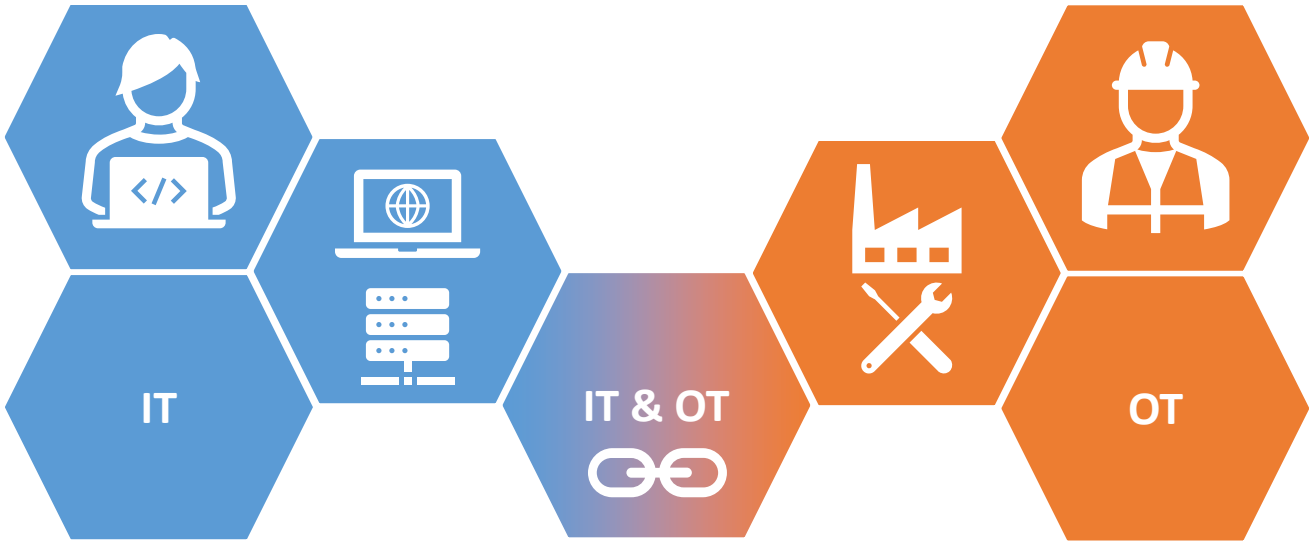




Operational Technology (OT)

The hardware and software used to detect and control physical devices, processes, and events. OT incorporates a range of programmable systems and equipment that interacts with the physical world.

OT & IT in smart buildings



The convergence of OT and IT has caused a shift from traditional OT to an OT that:

1. is no longer isolated from IT
2. does no longer run on proprietary protocols but runs on common internet protocols instead
3. runs in general purpose software
4. Runs mainstream IT operating systems
5. Is increasingly connected to wireless technologies

Existing standards

- ISO 27000 series
- IEC 62443 series
- NIST Cybersecurity Framework (CSF)
- ISO 31000

Existing standards

- ISO 27000 series

Information technology – Security techniques
Information security management systems

- IEC 62443 series
- NIST Cybersecurity Framework (CSF)
- ISO 31000

Image source: (PDF) GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking (researchgate.net)

Existing standards

- ISO 27000 series
- IEC 62443 series

Industrial communication networks - Network and system security

- NIST Cybersecurity Framework (CSF)
- ISO 31000

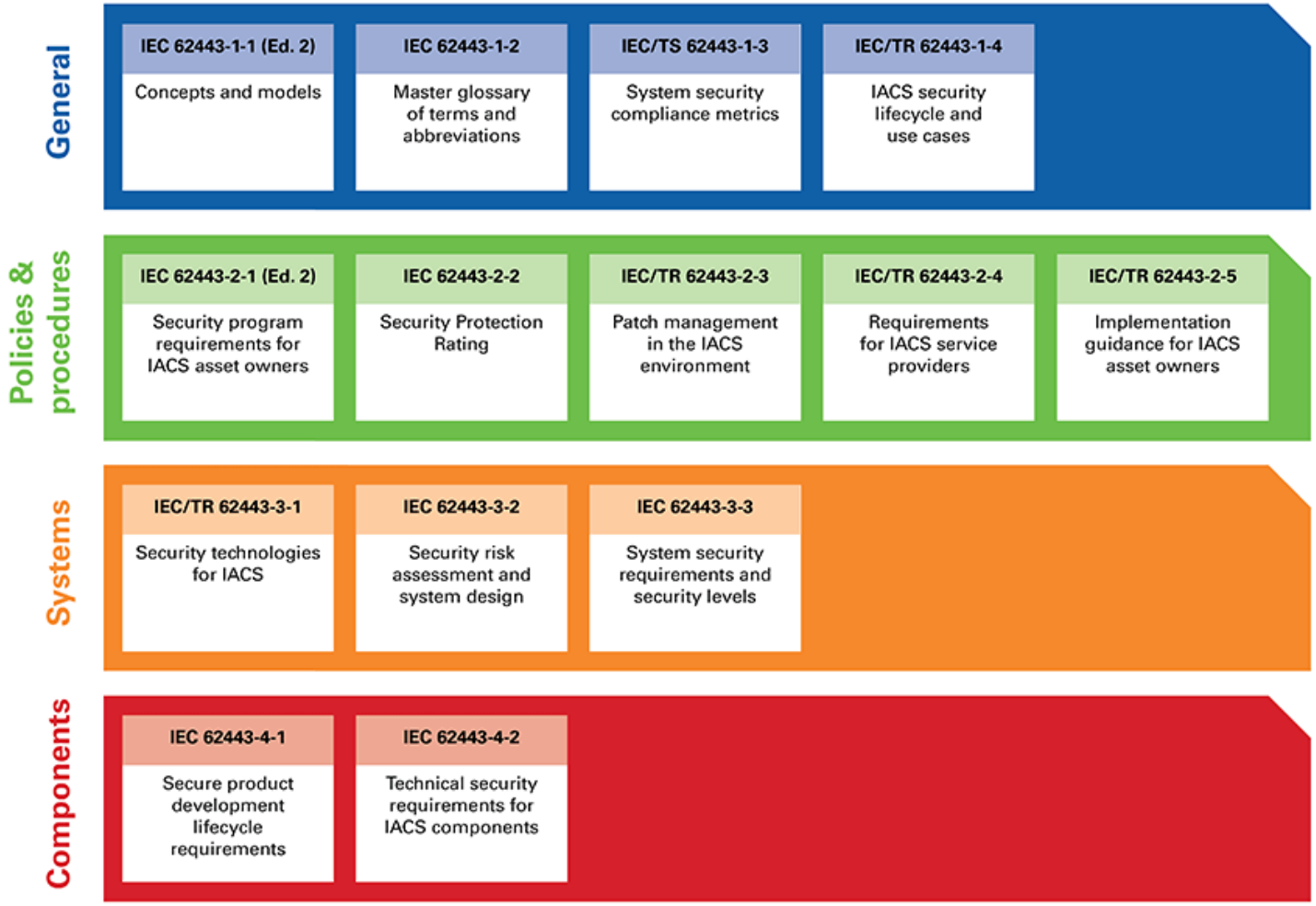


Image source: IEC 62443 certification, get the cyber security certificate for IACS (kiwa.com)

Existing standards

- ISO 27000 series
- IEC 62443
- NIST Cybersecurity Framework (CSF)
- ISO 31000

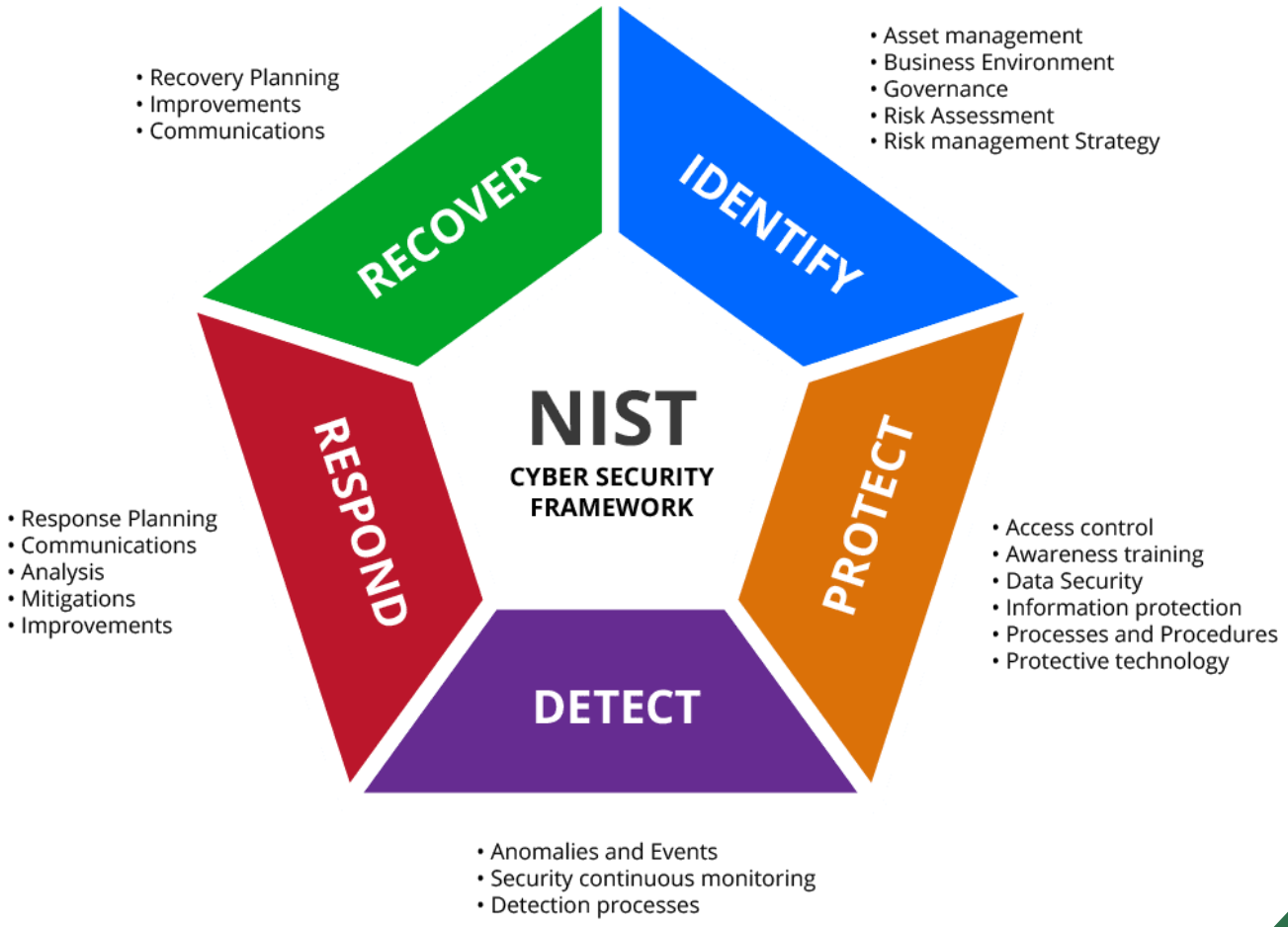


Image source: NIST Support - CorCystems

Existing standards

- ISO 27000 series
- IEC 62443 series
- NIST Cybersecurity Framework (CSF)
- ISO 31000

Risk management - Guidelines

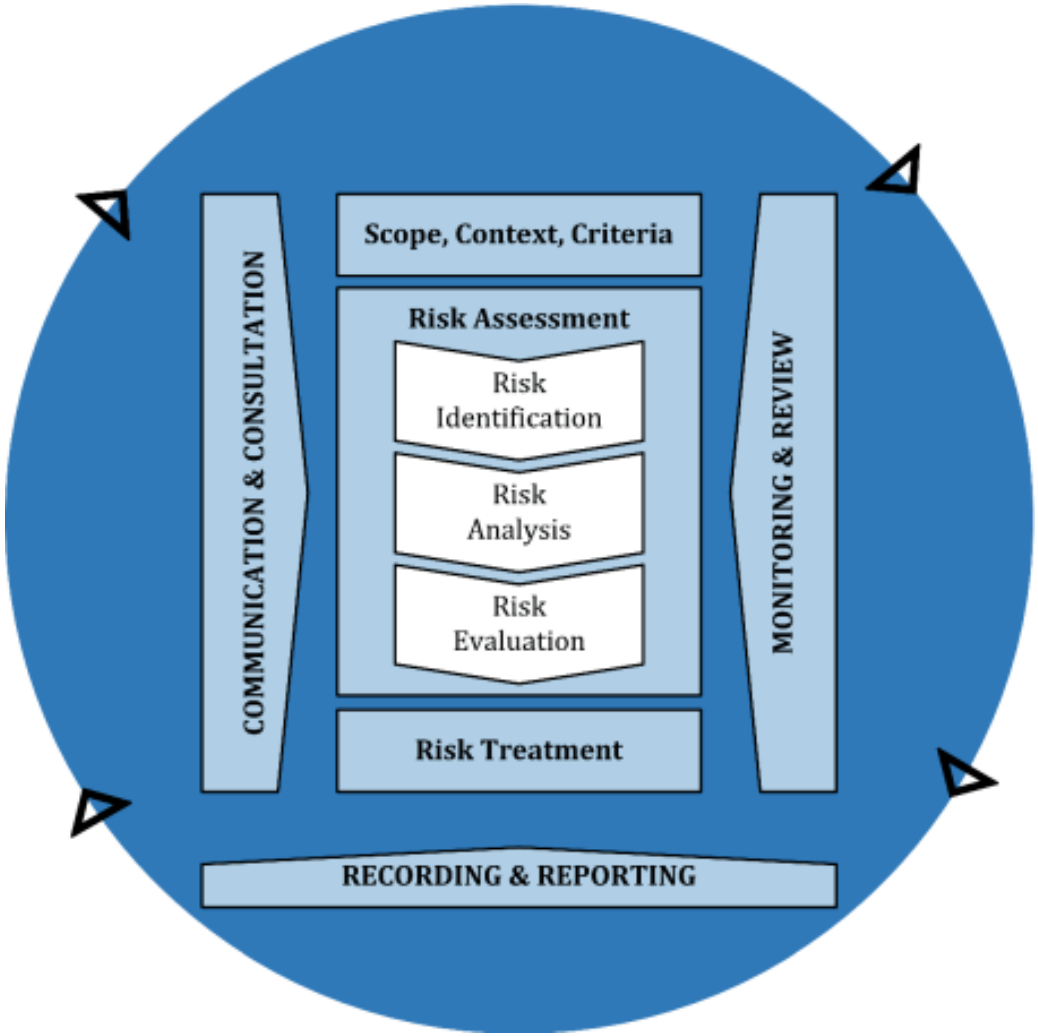
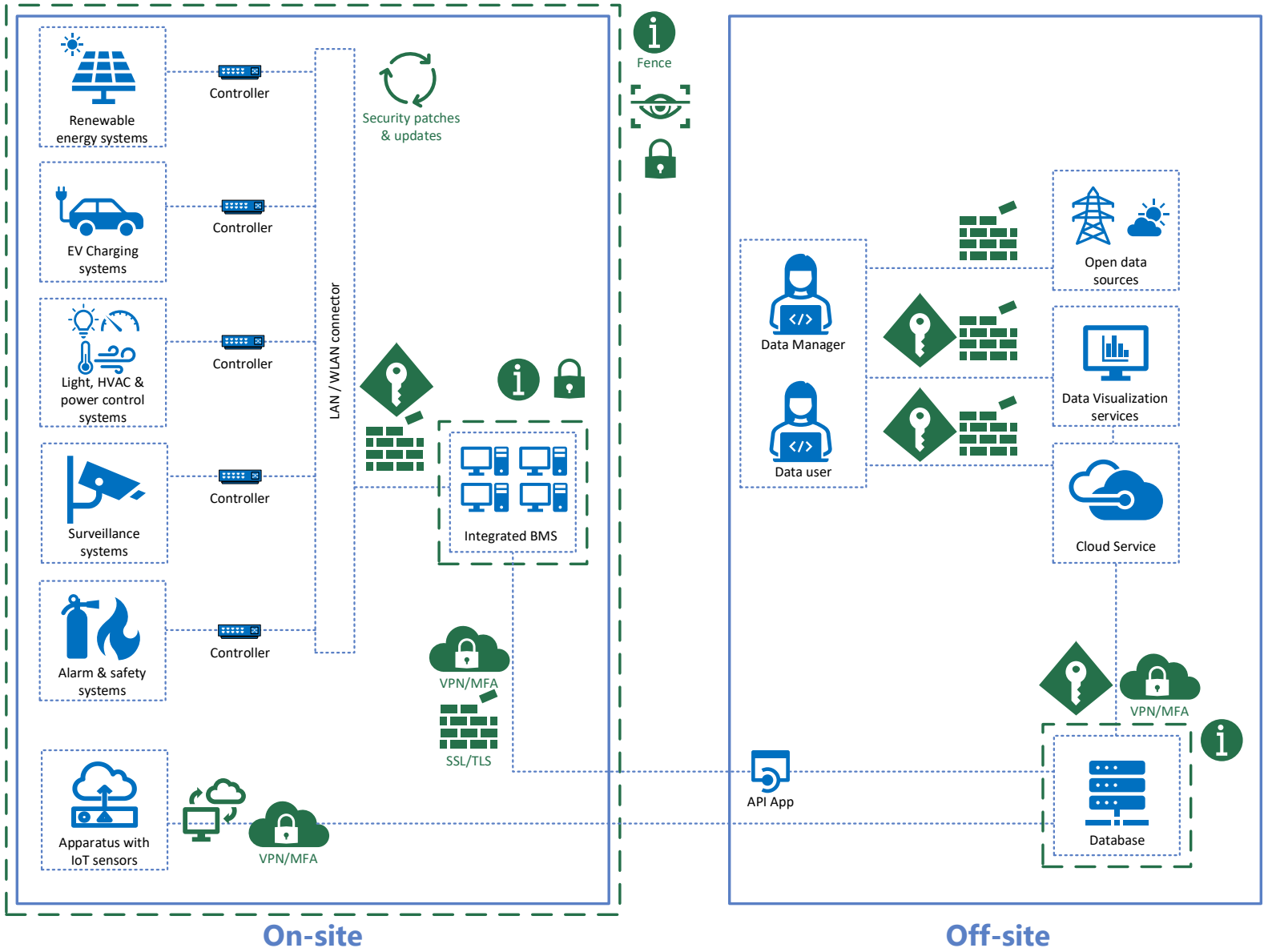


Image source: NEN Connect - NEN-ISO 31000:2018 en

Data security measures



Digital access control
e.g. internet access, VPN connection

Physical access control
e.g. physical locks, doors, etc.

Regular updates
For software and firmware

Digital authorization & authentication
e.g. Multi-factor authentication

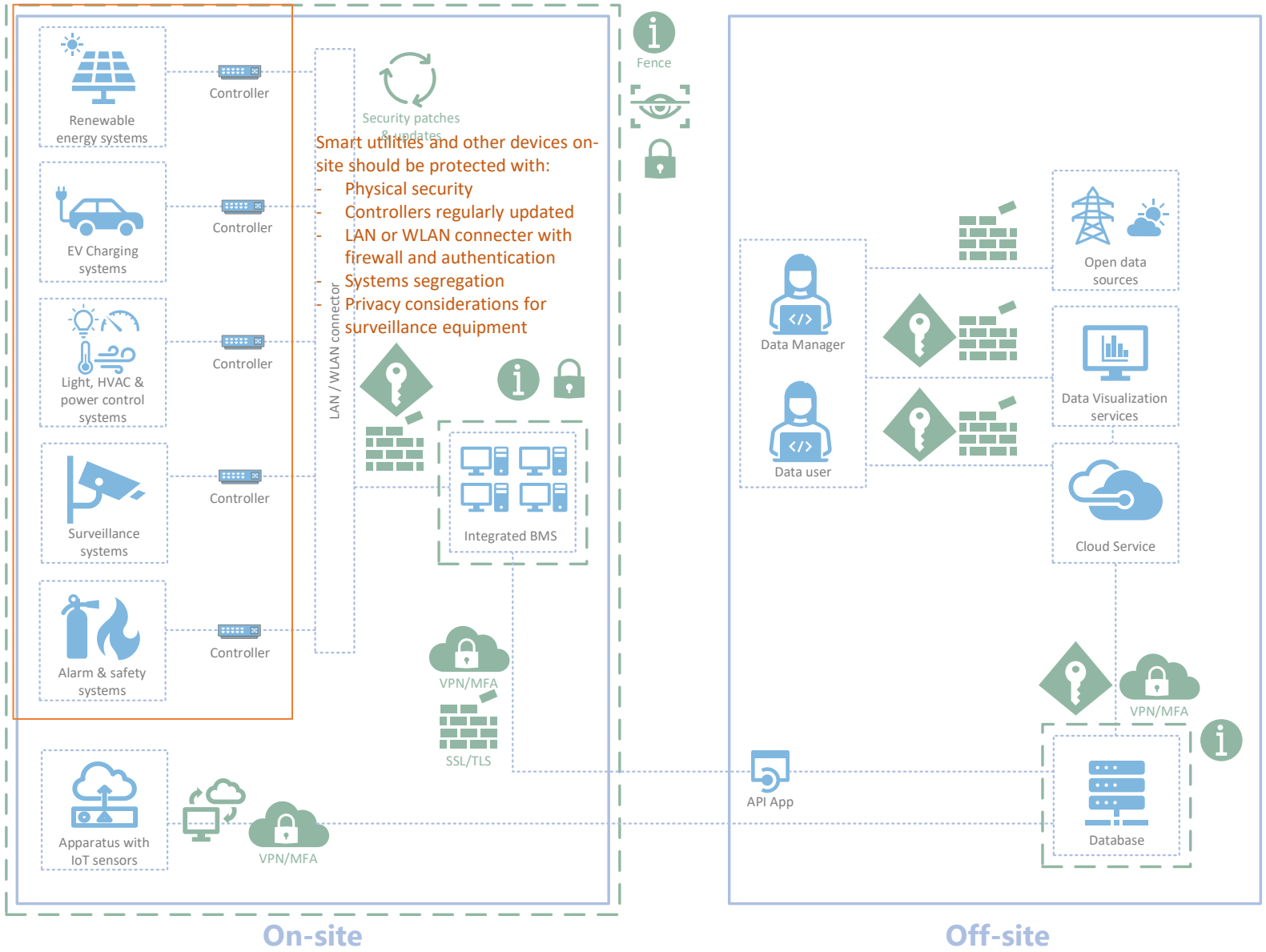
Physical authorization & Authentication
e.g. personalized key /pass, fingerprint scan

Firewall

Data backup

Other

Data security measures



Digital access control
e.g. internet access, VPN connection

Physical access control
e.g. physical locks, doors, etc.

Regular updates
For software and firmware

Digital authorization & authentication
e.g. Multi-factor authentication

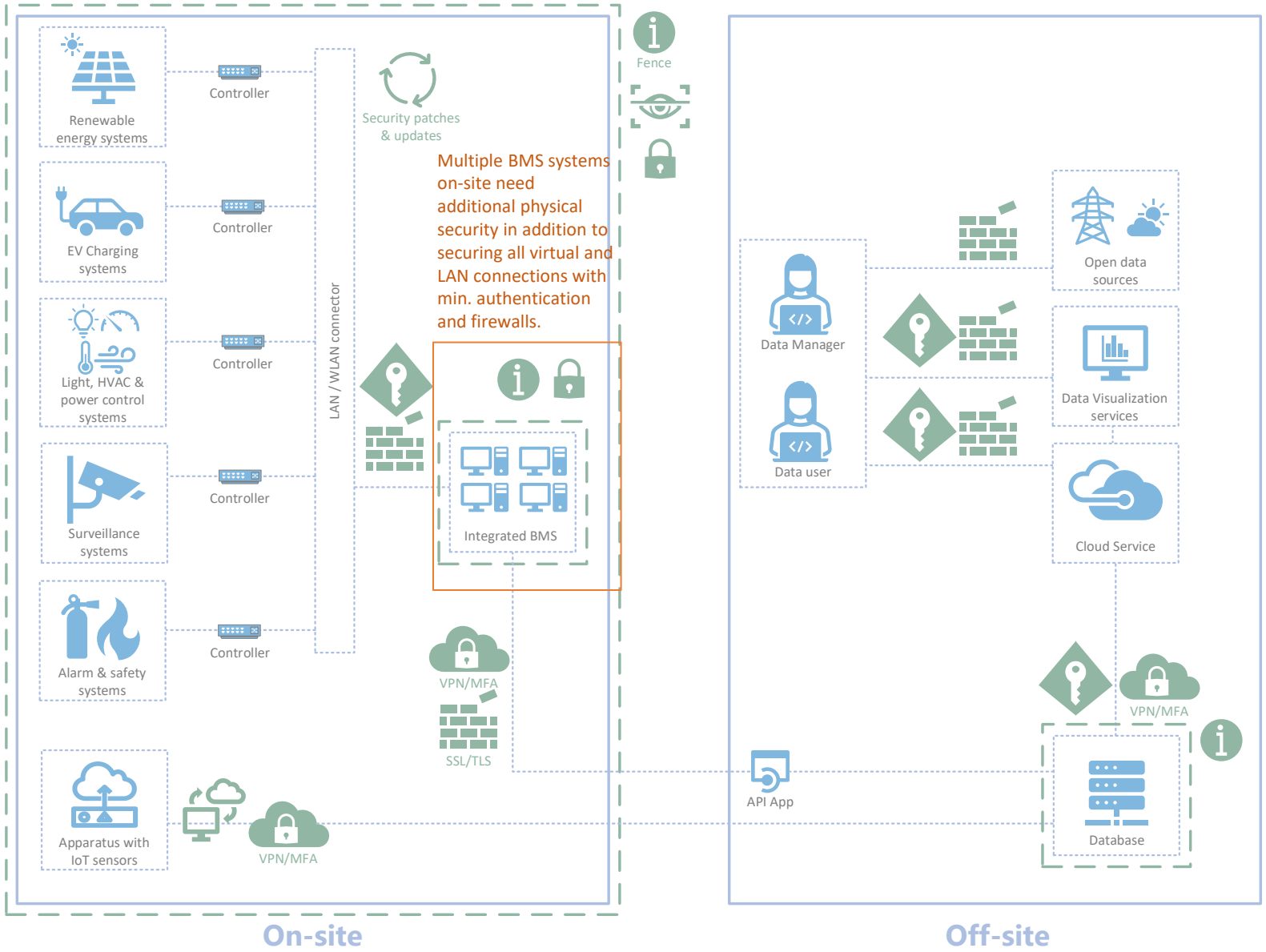
Physical authorization & Authentication
e.g. personalized key /pass, fingerprint scan

Firewall

Data backup

Other

Data security measures



Digital access control
e.g. internet access, VPN connection

Physical access control
e.g. physical locks, doors, etc.

Regular updates
For software and firmware

Digital authorization & authentication
e.g. Multi-factor authentication

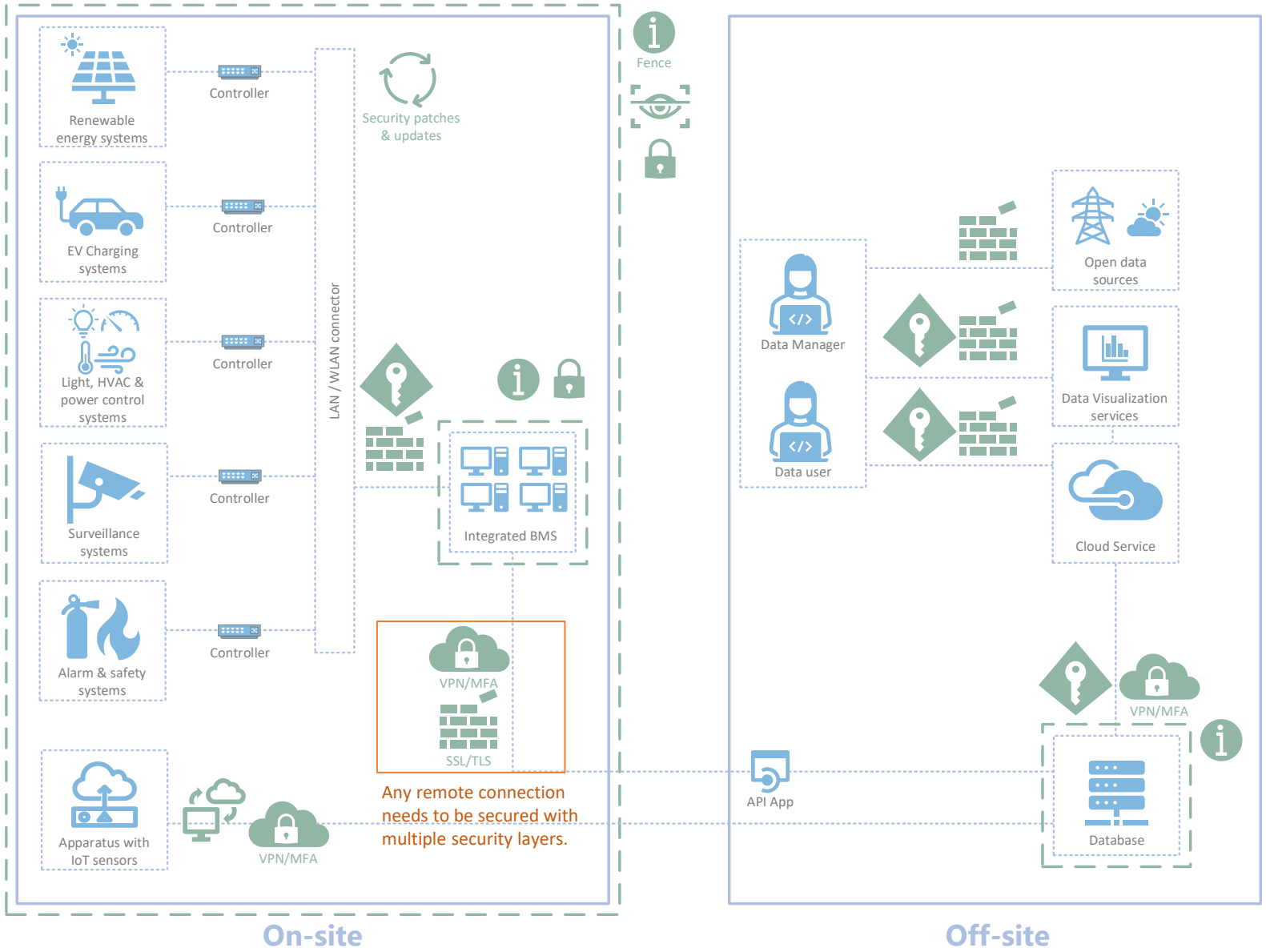
Physical authorization & Authentication
e.g. personalized key /pass, fingerprint scan

Firewall

Data backup

Other

Data security measures



Digital access control
e.g. internet access, VPN connection

Physical access control
e.g. physical locks, doors, etc.

Regular updates
For software and firmware

Digital authorization & authentication
e.g. Multi-factor authentication

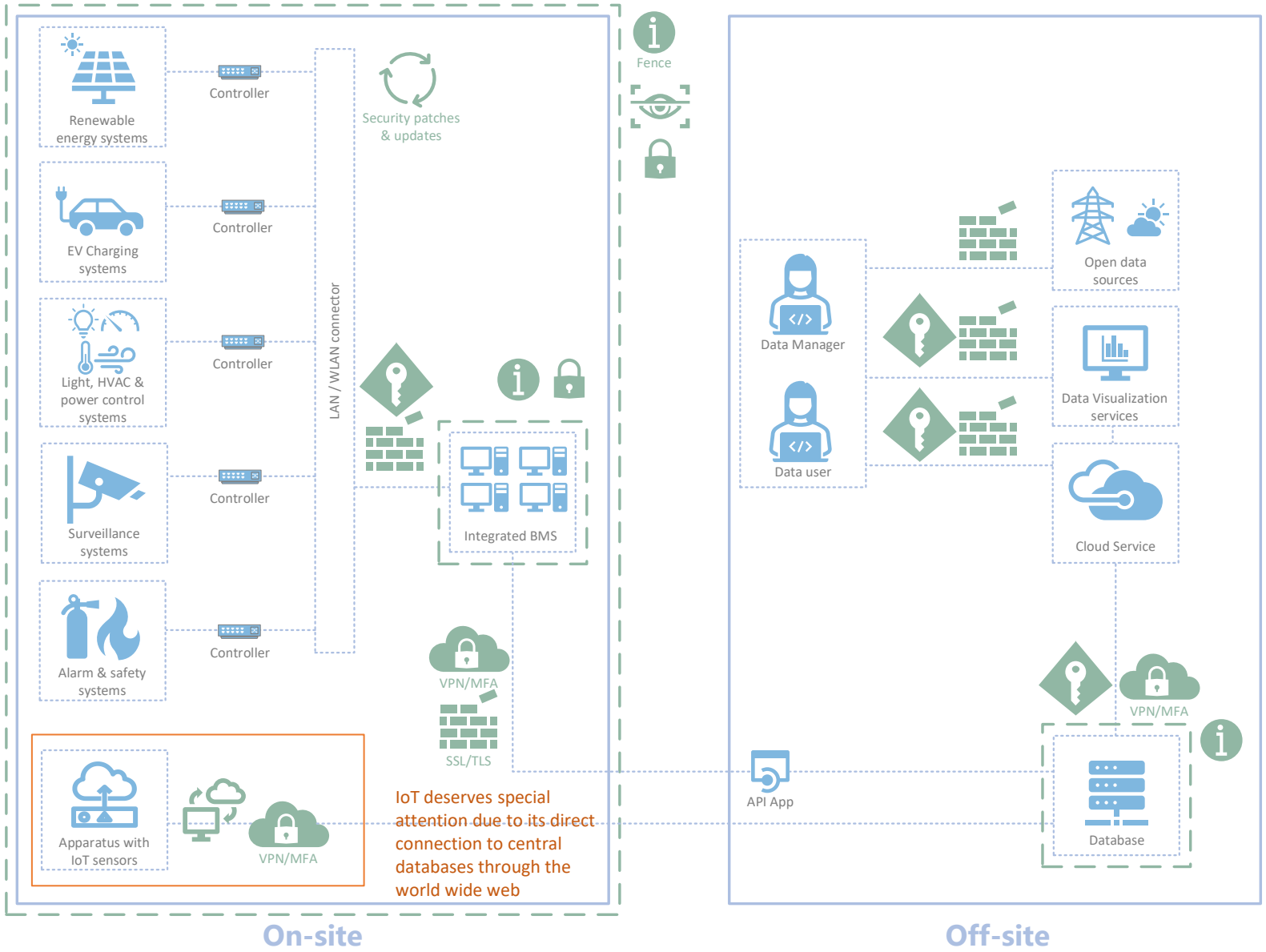
Physical authorization & Authentication
e.g. personalized key /pass, fingerprint scan

Firewall

Data backup

Other

Data security measures



Digital access control
e.g. internet access, VPN connection

Physical access control
e.g. physical locks, doors, etc.

Regular updates
For software and firmware

Digital authorization & authentication
e.g. Multi-factor authentication

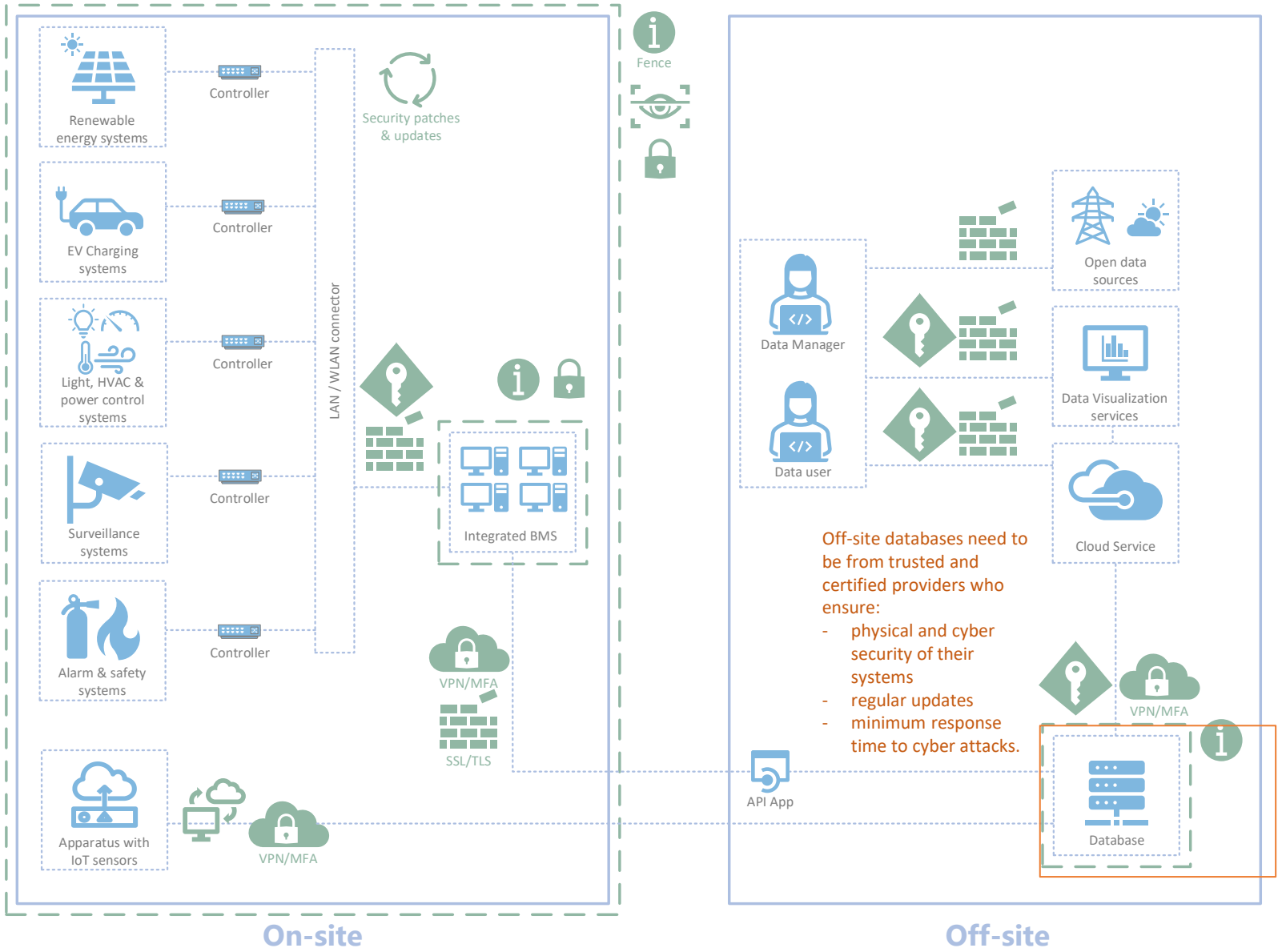
Physical authorization & Authentication
e.g. personalized key /pass, fingerprint scan

Firewall

Data backup

Other

Data security measures



Digital access control
e.g. internet access, VPN connection

Physical access control
e.g. physical locks, doors, etc.

Regular updates
For software and firmware

Digital authorization & authentication
e.g. Multi-factor authentication

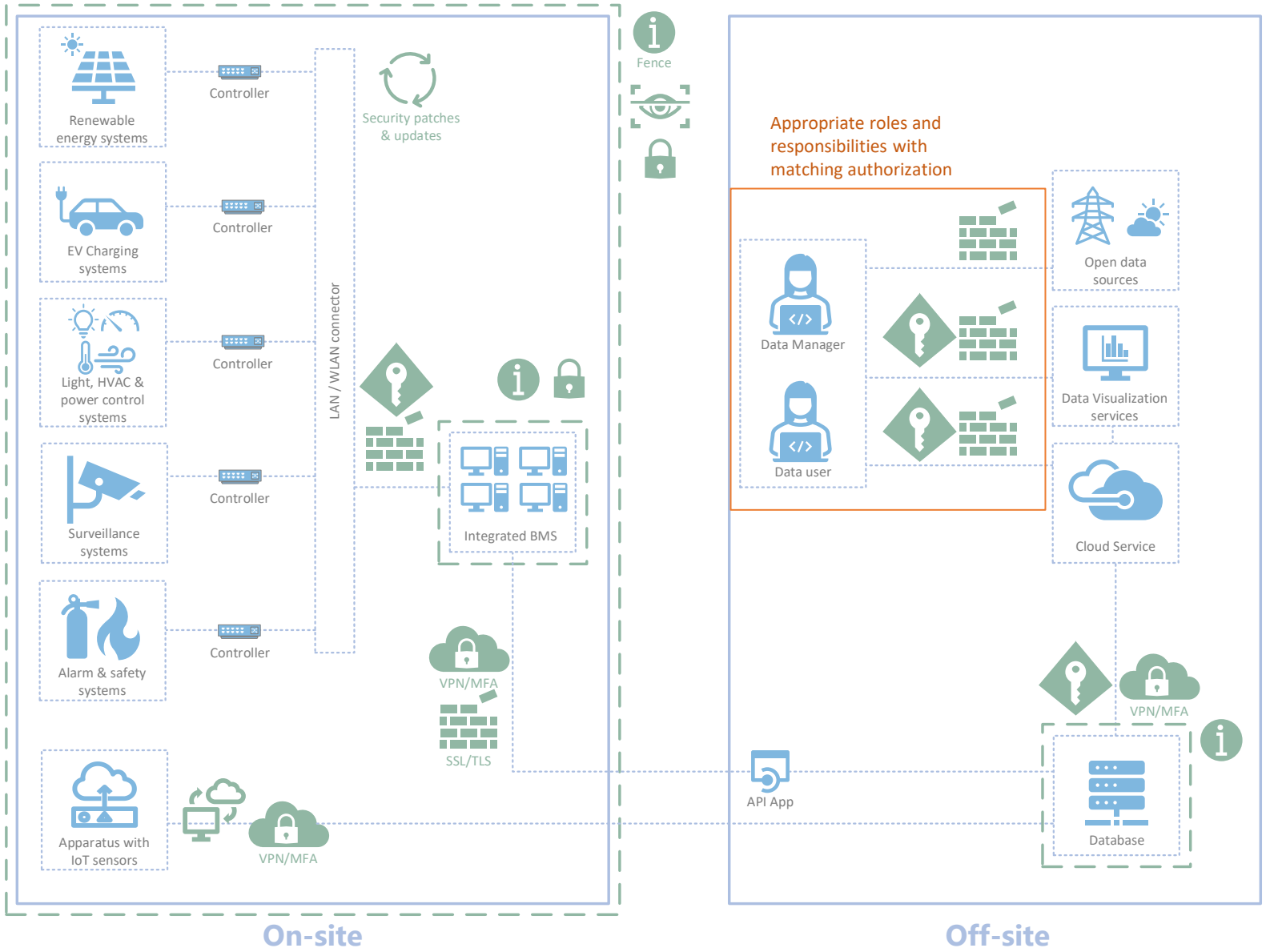
Physical authorization & Authentication
e.g. personalized key /pass, fingerprint scan

Firewall

Data backup

Other

Data security measures



Digital access control
e.g. internet access, VPN connection

Physical access control
e.g. physical locks, doors, etc.

Regular updates
For software and firmware

Digital authorization & authentication
e.g. Multi-factor authentication

Physical authorization & Authentication
e.g. personalized key /pass, fingerprint scan

Firewall

Data backup

Other

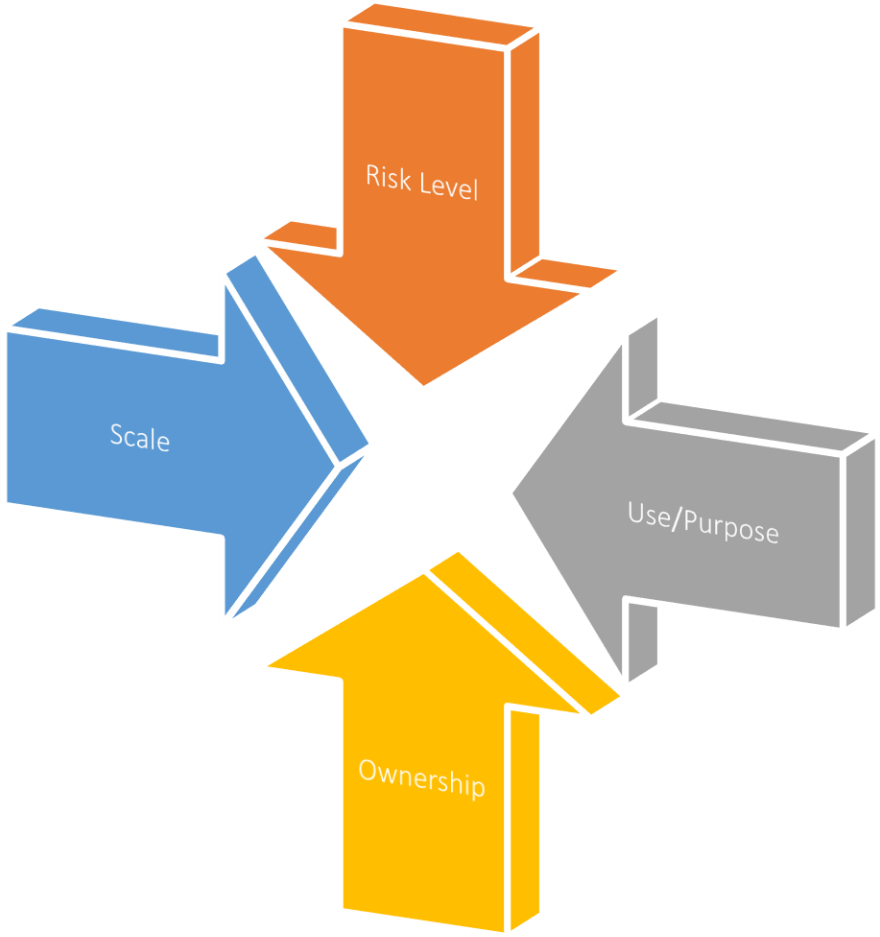
Recommendations for safer smart buildings

Many and diverse stakeholders:

- building owners
- general contractors (and subcontractors)
- architects
- individual system business operators
- building management companies
- tenants
- service providers
- municipalities, other agencies
- other…

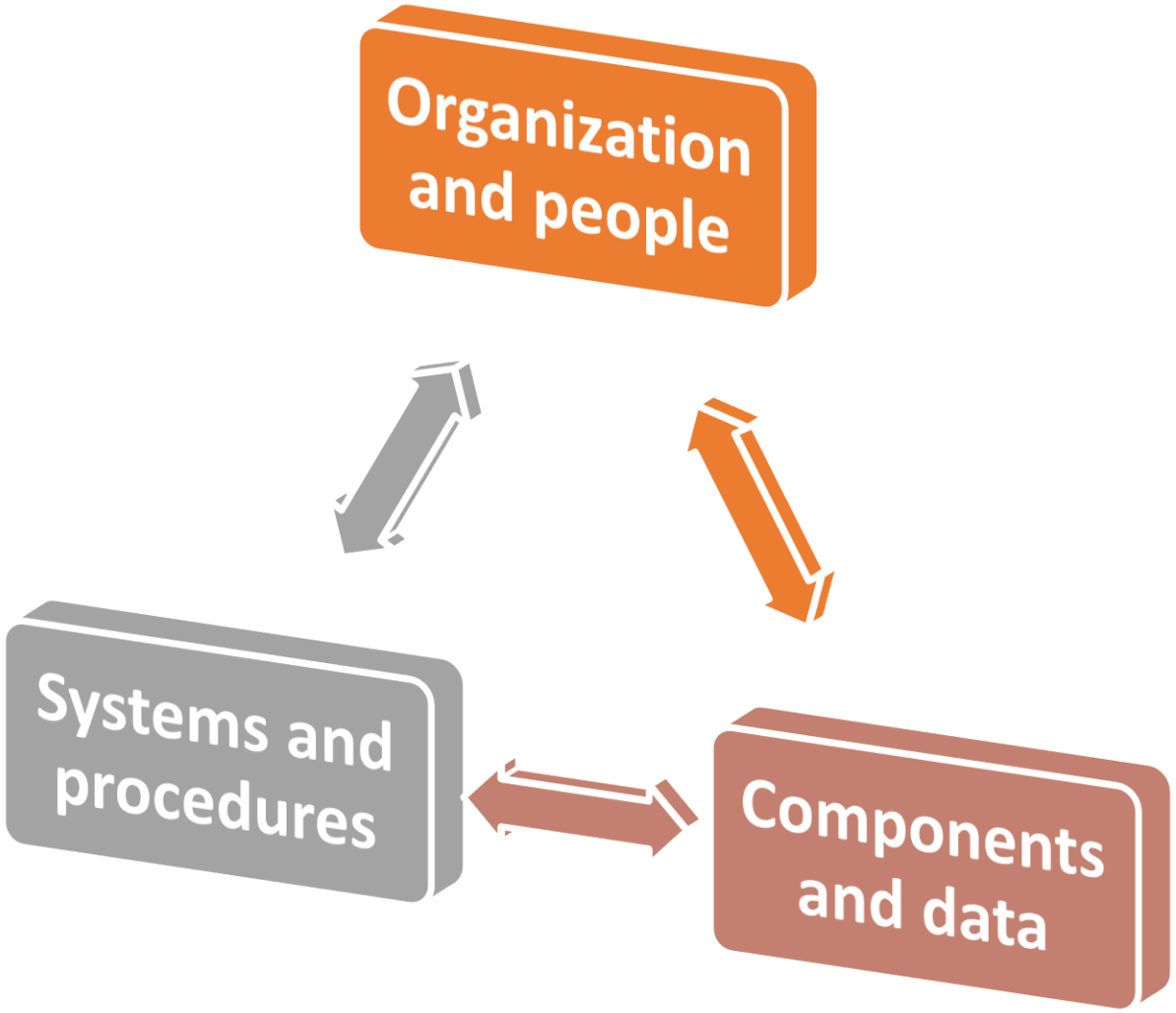
Recommendations for safer smart buildings

Define the necessary security level of the building based on several fixed parameters



Recommendations for safer smart buildings

Establish security measures to match the risk level on the three dimensions:



Recommendations for safer smart buildings

Organization and People

- Awareness
- Training
- Roles
- Trust

Components and Data

- Software and hardware security
- Data flows
- Procurement

Systems and Procedures

- Data governance procedures in place
- All data flows

Paving the way for Industry 5.0

1st industrial revolution

Mechanization

Steam & water power.

2nd industrial revolution

Electrification

Mass production

3rd industrial revolution

Automation

Electronic & IT systems

4th industrial revolution

Digitalization

Cyber physical systems, IoT

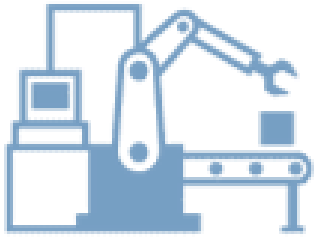
5th industrial revolution

Humanization

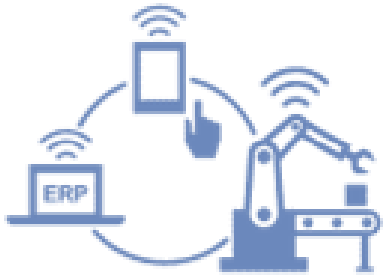
Cyber-physical cognitive systems

1784

1870



1969



2014

20XX

Thank you for your attention.