| | |
|---|---|
| Project acronym | B4B |
| Project full name | Brains for Building's Energy Systems |
| Grant No | M00I32004 |
| Project duration | 4 year (Starting date May 1, 2021) |

# Deliverable D4.05

## Privacy, ethics, and security framework with a view to increasing market acceptance and innovation

Lead authors: Tousif Rahman, Elena Chochanova (TNO)

Co-authors: Pieter Pauwels (TU/e)

| | |
|---|---|
| Work package | WP4 |
| Result | 7 |
| Lead beneficiary | TNO |
| Due Date | 30 April 2023 |
| Deliverable Status | Final |
| File name | B4B WP4 D4.5_Privacy, security and ethics framework |
| Reviewers | Johan de Wit (Siemens), Berno Veldhuis (RVB) |

# SAMENVATTING

Brains for Buildings' Energy Systems (B4B) is een 4-jarig samenwerkingsproject met meerdere belanghebbenden van 44 partners dat gericht is op het ontwikkelen van methoden om big data van slimme meters, Internet of Things (IoT)-apparaten en gebouwbeheersystemen te benutten in slimme gebouwen. Dit met het doel om om de activiteiten in gebouwen energie-efficiënter te maken en de CO2-uitstoot te verminderen, om flexibel energieverbruik mogelijk te maken, om comfort van de gebruikers te verhogen en om installatietechnisch onderhoud slimmer en kost-efficiënter te maken. Dit wordt bereikt door snellere en efficiëntere modellen en algoritmen voor Machine Learning (ML) en Artificial Intelligence (AI) te ontwikkelen. Het project is afgestemd op bestaande utiliteitsbouw.

Er zijn vijf werkpakketten in dit project gewijd aan de bovenstaande taken. Dit rapport is een uitkomst van het Werkpakket 4 (WP4) van het B4B-project. WP4 werkt onder het thema "Data-integratie". Er zijn veel heterogene gegevensbronnen in gebouwen, b.v. sensorgegevens, 3D-modelgegevens, tijdschema's, gebruikersgegevens, onderhoudsgegevens van bedrijfsmiddelen, elektrische systeemgegevens, enz. Gegevensbronnen of systemen communiceren via verschillende protocollen en wisselen gegevens uit in verschillende formaten, naamgevingsconventies en standaarden, waardoor het moeilijk wordt om deze gegevens te gebruiken voor het ontwikkelen van modellen en algoritmen. Daarom zijn deze gegevensbronnen vaak geïsoleerd en niet beschikbaar via één enkel platform, wat betekent dat er weinig tot geen interactie tussen is. WP4 heeft tot doel methoden te ontwikkelen om deze gegevenssilo's te integreren voor het ontwikkelen van modellen en algoritmen voor machinaal leren en kunstmatige intelligentie, terwijl ook privacy, veiligheid en ethiek worden gegarandeerd bij het verzamelen, opslaan, integreren, delen, beheren of gebruiken van gegevens in slimme gebouwen.

In deze deliverable kijken we met name naar deze socio-technische aspecten als middel om innovatie op te schalen door op een verantwoorde manier om te gaan met data uit slimme gebouwen. Het doel is om een alomvattend raamwerk voor te stellen dat data privacy, beveiliging en ethiek omvat en dient als middel voor vastgoedeigenaren, leveranciers en onderhoudspartijen van gebouwinstallaties, aangemelde instanties, en andere belanghebbenden om robuuste digitale strategieën op te zetten die bestendig zijn tegen de toenemende cyber-fysieke bedreigingen op hun digitale en fysieke systemen.

# SUMMARY

Brains for Buildings Energy Systems (B4B) is a 4-year collaborative, multi-stakeholder project between 44 partners that aims to developing methods to harness big data from smart meters, Internet of Things (IoT) devices and Building Management Systems (BMS) in smart buildings to reduce energy consumption and $CO_2$ emissions, increase comfort, respond flexibly to user behaviors and local energy supply and demand, reduce maintenance costs of building utilities. This can be achieved by developing faster and more efficient Machine Learning and Artificial Intelligence models and algorithms. The project is geared towards existing utility buildings, such as commercial and institutional buildings.

There are five work packages in this project dedicated to above tasks. This report is an outcome from the Work Package 4 (WP4) of the B4B project. WP4 works under "Data integration" theme. There are many heterogeneous data sources in buildings, e.g. sensor data, 3D model data, time schedules, occupant data, asset maintenance data, electrical system data, etc. Data sources or systems communicate using different protocols and exchange data in different formats, naming conventions and standards, making it difficult to use this data for developing models and algorithms. Therefore, these data sources are often siloed and not available via a single platform, meaning there is little to no interaction between them. WP4 aims to develop methods to integrate these data silos for developing Machine Learning and Artificial Intelligence models and algorithms while also guaranteeing privacy, security and ethics when collecting, storing, integrating, sharing, managing or utilizing data in smart buildings.

In this deliverable we look in particular at these socio-technical aspects as a means to scale up innovation by handling data from smart buildings in a responsible manner. The goal is to propose a comprehensive framework that incorporates data privacy, security and ethics and serves as a means for building owners, building services suppliers and maintenance providers, notified bodies, and other stakeholders to set up robust digital strategies that can withstand the increasing cyber-physical threats on their digital as well as their physical systems.

# TABLE OF CONTENTS

# 1 INTRODUCTION

## 1.1 Why are data security, privacy and ethics important

Buildings are becoming ever smarter, utilizing technology, such as smart meters, Internet of Things (IoT) devices and Building Management Systems (BMS) to optimize building efficiency, sustainability, and convenience. However, due to the interconnected networks, which are quintessential for these technologies, new threats and vulnerabilities emerge concerning the privacy, security, and ethics of the data that is collected. These data vulnerabilities can be easily overlooked in today's ever more connected world. While possible associated risks are more readily addressed within buildings that host critical infrastructure, high-tech industry or government, the average real estate owner can face similar issues and not be aware of them until it is too late. This could result in data loss or damage with financial consequences in the best case and in the worst: negative consequences on the reputation of the organisation and even on human life and well-being (directly or indirectly). It is therefore crucial to understand those risks and what can businesses do to protect individuals' privacy and rights, keep the collected data secure, while handling it in ethical and responsible ways. In the following chapters, we will look at what defines data ethics, privacy and security in smart buildings, what principles and standards are there, and how can we effectively apply these standards through a newly proposed framework. Inspired by earlier work by Siemens Building Technologies on security system design in critical infrastructure[1], the focus is placed greatly on the cyber-physical security aspect in smart buildings that results from the new connection between information and operational technologies (read more in chapter 2).

Firstly, appropriate definitions for ethics, privacy and security are presented (Fig. 1). The central questions pertaining to these concepts, which we will attempt to answer through the proposed framework, can be summarised as follows:


- What kinds of principles should guide the actions of individual users and of companies when using data and how do their actions affect society?
- What are the threats to personal privacy and how do we protect against them?
- How can access to sensitive information be controlled and how can we secure hardware and software?

*Figure 1: Ethics, Privacy, and Security*

### Data Ethics

Ethics refers to the moral principles that guide behaviour and decision-making. Ethical principles include concepts such as fairness, transparency and respect for privacy. Data ethics in particular involves applying ethical principles in the process of collection, analysis, and use of data.

In smart buildings, ethics play a critical role, since the data collected can be used to monitor and control the behaviour of individuals. For example, data collected from cameras can be used to monitor the movements of individuals, and data collected from sensors can be used to analyse their behaviour patterns. Even when data is anonymized and cannot be traced back to individuals, it could be subject to possible unethical handling. It is therefore imperative to apply ethical principles when handling data in smart buildings to ensure that it is used responsibly and that the privacy and rights of individuals are respected.

[1] De Wit, J. (2023). Convergence of Physical and IT Security in Critical Infrastructure, Great! But what about OT?. *Cyber-Physical Security and Critical Infrastructure*, (37-39). International Security League. https://www.security-ligue.org/fileadmin/user_upload/ISL-CoESS_Brochure_WP_v7_LRweb_.pdf

### Data Privacy

Data privacy is the fundamental right of individuals to control how their personal information is collected, used, and shared. In smart buildings, personal data can be collected through various sources, such as smart sensors and IoT, cameras, and access control systems. This data can include sensitive information, such as biometric data, health data, and financial data. In order to protect individuals' fundamental right to privacy, it is crucial to comply with data privacy standards and guidelines, such as the General Data Protection Regulation (GDPR), to protect that right and to ensure that their personal data is collected and processed lawfully. The GDPR is a regulation within European Law that came into force on May 25th, 2018. It states that the protection of natural persons in relation to the processing of personal data is a fundamental right. Personal data can include the name, contact data, location, age, sex, religion or anything that can describe a natural person's physical, physiological, mental, economic, cultural, or social identity.

### Data security

Data security is the practice of protecting digital information from unauthorised access, corruption, use, disclosure, modification, or destruction throughout its entire lifecycle. Among other things, this can be the result of targeted attacks, which can aim to either obtain, alter or damage (sensitive) data, extract money from users (for example by applying ransomware) or otherwise hinder regular business or industrial processes or even, directly or indirectly, place human life and wellbeing in danger. In smart buildings, data security is concerned as much with the cyber security of the connected applications and software as it is with the physical security of the building and all its contained systems and hardware, since the data collected can be used to control physical building systems, such as lighting, heating, and ventilation. It therefore encompasses every aspect of data security, including but not limited to physical security of hardware and storage devices, administrative and access controls, logical security of software applications and even organizational policies and procedures. For that reason, it is critical for stakeholder organisations to address data security in smart buildings, by raising awareness about the possible threats, complying with relevant data security standards and/or guidelines[2] to protect the data and in the best case scenario, having a well-formulated and implemented data security and risk mitigation strategy.

## 1.2 Terms and definitions

**OT (operational technology)** – is a term used to describe 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 and it is found in almost all industries, such as manufacturing, automotive, science, government, education, healthcare, retail, critical infrastructure and utilities.

**ICS (Industrial Control Systems)** - a class of Information and Communication Technology (ICT) which measure, monitor and control physical processes. ICS is an overarching term describing all of the devices controls and associated instruments, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes (such as those taking place in data centres, manufacturing plants and factories). Synonyms for ICS include SCADA, DCS, and IACS that are part of the Operational Technology (OT) or Process Automation (PA) domain.

**SCADA (Supervisory Control and Data Acquisition)** – is one type of OT. It's a control system architecture in an OT. The system collects data from various sensors within an OT network (such as a factory, plant or another remote location). Then it sends the data to a central computer that manages the data.

**IT (information technology)** - The entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services.

**IoT (Internet of Things)** - the process of connecting everyday physical objects to the internet. Those can be common household objects such as lightbulbs and thermostats but they can also be healthcare assets like medical devices. Wearables, smart devices and even smart cities are also considered IoT.

[2] See overview of relevant standards and guidelines in Chapter 2.4.

**IIoT (Industrial Internet of Things)** - a subset of IoT, refers to connected devices that are used in manufacturing, energy and other industrial settings. IIoT helps manufacturers solve problems faster by transforming operations, assisting end users in making business decisions, and making plants more productive.

**BMS (Building Management System)** - a combination of software, hardware and communications infrastructure designed to support the building operation, including the HVAC systems and subsystems such as fans, pumps and chillers. This is also referred to as a Building Automation System (BAS).

**Ransomware** - a form of malware that locks the user out of their files or their device. The attackers then demand a ransom, unusually in the form of a payment to restore access.

## 1.3 Literature

In smart buildings, data ethics, privacy and security are concerned as much with the digital systems as with the physical systems that are being governed by them. This interaction is characteristic of operational technology (OT), which lies in the centre of building systems. However, with modern trends towards digitization the amount of data available about modern cyber-physical systems, such as smart buildings' OT, has dramatically increased. This enables new types of data-driven processes in buildings, automating and replacing many of the traditionally manual tasks, such as fault detection and diagnosis (FDD), optimised control strategies (e.g. Model-Predictive Control – MPC) and sequences of operations, performance measurement, benchmarking, and energy auditing. These new automated tasks enable buildings to be more efficient and resilient in their operation and more comfortable and reactive to their occupants.[3] Thus, while increased interconnectivity in smart buildings brings about many benefits, it is always accompanied by a corresponding amount of risk.

Mitigating these risks in smart buildings requires more than the traditional IT cybersecurity measures as we shall see in Chapter **Error! Reference source not found.**. One needs a model or a framework that can encompass the entire cyber-psychical system architecture and guide the user to take appropriate preventive and response actions to data risks and threats. Internationally there are a few noteworthy models and tools developed specifically in the field of Industrial Control Systems (ICS) that illustrate that approach. Below three such models have been explained in more detail: the "Purdue Model", the "Think Secure" concept and the Dutch Digital Trust Center's "online security check for process automation".

### Purdue Model

The Purdue Model, also known as the Purdue Enterprise Reference Architecture (PERA) or "Purdue Model" in short, is a conceptual framework for designing and organizing ICS and smart building systems. The model was developed by researchers at Purdue University in the 1990s and has since become a widely used standard in the field of ICS and smart buildings. Its structure is shown in Figure 2 [4].

The Purdue Model organizes systems into hierarchical levels based on their functions, operations, and physical location. The model consists of six levels, each with a specific purpose, and isolated from the other layers for security purposes. The levels from top to bottom are:

[3] International Energy Agency. (2022). *IEA EBC - Annex 81 - Data-Driven Smart Buildings.* International Energy Agency's Energy in Buildings and Communities Programme. https://annex81.iea-ebc.org/publications

[4] Sectrio. (2022). *Threat Modeling Using the Purdue Model for ICS Security.* Sectrio. https://sectrio.com/threat-modeling-using-purdue-model-for-ics-security/

- Level 5: Enterprise
- Level 4: Manufacturing Operations Management
- Level 3: Operation / Production Control
- Level 2: Supervisory Control
- Level 1: Basic Control
- Level 0: Process Control

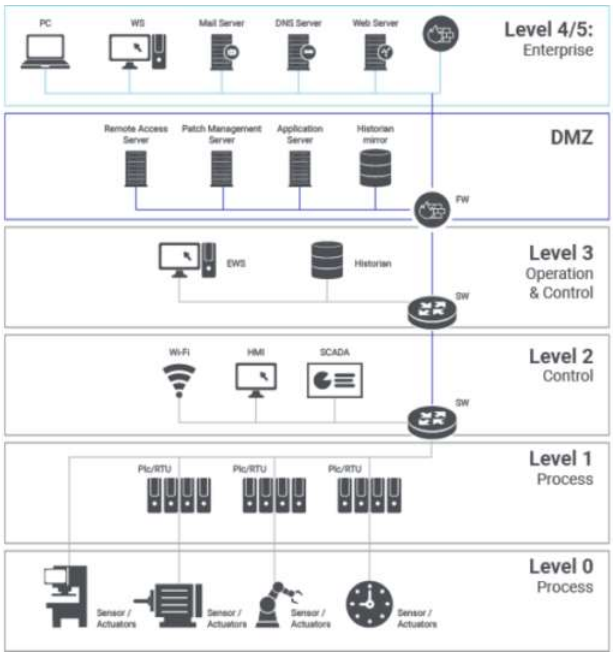


*Figure 2: The Purdue model.*

Each level has a specific function and set of responsibilities: the enterprise level deals with business-level activities such as planning, logistics, and accounting, while the process control level is responsible for controlling the physical processes. The model helps ensure that each level is isolated from the others, preventing unauthorized access and potential cyber-attacks.

The Purdue Model is used in ICS and smart building systems for a variety of purposes. For example, it provides a standard framework for designing, organizing, deploying, and managing the different technologies that comprise these systems, ensuring that they are secure, reliable, and efficient. The model helps ensuring that these systems and technologies are integrated and work together seamlessly, improving energy efficiency, occupant comfort, and building safety.

While the Purdue model provides a valuable hierarchical structure that can be used as the basic structure for system architectures in smart buildings, it misses the risk identification element[5]. Because the model was originally designed to integrate otherwise separate systems, it is currently considered insufficient as a blueprint for system architectures. With the rise of IoT, the traditional airgap between the top 2 (mostly IT) and bottom 3 (mostly OT) layers has been bridged (read more on that in chapter 2.2). However, the Purdue model remains relevant thanks to its ability to help in the integration of disparate systems and technologies, making it easier to manage complex systems, and ensuring the security and efficiency of these systems. In addition, following the principles of this model can help organizations comply with other standards such as the IEC 62443.

### Think Secure

The culture of ICS security, also known as the "Think Secure" concept, is used to promote a security mindset among operators, engineers, and other personnel involved in the operation and maintenance of ICS. The goal is to raise awareness of potential security risks and encourage people to take steps to protect ICS against cyber threats. To apply the "Think Secure" concept, organizations should provide training and education to their staff about the importance of cybersecurity and the best practices to mitigate security risks. This may include:

- Identifying potential security threats and vulnerabilities in the ICS environment, such as outdated software or weak passwords,
- Developing and implementing policies and procedures to address those risks,
- Regularly testing and assessing the effectiveness of security measures, such as penetration testing and vulnerability assessments,

[5] Peterson, Dale. (2019). *Is the Purdue Model Dead? - Dale Peterson: ICS Security Catalyst*. Dale Peterson. https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/

- Encouraging a culture of security awareness, where employees are vigilant about potential threats and report any suspicious activity,
- Continuously monitoring and improving security measures, including staying up to date with the latest security threats and trends.

In brief, "Think Secure" is a security mindset that encourages ICS personnel to be proactive in identifying and addressing security risks throughout the lifecycle of an ICS, from requirements specifications, through procurement, engineering and operations to end-of-life (EoL). By following best practices and staying vigilant, organizations can thus better protect their ICS against cyber threats.[6]

### National security check tools - Digital Trust Center [7]

In order to help protect organisations' OT from cyber incidents, the Dutch ministry of economic affairs and the climate has launched an online security check for process automation ("*Security Check Procesautomatisering*"). This check can be done by companies to help them gauge the level of security they would require in order to protect their industrial control systems (ICS) in their OT environment.

The scan is comprised of 14 sections of questions that evaluate different security aspects such as risk analysis, training, network architecture, software updates and incidence response to name a few.


*Figure 3: The Dutch security check for process automation distinguishes 14 different security aspects in its online evaluation.7 above*

[6] Luiijf, Eric & Te Paske, Bert. (2015). *Cyber Security of Industrial Control Systems.* TNO. http://dx.doi.org/10.13140/RG.2.1.3797.4566

[7] Security Check Procesautomatisering (https://tools.digitaltrustcenter.nl/security-check-procesautomatisering/)

# 2 DATA SECURITY ASPECTS

Wherever there is data flowing between connected devices, there will be vulnerabilities that might be subject to data breaches, data loss or in any other way data or business damage. As we have already seen in chapter 1.1, data security is the act of protecting the data from these undesirable results. 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 strategies should therefore be concerned with more than just the technical solutions but also with organizational and process-related risk mitigation strategies. It is a known fact that the human factor in any system remains the weakest link, in fact in over 95% of all security information incidents can be traced back to human error.[8] Therefore, any proposed framework needs to address the organisational aspects of data security. In smart buildings that could be challenging considering the wide range of stakeholders involved with the systems.

In this chapter we will look at the key elements of data security, we'll examine the differences between IT and OT and why cyber security measures as applied in IT cannot be used directly for OT and how that puts modern OT systems at risk. Further on we will look at some existing and relevant standards for OT data security and lastly we will look at some examples of data breaches and cyber-attacks on ICS and the lessons learnt from them.

## 2.1 Key elements

The Confidentiality, Integrity, and Availability (CIA) triad is a widely recognized guiding model for information security. The three elements form the basis of the security of data and systems, and they are often used as a benchmark for evaluating the effectiveness of security measures and strategies, such as policies and security controls [9]. The three elements of the CIA triad are:

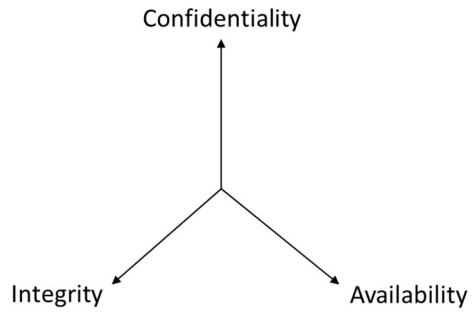


*Figure 4: The Confidentiality, Integrity, and Availability (CIA) triad.*

### Confidentiality

Confidentiality refers to protecting sensitive information from unauthorized access. Confidentiality is achieved by implementing access controls and encryption to prevent unauthorized disclosure of information. In short, it ensures that data is accessed only by authorized users with the proper credentials. It should not be confused with privacy.

### Integrity

This principle refers to the accuracy and completeness of information. Maintaining data integrity means ensuring that information stored is reliable, accurate, and is not tampered with or altered in any unauthorized or

[8] Koza, E. (2022). *Information Security Awareness and Training as a Holistic Key Factor – How Can a Human Firewall Take on a Complementary Role in Information Security*?. In: Tareq Ahram and Waldemar Karwowski (eds) Human Factors in Cybersecurity. AHFE (2022) International Conference. AHFE Open Access, vol 53. AHFE International, USA. http://doi.org/10.54941/ahfe1002201

[9] Office of Information Security (2023). *Confidentiality, Integrity, and Availability: The CIA Triad*. Washington University in St. Louis. https://informationsecurity.wustl.edu/items/confidentiality-integrity-and-availability-the-cia-triad

unwarranted manner. Data integrity can be maintained through measures such as data backups, checksums, and digital signatures.

### Availability

The availability principle ensures that information and systems are available and (safely) accessible to authorized users when they need them. Availability can be maintained through measures such as redundancy, fault tolerance, and disaster recovery planning.

The CIA triad provides a comprehensive framework for evaluating and implementing security controls in information systems. By focusing on these three core principles, organizations can ensure that their information is protected from a wide range of threats, including cyberattacks, data breaches, and even natural disasters. The CIA triad applies to all types of information systems, including computer networks, databases, and other electronic systems in the IT domain. However, it is also applicable to physical security systems, such as access control systems and surveillance cameras in the OT domain.[10]

## 2.2 Difference between IT and OT data security

The domains of OT and IT are essentially very different; IT systems are primarily used to solve business problems by communicating with each other through data exchange, while OT systems are primarily used to interact with the physical world. Some subsets of OT include SCADA, ICS and even field sensors and actuators and in the world of buildings, industry and infrastructure, OT is used to control various systems, such as building management, transportation, physical access control, physical environment monitoring, and physical environment measurement systems.

In terms of networks, IT networks can be comprised of elements from the entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services. While OT networks can also be comprised of hardware and software, they are mainly used to detect and control physical devices, processes, and events. In summary, OT networks communicate with the physical world and IT networks deal with digital information.[11]

The original purposes and functions of IT and OT are essentially different and therefore in the realm of data security we find that both domains prioritize different elements from the CIA triad (see Figure 5). For example, OT systems are typically used to control critical physical processes, so key priorities are the 24/7 continuity and the continuous ability for operations to view and control the processes. That places a high priority on the availability of the data and results in a low tolerance to disruption caused by changes in the system, such as antivirus updates and patches that are otherwise necessary for keeping the system secure.


*Figure 5: IT (left) prioritizes different elements of the CIA triad than OT (right)*

[10] Krzyzanowski, P. (2022). Introduction to Computer Security. https://people.cs.rutgers.edu/~pxk/419/notes/intro.html

[11] De Wit, J. (2023, April 6). *Securing Operational Technology (OT): New Kid on the Block or Familiar Risk? A wake-up call for one of the biggest threats for the future.* B4B Webinar. https://brains4buildings.org/2023/04/06/12-securing-operational-technology-ot-new-kid-on-the-block-or-familiar-risk-a-wake-up-call-for-one-of-the-biggest-threats-for-the-future/

Characteristic for IT networks is that the embedded devices are designed with a certain level of resilience through built-in redundancies and reserving large parts of the system for error handling. The devices within these networks are also often homogeneous, utilizing only standard protocols (such as TCP/IP) to communicate. Unlike IT networks, OT networks are usually not as resilient, since they do not have enough resources to run any error handling. In addition, OT network components tend to be widely diverse and not transferrable between systems with communication mostly being based on proprietary protocols. That makes them, in general, less flexible. In addition, OT systems have a longer lifespan than IT systems and therefore most OT environments and their data security have to cope with legacy systems and components. These and other main differences between IT and OT are summarized in Table 1 below.

| | IT | OT |
|---|---|---|
| Security priority | confidentiality, integrity, availability | availability, safety, integrity, visibility, operability and process efficiency |
| Availability | Down time/restart when needed | 24/7, with none or limited down time allowed |
| Resilience | Large resources for error handling | Little to no resources for error handling |
| Technical & economic lifespan | Short (3-5 years) | Long (10-25 years) |
| Standardisation | Homogeneous, utilizes standard protocols to communicate | Diverse, based on proprietary protocols |
| Latency | Various response times | Real-time requirements (usually critical) |
| Software robustness | Implementations under continuous hacker scrutiny | Designed for benign environments, vulnerable when connected to the outside world |
| Anti-malware | Standard | Infrequent or not possible |
| Patching and updates | Uses strict policies, regular and easy deployment | No representative testing environment for patches and updates, difficult deployment due to availability requirements |
| Passwords | Regularly changed | Often unchanged or hardwired into the system |
| Default accounts | Removed / changed | Often unchanged |
| Physical security | High (for critical IT such as server and network) | Occasional |
| Security testing/audits | Planned regular testing | Infrequent testing |
| Security awareness | High | Low / rising |
| Security standards | Existing and implemented | In development |

*Table 1: Main differences between IT and OT based on some key characteristics* [6]

## 2.3 Increasing connectivity and security risks in smart buildings

As we have seen, OT has multiple inherent characteristics that differ greatly from IT and therefore data security strategies within IT networks cannot be simply projected onto OT networks and expect the same effect. Interestingly, these OT characteristics have never posed data security threats in the past. This is because OT data security has historically relied on the "air gap" between the physical systems within the building or facility and the outside (digital) world. In short, the IT- and OT-networks were traditionally intentionally separated from each other, as they did not need to mutually share information (Figure 6). This is not at all surprising considering that IT and OT have been historically different domains, managed by different departments.

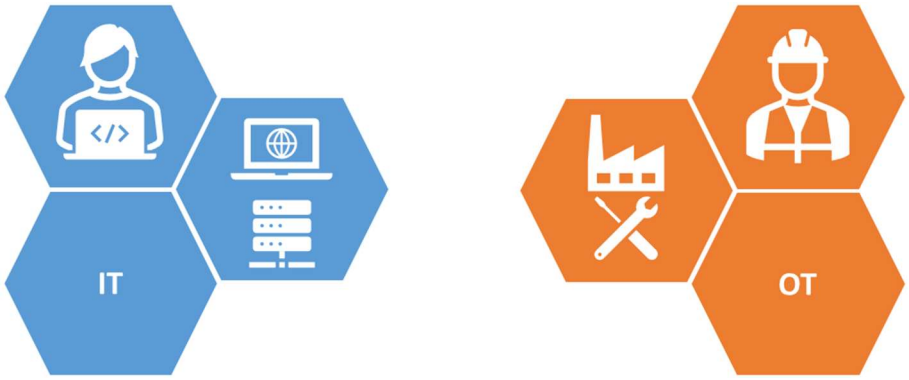


*Figure 6: The world of IT and that of OT have historically been completely separated*

However, with the expanding application of smart and connected technologies, IT and OT are becoming increasingly interconnected. OT that were originally designed for closed proprietary and benign environments have, over time become open, networked and sometimes even publicly connected. The reason for that is that data coming from the OT systems is distributed to different stakeholders digitally through IT networks. In this way the traditional “air gap” between the two networks is bridged (Figure 7). This convergence is often referred to as the emergence of “cyber-physical systems” (CPS).

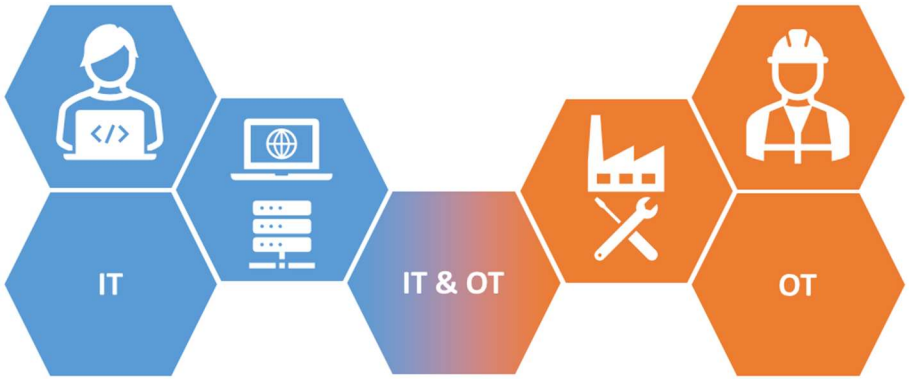


*Figure 7: The world of IT and that of OT is becoming increasingly interconnected*

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

- is no longer isolated from IT,
- runs on common internet protocols (and no longer on proprietary protocols),
- runs in general purpose software,
- makes use of open-source environments,
- operates on top of commercial off-the-shelf (COTS) hardware and mainstream IT operating systems,
- is increasingly connected to public information networks through wireless technologies and IoT (and less on wired local connections).

For smart buildings, this has manifested in the application of various systems and smart devices that enable faster and ever more convenient collecting and sharing of building data, such as IoT devices, remote access management systems, third part data storage, and more. These systems and devices play an important role in making processes more efficient, through enabling centralized operations with less human operators, allowing for 24/7 remote support and maintenance, increased flexibility and process adaptability, integration with corporate IT, and other cost reductions due to the use of COTS computers and software. It is therefore a no-brainer that in recent years organizations have been eagerly adopting these technology shifts in order to reap the business benefits.

All of these smart developments bring about new risks with them. This gaining interconnectivity has resulted in an increased vulnerability of the environments, therefore exposing them to security risks, such as:

- Malicious actors seeking to gain access to confidential data for financial or other gains,
- Accidental data loss or destruction,
- Breach of a contract or unauthorized access by employees,
- Unauthorized access by third-party vendors,
- Phishing and other social engineering attacks,
- Possible threat to human wellbeing and even lives.

These risks are usually caused by inherent vulnerabilities in OT networks that have only become apparent through the interconnectedness with IT in recent years (see Table 1 for more detail). The various vulnerabilities can be grouped into several main categories:

### Network & access controls vulnerabilities

Smart buildings have complex network systems that can be vulnerable to hacking or cyber-attacks. In addition, if access controls are not properly implemented, unauthorized individuals may be able to access sensitive information or control systems within a smart building. Hackers can also use social engineering tactics, such as phishing or impersonation, to trick employees or building occupants into revealing sensitive information.

### Hardware vulnerabilities

Smart devices and IoT devices in a smart building can be a target for hackers, and if they are not properly secured, they can provide an entry point into the building's network.

### Software vulnerabilities

Outdated software can contain known vulnerabilities, such as unpatched or outdated software, that hackers can exploit to gain access to a building's network.

### Physical security vulnerabilities

Smart buildings often have a large number of physical access points, such as doors and windows, that can be targeted by hackers to gain entry into the building's network.

The reasons behind these risks and vulnerabilities vary. In part, these risks and vulnerabilities exist simply because of the history of OT as we have already discussed in previous paragraphs. One example is that traditional building protocols lack adequate cybersecurity features; one of the most widely used data layer protocols for HVAC control, BACnet, is deployed in an unencrypted format. Another example is the lack of awareness among building owners, facility managers, suppliers and maintenance service providers, notified bodies and other stakeholders, and therefore a lack of market demand for security features. This results in manufacturers and vendors of OT systems and equipment placing the focus on new features rather than more secure systems to meet the demand of their customers.

In conclusion, both OT systems and the physical processes they control have thus become more susceptible to malware, hacking and deliberate network disruptions where OT-controlled critical infrastructure may be disrupted or physically damaged, which can have a serious impact on their business continuity and in the worst case on human life and wellbeing.

In order to exchange knowledge between the departments, a common recommendation for organizations is to bring these departments to work together, since OT has limited data security knowledge and IT has cyber-security knowledge but needs to understand the peculiarities of OT.

## 2.4 Examples of cyber security incidents and mitigation strategies

In recent years, hackers and other threat actors, working either independently, for governments, within terrorist or other malevolent organisations, have been gaining traction and threatening to cause reputational, monetary or even physical damage not only to individuals and companies but also public services. The cost and the frequency of cyber-attacks are rising globally. In a 2022 report, IBM stated that the cost of data breaches in the various sectors are steadily on the rise, reaching an all-time high in 2022 (which averaged USD 4.35 million, a 12.7% increase from 2020).[12] Yet, already in 2019, reports indicate that nearly 40 percent of 40,000 smart buildings were impacted by a cyber-attack.[13] Findings suggest that the attacks have been caused by vulnerabilities in the systems, such as the fact that 70% of IoT devices were still using the factory-set default passwords, most IoT devices were often too critical to stop operations for software updates and BAS systems are not sufficiently protected. It is therefore evident that, as the OT systems of smart buildings and basic public services such as water or electricity plants become more advanced and interconnected, they become more susceptible to cyber-attacks. When cyber-attacks target physical systems through taking control of ICS, it is referred to as a *cyber-physical attack*. In the following paragraphs we look at some examples of cyber-physical attacks on ICS and OT systems and their resulting mitigation strategies in order to prevent future attacks.

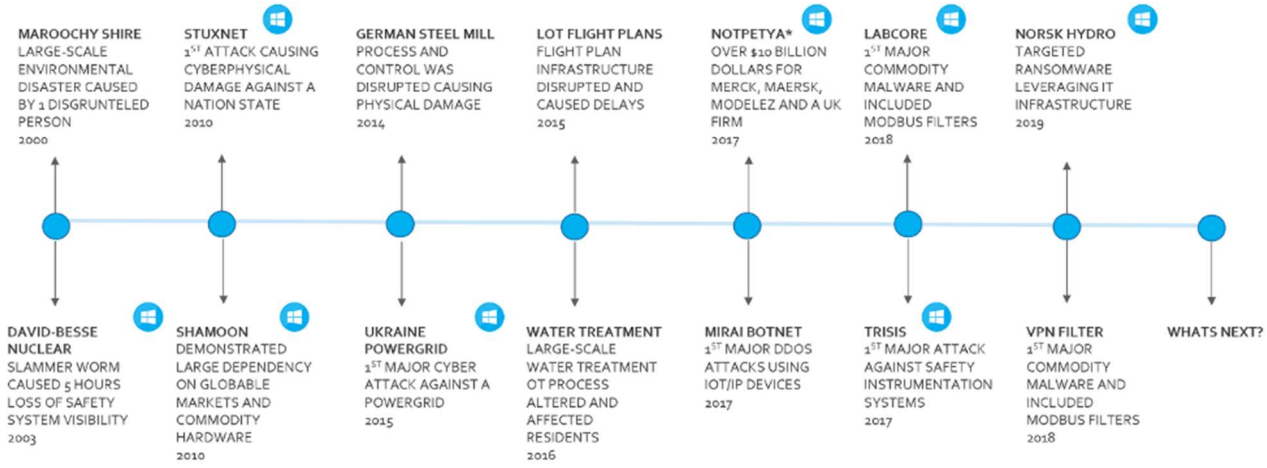


*Figure 8: A timeline of famous cyber-physical attacks on OT systems in public services, industry and infrastructure [14]*

### Maroochy Water Services case [15]

The cyber-attack on Maroochy Water Services took place in 2000 in Queensland, Australia. It involved a disgruntled former employee named Vitek Boden, a computer programmer, who used his insider knowledge and access to the company's systems to cause havoc, resulting in significant damage and disruption. He planted

[12] IBM Security (2022). *Cost of a Data Breach Report 2022*. [online] IBM.com, USA: IBM Corporation, p.59. https://www.ibm.com/downloads/cas/3R8N1DZJ [Accessed 26 Feb. 2023].

[13] Kaspersky (2019). *Nearly Four in Ten Smart Buildings Targeted by Malicious Attacks in H1 2019.* https://usa.kaspersky.com/about/press-releases/2019_smart-buildings-threat-landscape [Accessed 26 Feb. 2023].

[14] Verve (2020). *How 20 years of cyber security incidents inform future strategy.* https://verveindustrial.com/resources/blog/how-20-years-of-cyber-security-incidents-inform-future-strategy/ [Accessed 6 Apr. 2023].

[15] Slay, Jill & Miller, Michael. (2007). *Lessons Learned from the Maroochy Water Breach*. International Federation for Information Processing Digital Library; Critical Infrastructure Protection;. 253. 73-82. http://dx.doi.org/10.1007/978-0-387-75462-8_6 [Accessed 1 Feb. 2023].

malicious software, also known as a "logic bomb" into the company's computer network before he left the organization. The logic bomb was designed to trigger on a specific date, months after Boden's departure from the company, and resulted in widespread disruption to Maroochy Water Services' computer systems. The attack caused sewage overflows, pump failures, and other operational failures, leading to environmental damage, extensive clean-up efforts, and financial losses for the company.

The Maroochy Water Services cyber-attack serves as a stark reminder of the potential dangers of insider threats and the need for robust cybersecurity measures to protect critical infrastructure and related cyber-physical systems from cyber-threats as they have real-life impacts. It also highlighted the importance of proper access controls, monitoring, and response protocols to prevent and mitigate cyber-attacks.

### Stuxnet worm [16]

The Stuxnet is known as the world's first sophisticated cyber-weapon that was designed to target the centrifuges used in Iran's uranium enrichment program causing them to malfunction. Stuxnet was a computer worm that was discovered in 2010 and is believed to have been developed by the United States and Israel to sabotage Iran's nuclear program. The malware, which operated autonomously and in silence, infected the ICS that controlled the centrifuges, used fake input for the execution code and caused them to spin at inconsistent and damaging speeds, ultimately causing them to fail. Stuxnet was also designed to remain hidden and undetected for as long as possible, using sophisticated techniques to evade detection by antivirus software. The worm was spread through infected USB drives. Once the USB drive was inserted into a computer connected to the plant's network, Stuxnet would begin to spread through the network and seek out vulnerable systems to infect.

Overall, Stuxnet was a highly targeted and carefully crafted attack that exploited multiple vulnerabilities in the ICS software used by the enrichment plant. The discovery of Stuxnet was a major turning point in the use of cyber-weapons for political and military purposes. It demonstrated the potential for computer viruses and other malicious software to cause real-world damage to critical infrastructure, thereby emphasizing the need for improved cybersecurity measures in those systems. For that reason it is one of the most famous cases of a cyber-physical attack on OT systems.

### Ukrainian power grid attack [17]

In December 23, 2015, the Ukrainian electricity distribution system experienced a significant cyber-attack, which resulted in a widespread power outage leaving 225,000 Ukrainians to sit out Christmas in the dark. The attack involved sophisticated malware to target and compromise the IT and OT systems of three energy distribution companies in Ukraine. The attackers used a phishing attack to gain access to the networks, exploiting vulnerabilities in the companies' systems. Once inside, the attackers moved laterally, gaining control over critical systems, including the grid's SCADA systems, before launching a coordinated and highly destructive attack, using the malware to disable critical infrastructure components, including switches and circuit breakers, which caused widespread power outages.

The Ukrainian power grid cyber-attack is widely believed to be the first known instance of a cyber-attack causing a widespread power outage. It served as a wake-up call for the importance of securing critical infrastructure against cyber threats and highlighted the need for robust cybersecurity measures, including network segmentation, intrusion detection systems, regular patching, and employee training to prevent and mitigate such attacks in the future. The attack was attributed to a state-sponsored hacking group with alleged ties to Russia, although no official confirmation exists.

[16] CSO (2022). *Stuxnet explained: The first known cyberweapon.* https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html [Accessed 1 Feb. 2023].

[17] International Society of Automation (2017). *Ukrainian power grids cyberattack.* https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack [Accessed 30 Mar. 2023]

### Ransomware in an Austrian hotel [18]

During the 2017 cyber-attack on the 4-star luxury hotel Romantik Seehotel Jaegerwirt in Austria, hackers used a form of ransomware called Locky to encrypt the hotel's computer systems and demanded a ransom in Bitcoin for the release of the data. The attack resulted in the hotel's entire IT infrastructure being locked, including reservation systems, guest registration, and key card access. This caused significant disruption to the hotel's operations, as guests were unable to check in or out, reservations were lost, and hotel staff had to resort to manual processes. Even though the hotel's management made the decision not to pay the ransom and instead worked to restore their systems from backups, the attack highlighted the hotel's lack of cybersecurity measures, including weak passwords and outdated systems, which made them vulnerable to the attack.

In response to the attack, the hotel implemented enhanced cybersecurity measures, including regular system updates, stronger passwords, and employee training on cybersecurity best practices. The hotel has even considered a technological downgrade at the next refurbishment, in the form of old fashioned physical keys, as a mitigation strategy against future attacks. The incident also served as a cautionary tale for other businesses about the importance of pro-active cybersecurity measures in low-risk environments (other than critical infrastructure) to prevent and mitigate ransomware attacks.

### Mitigation strategies (summarized):

The above examples show how the inherent vulnerabilities of OT systems make them susceptible to cyber-attacks and what mitigation strategies have been devised and put into place only after these attacks have caused significant damage.

- Establish proper access control management, monitoring, and response protocols, especially when external employees are involved or when external access to the systems is common place (for example manage and update passwords regularly, especially when employees leave the company),
- Establish a secure environment through firewalls, geo-blocking, and a secure internet connection (such as VPN),
- Implement network segmentation and isolation of ICS networks from any untrusted networks,
- Install intrusion detection systems,
- Develop awareness, organize employee trainings and establish roles and responsibilities,
- Monitor systems regularly, perform regular software updates and patches, identify and check vulnerabilities in the system, both in terms of physical and cyber security,
- Hire ethical hackers to test the system,
- Get a security certification, such as ISO 27001 and IEC 62443,
- Choose vendors of security system components or of cloud data solutions that are certified and offer support and liability of their products,
- Oblige third parties to adhere to your organisation’s cyber security policies and protocols.

However, there are some problems remaining when trying to build and implement an automated response to hinder cyber-attacks into existing OT system architectures such as large amount of diverse vendors to choose from, lack of trained personnel, and high cost and complexity of such implementations.

## 2.5 Existing standards and frameworks

[18] CSO (2017) *Ransomware locked hotel out of its electronic key lock system*. https://www.csoonline.com/article/3162764/ransomware-locked-hotel-out-of-its-electronic-key-lock-system.html [Accessed 30 Mar. 2023]

A number of standards and guidelines exist that provide guidance regarding the securing of cyber-physical systems.

### ISO 27000 series "Information technology – Security techniques - Information security management systems"

The ISO 27000 series is a set of international standards that provide guidelines and best practices for implementing an Information Security Management System (ISMS). The ISMS helps organizations to systematically manage and protect their sensitive information, including customer and operational data, intellectual property, financial information, and employee records. The ISO 27000 series outlines a framework for establishing, implementing, maintaining, and continually improving an ISMS. It also provides a systematic approach to risk management, identifying and addressing potential security threats, and ensuring compliance with legal and regulatory requirements. The series includes a range of standards, such as ISO 27001, which specifies the requirements for an ISMS, and ISO 27002, which provides a code of practice for information security management (Figure 9).


*Figure 9: ISO 27000 includes a series of standards with focus on different sub-topics*[19]

### IEC 62443 series "Industrial communication networks - Network and system security"

The International Electrotechnical Commission (IEC) is a global organisation that prepares and publishes international standards specifically on electrical, electronic and related technologies. One of these standards that specifically addresses ICS is the IEC 62443.

The IEC 62443 series is an international standard that provides guidelines and best practices for securing industrial communication networks and systems. The standard is designed to help organizations protect their critical infrastructure, such as power plants, chemical facilities, and manufacturing plants, from cyber- and cyber-physical attacks and other security threats. The IEC 62443 series outlines a framework for implementing security measures at every stage of the network and system lifecycle, from design and development to implementation, operation, and maintenance. It also provides guidance on risk assessment and management, network segmentation, access control, incident response, and other critical security practices. The series includes

[19] Al-Karaki, J.N., et. al. (2020). *GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking.* Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2020.09.011

a range of standards (Figure 10), such as IEC 62443-2-1, which provides a general security framework for ICS, and IEC 62443-3-3, which specifies security requirements for system integration in ICS.

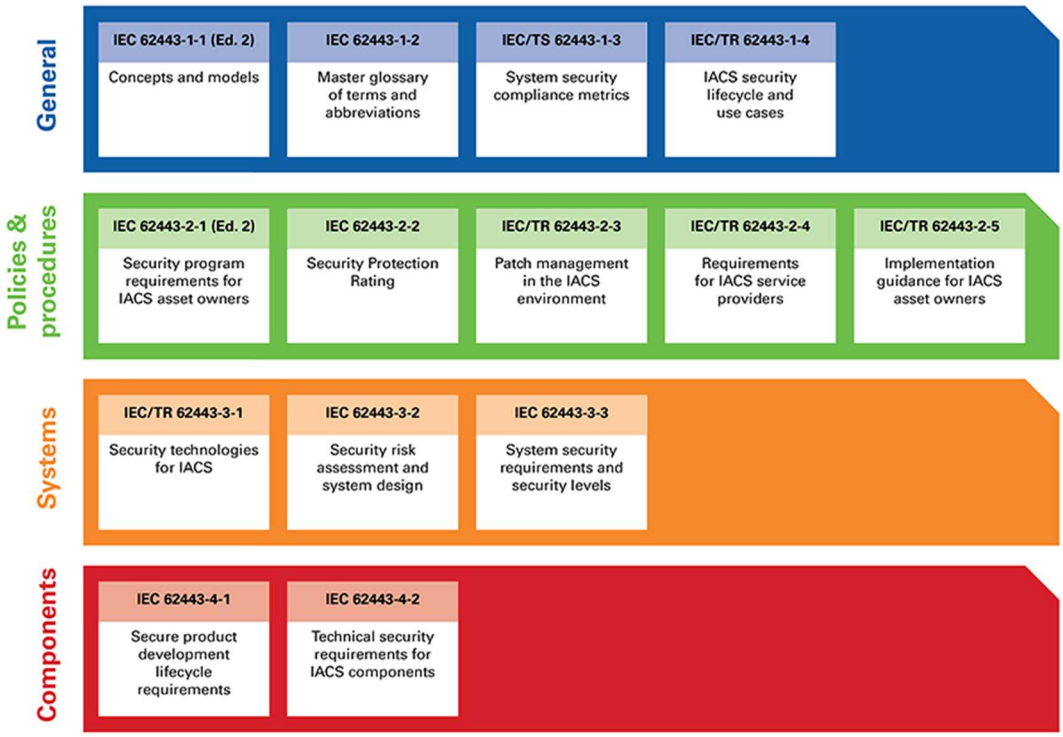


*Figure 10: overview of the IEC 62443 series20*

The IEC 62443 standard defines four security levels (SL): from SL 1 (Casual or Coincidental violations) to SL 4 (Nation State attack). The security levels ensure that systems are classified based on their inherent risks. It is therefore essential that risk assessment is performed in order to assign the appropriate corresponding security level to the OT system in question.

### NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) is a set of guidelines, best practices, and standards developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce cybersecurity risk. The framework provides a common language and a structured approach for organizations to manage their cybersecurity risks, as well as a roadmap for improving their cybersecurity posture. It consists of five core functions - Identify, Protect, Detect, Respond, and Recover - which provide a comprehensive view of an organization's cybersecurity capabilities (Figure 11).

The Identify function helps organizations to understand their assets, risks, and vulnerabilities and to develop a risk management strategy. The Protect function focuses on implementing appropriate safeguards to protect against cybersecurity threats. The Detect function aims to identify cybersecurity events promptly. The Respond function outlines the steps that organizations should take to respond to cybersecurity events when they occur. Finally, the Recover function helps organizations to recover from a cybersecurity incident and restore normal operations as quickly as possible.

[20] KIWA IEC 62443 certification: Cyber Security for Industrial Automation & Control Systems (IACS). https://www.kiwa.com/en/service2/certification/iec-62443-certification-cyber-security-for-industrial-automation-control-systems-iacs/

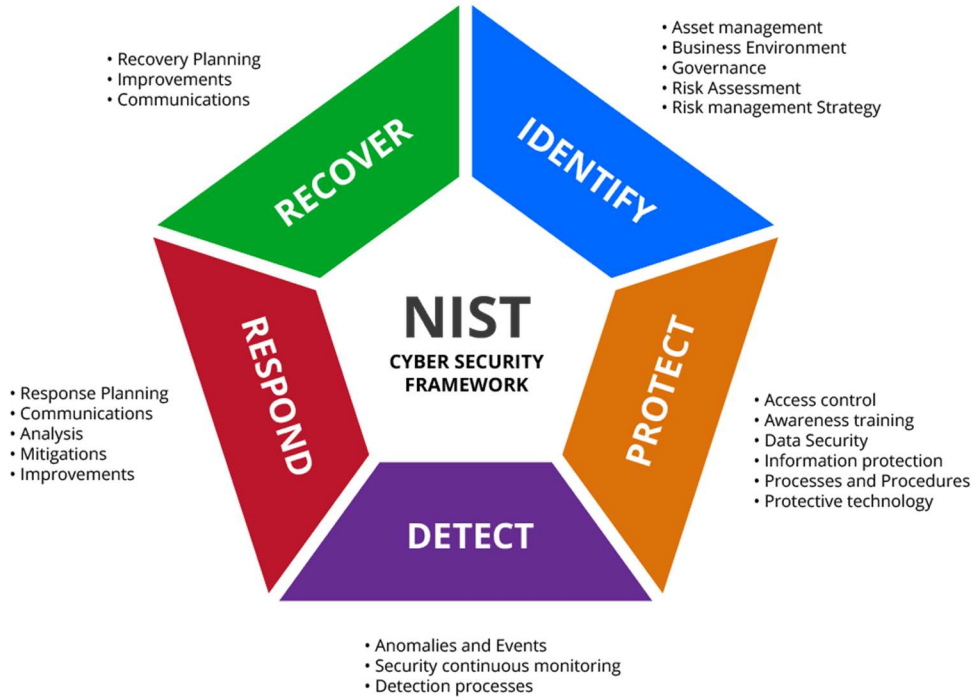


*Figure 11: the NIST cybersecurity framework*[21]

The CSF is widely used by organizations of all sizes and sectors to improve their cybersecurity resilience and has become a recognized standard for cybersecurity risk management. It is a flexible and customizable framework that allows organizations to tailor their cybersecurity programs to their specific needs, risk profile, and industry requirements.

### ISO 31000 Risk management – Guidelines

Risk is defined as "effect of uncertainty on objectives". ISO 31000 is an international standard that provides guidelines and principles for risk management. The standard provides a framework for organizations to identify, assess, treat, and monitor risks that may affect their objectives. The ISO 31000 standard is applicable to any organization, regardless of its size, sector, or location.

The ISO 31000 standard emphasizes the importance of a systematic and structured approach to risk management. It highlights the need for organizations to establish a risk management process that is integrated into their overall management system. The standard provides a set of principles, framework, and processes for managing risk effectively.

ISO 31000 is a flexible standard that can be adapted to the needs of different organizations. It promotes a risk management culture that involves all levels of the organization, encourages continuous improvement, and ensures that risks are managed consistently across the organization. The standard provides guidance on risk identification, risk analysis, risk evaluation, risk treatment, and risk communication.

Overall, the ISO 31000 standard provides a comprehensive approach to risk management that helps organizations to make informed decisions, prioritize their resources, and minimize the negative impact of risks on their objectives.

[21] CorCystems Managed IT Services. (2023). NIST Cybersecurity Protection. https://www.corcystems.com/services-solutions/cyber-security-compliance/nist

### NIS Directive[22]

The NIS Directive (Directive on Security of Network and Information Systems) is an EU-wide directive that was introduced to enhance the cybersecurity of critical infrastructure and essential services across EU member states. Its first version was enforced in 2016, and its follow-up version, the NIS2, has come into force in January 2023. Member states have until October 2024 to implement the new version of the directive into their local legislation.[23]

The NIS Directive aims to improve the resilience and security of networks and information systems in sectors that are critical for the functioning of society, such as energy, transportation, finance, health, and digital services (Figure 12). It sets out requirements for the security and incident reporting of network and information systems to prevent and mitigate cybersecurity risks. Under the NIS Directive, operators of essential services and digital service providers are required to implement appropriate security measures and report significant cybersecurity incidents to relevant national authorities. The directive also encourages cooperation and information sharing among member states to foster a coordinated response to cyber threats. The NIS Directive sets a baseline for cybersecurity requirements, and member states have flexibility in implementing it into their national legislation, taking into account their specific contexts and sectors. It is part of the broader EU cybersecurity strategy and complements other cybersecurity regulations, such as the GDPR and the Cybersecurity Act.[24] Compliance with the NIS Directive is important for operators in critical sectors, but also for OT manufacturers and suppliers, to ensure that they are adequately protecting their networks and information systems from cyber threats, and to meet their reporting obligations to the relevant national authorities.

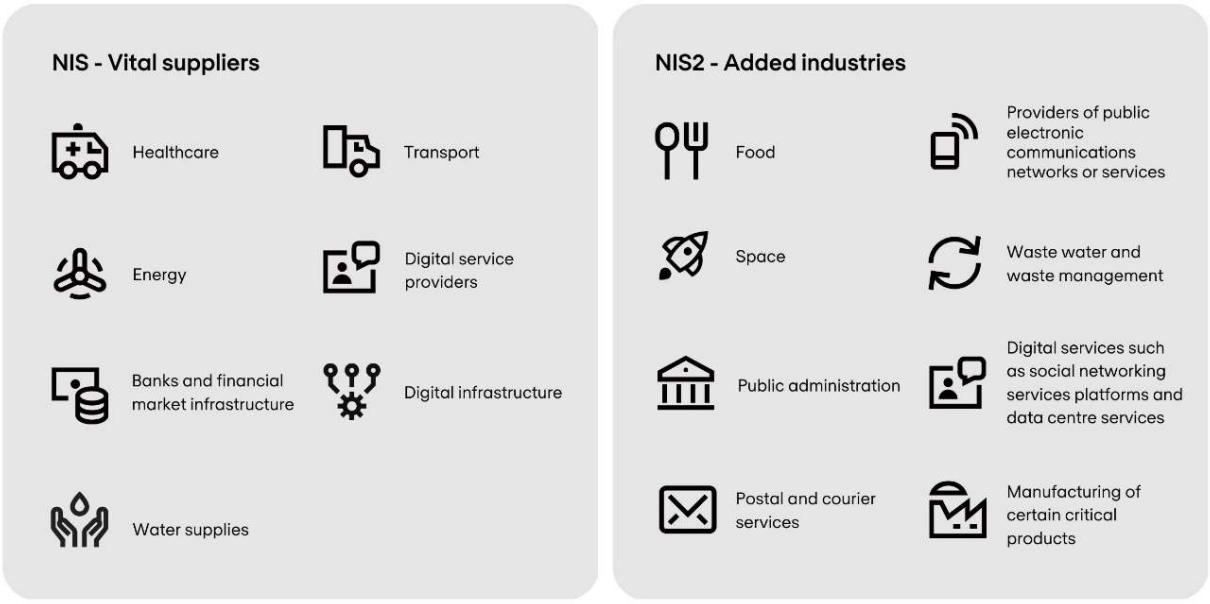


*Figure 12: An overview of the sectors where NIS and NIS2 apply.[25]*

[22] ENISA. (2023) *NIS Directive*. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

[23] European Parliament. (2023). *The NIS2 Directive: A high common level of cybersecurity in the EU.* Briefing: EU Legislation in Progress https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

[24] European Commission. (2023). *The EU Cybersecurity Act*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[25] Nomios. (2023). *What is NIS2 and what does it mean for your organisation?* https://www.nomios.com/resources/what-is-nis2/

# 3 #HACKMYBUILDING WORKSHOP

This chapter explores the outcomes of the #hackmybuilding workshop held during the 4th consortium meeting of the B4B project. It provides an overview of the workshop setup, discusses the results of the hands-on exercise, and outlines the main lessons learned. The chapter emphasizes the importance of data security in smart buildings, the challenges posed by interconnectivity, and the need for a comprehensive approach to securing building management systems.

## 3.1 Workshop Setup

The #hackmybuilding workshop was divided into two parts, focusing on both theory and hands-on exercises. In the first part, participants were introduced to the data security aspects and main risks in smart buildings and operational technology (OT) due to the increasing interconnectivity of devices. The second part involved a hands-on exercise, where participants were divided into two teams and given several tasks.

The tasks included setting up a building management system (BMS) architecture, identifying weak points, assessing risks, and securing the BMS architecture. Both teams were then asked to hack each other's BMS architecture. The BMS architecture was provided on paper, and teams used stickers and pens to mark necessary risks, weak points, and hacking strategies (Figure 13).


*Figure 13: #Hackmybuilding workshop setup (Teams, Rules and Provided BMS Architecture)*

## 3.2 Workshop Outcome

The two teams successfully set up and secured their respective BMS architectures, and then attempted to hack the other team's system. The exercise highlighted the vulnerabilities inherent in BMS architecture and emphasized the importance of a thorough risk assessment. It also demonstrated the complex relationship between physical and cyber security, as well as the role of supply chain security in overall system protection. Figure 14 shows the summary of the outcome of that workshop.


*Figure 14: Workshop outcome summarized*

## 3.3 Resultant from the workshop

Based on the findings from the workshop, we learned that data security measures play a crucial role in ensuring the safety and integrity of Building Management System (BMS) architectures. As smart buildings become more interconnected and technologically advanced, implementing effective security strategies across various components of BMS architectures is essential. Figure 15 outlines the different aspects of a BMS architecture and the corresponding security measures that should be in place:

The key points are:

1. On-site smart utilities and devices must be protected through a combination of physical security measures, regular controller updates, firewall-secured LAN or WLAN connections, and authentication processes. Additionally, systems segregation should be implemented to limit potential breaches, and privacy considerations must be addressed, particularly with regard to surveillance equipment.

2. When multiple BMS systems are present on-site, additional physical security measures are required to complement the virtual and LAN connection security. This includes implementing authentication processes and firewalls to safeguard sensitive information and systems.

3. Remote connections to the BMS architecture necessitate the implementation of multiple security layers to ensure that data and system integrity is maintained when accessed from off-site locations.

4. IoT devices warrant special attention due to their direct connection to central databases via the internet. Ensuring that these devices are secure and protected from potential cyber threats is essential for maintaining overall system security.

5. Off-site databases should be provided by trusted and certified providers who guarantee the physical and cyber security of their systems, regular updates, and rapid response times to cyber-attacks.

6. Establishing appropriate roles and responsibilities within the BMS architecture is crucial for maintaining security. Ensuring that personnel have access to information and systems only at the level required for their role helps prevent unauthorized access and potential security breaches.

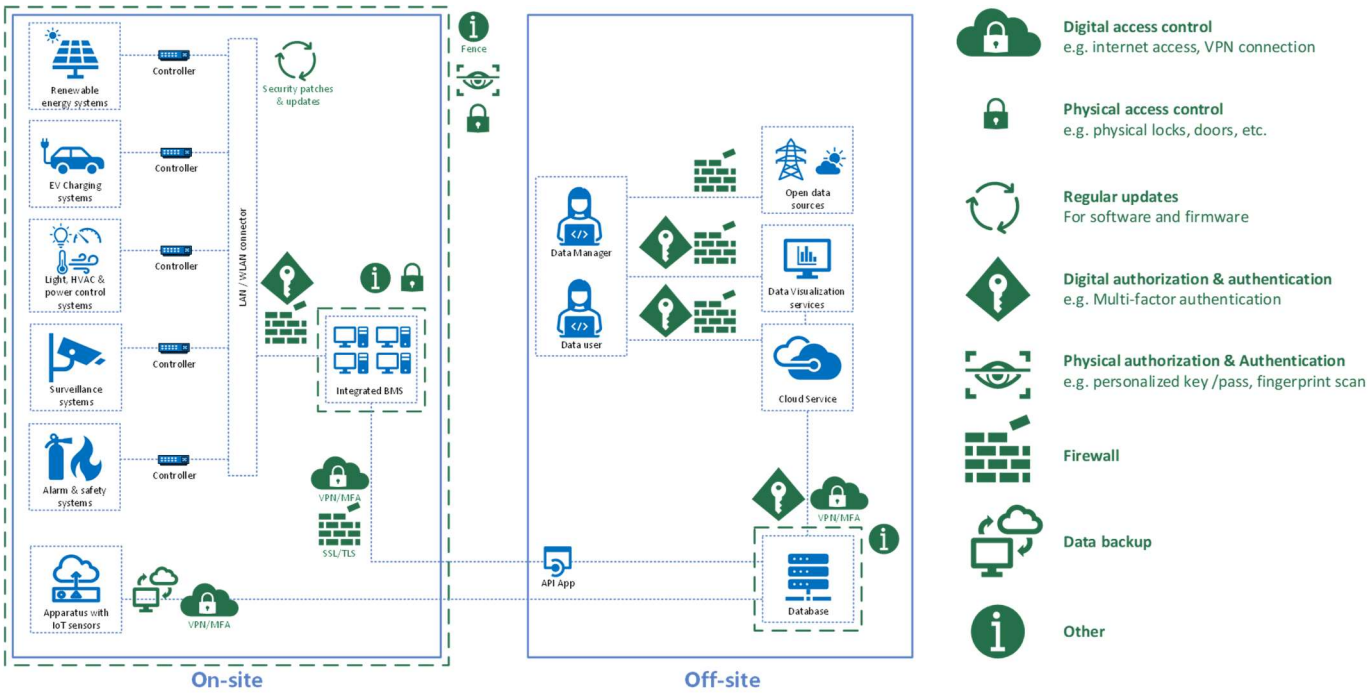


*Figure 15: Data Security measures applied to a typical smart building use case*

## 3.4 Main takeaways from the workshop

The main takeaways from the #hackmybuilding workshop are as follows:

1. Data security is ultimately about ensuring the health and safety of people. As buildings become smarter and more interconnected, the potential impact of a cyber-attack on occupants' well-being increases.

2. Given enough time, a determined attacker can always find a way to compromise a system. The key is to introduce enough barriers to deter attackers and encourage them to move on to an easier target.

3. The lack of clarity regarding data ownership complicates cyber security efforts. Clear policies and guidelines are needed to protect the data generated and transmitted by smart building systems.

4. Physical security and cyber security are intertwined. Protecting the hardware and firmware of building system components is crucial to maintaining overall system security.

5. System-level security is a critical aspect of smart building security. Ensuring that each component in the system is secure helps prevent weak links from compromising the entire architecture.

In conclusion, the #hackmybuilding workshop provided valuable insights into the challenges and complexities of securing smart building systems. A comprehensive, multi-faceted approach to security is necessary to protect the health and safety of building occupants, and to maintain the overall integrity of smart building infrastructure. By incorporating these data security measures into the BMS architecture, stakeholders can create a more secure, resilient, and reliable environment for occupants and users, ultimately fostering a safer and more efficient smart building ecosystem.

# 4 DATA PRIVACY AND ETHICS ASPECTS

The rapid development of smart buildings has introduced innovative solutions for energy management, security, and overall efficiency. Yet, as these buildings become increasingly reliant on data collection and sharing, concerns over data privacy and ethics arise. As we've already seen in chapter 1.1, Data privacy is the fundamental right of individuals to control how their personal information is collected, used, and shared, while data security is the practice of protecting digital information from unauthorized access, corruption, use, disclosure, modification, or destruction throughout its entire lifecycle. The two are intrinsically interconnected since ensuring adequate data security for all on- and off-site data platforms can protect sensitive data that may be subject to privacy laws. In the EU, the General Data Protection Regulation (GDPR) harmonizes data privacy laws across European member states. Building owners, building services suppliers and maintenance providers, Technology providers, and other stakeholders dealing with data collected by smart buildings should adhere to these laws when dealing with person-related data.

This chapter explores the various aspects of data privacy and ethics in the context of smart buildings. It highlights the importance of balancing technological advancements with the protection of individual rights, and discusses findings from the STOA's Scientific Foresight Project on Ethical Aspects of Cyber-Physical Systems, at the same time highlighted the key elements of data privacy and security in smart buildings.

### Understanding Data Collection in Smart Buildings

Smart buildings employ a vast array of sensors, devices, and systems to collect data, which is then analysed to optimize building performance, security, and comfort. Data collected can include energy consumption, temperature, humidity, occupancy, and access control information. Within the B4B project two areas of data collection are particularly concerned with person-related data: 1) buildings occupancy data for optimization of energy consumption and maintenance; 2) data used to understand end-users' behavior in relation to energy performance (such as ease of use, comfort, and indoor environmental quality).[26] While this data is critical to optimize a smart building's functionality and performance, it raises concerns over the potential misuse of personal information and the ethical implications of data collection.[27]

### Data Privacy Concerns in Smart Buildings

Data privacy in smart buildings primarily revolves around the protection of personally identifiable information (PII). The collection, storage, and sharing of PII can lead to privacy breaches, identity theft, and unauthorized surveillance. As a result, it is crucial to establish a comprehensive privacy policy and ensure compliance with data protection regulations such as the General Data Protection Regulation (GDPR).[28]

### Ethical Considerations in Smart Buildings

Ethical considerations in smart buildings include transparency, consent, and fairness. Building operators should inform occupants about the data collected, its purpose, and how it will be used. Additionally, individuals should have the option to provide or withhold consent to data collection. Finally, ensuring equitable access to the benefits of smart buildings and preventing discrimination based on data are crucial aspects of ethical smart building design.[29]

[26] Sebastian, R., Chochanova, E. (2022). *Literature and market study of existing regulations and approaches regarding data privacy, ethics, and security, including GDPR constraints.* B4B. https://brains4buildings.org/wp-content/uploads/2022/02/B4B-WP4-D4.1_Study-on-data-privacy-security-and-ethics_FINAL.pdf

[27] IBM. (2018). *What are smart buildings?* https://www.ibm.com/topics/smart-buildings

[28] European Commission. (n.d.). *General Data Protection Regulation (GDPR).* https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

[29] European Commission. (2020). *Ethics guidelines for trustworthy AI.* https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

### Balancing Innovation and Privacy in Smart Buildings

To address data privacy and ethical concerns in smart buildings, stakeholders must adopt a multidisciplinary approach that encompasses technology, policy, and public awareness. Privacy-enhancing technologies such as anonymization, encryption, and differential privacy can help protect sensitive information. Additionally, incorporating privacy-by-design principles and adhering to data protection regulations can create a responsible framework for managing and sharing data in smart buildings.[30]

## 4.1 Ethical Aspects of Cyber-Physical Systems: Findings from the STOA's Scientific Foresight Project

The Scientific Foresight project on the ethical aspects of cyber-physical systems (CPS) was requested by the Science and Technology Options Assessment Panel (STOA) of the European Parliament. The study aimed to understand the societal and ethical implications of CPS, which are integral to smart buildings, and provide guidance on responsible development and deployment.[31]

### Key Findings

The study highlights the importance of a comprehensive ethical framework for CPS, addressing issues such as privacy, data protection, transparency, accountability, and non-discrimination. It emphasizes the need for strong data protection measures and adherence to data protection regulations, such as the GDPR. Furthermore, the study stresses the importance of preserving human autonomy in the face of increasing automation and decision-making by CPS, and underscores the need to clearly define and assign responsibility and accountability for their actions.

## 4.2 Key Elements of Data Privacy and Security in Smart Buildings

Ensuring data privacy and security in smart buildings requires a thorough understanding of the key elements involved in protecting sensitive information. These key elements include:

#### Data Minimization

Collect only the data necessary for specific purposes, reducing the risk of unauthorized access or misuse.

#### Access Control

Limit access to sensitive data to authorized personnel only, using techniques like role-based access control (RBAC) and multi-factor authentication (MFA).

#### Data Encryption

Employ encryption for data storage and transmission to protect it from unauthorized access, tampering, or theft.

#### Regular Security Audits

Conduct periodic security audits and vulnerability assessments to identify and mitigate potential threats to data privacy and security.

#### Incident Response Planning

[30] NIST. (2017). *An introduction to privacy engineering and risk management in federal systems*. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[31] European Parliament. (2016). *Ethical aspects of cyber-physical systems*. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/563501/EPRS_STU%282016%29563501_EN.pdf

Develop a comprehensive incident response plan to address security breaches or data privacy incidents effectively and efficiently.

### Employee Training

Provide regular training and education for employees to raise awareness about data privacy and security best practices and policies.

### Privacy-by-design

Integrate data privacy and security considerations into the design and development of smart building systems and technologies from the start of their design and throughout their life-cycle.

## Conclusion

As smart buildings continue to evolve, it is crucial to address data privacy and ethics concerns. By implementing robust privacy policies, such as the GDPR, utilizing privacy-enhancing technologies, and promoting transparency, consent, and fairness, the industry can harness the benefits of smart buildings while protecting the rights and interests of occupants. Collaboration between stakeholders, including building owners, technology providers, policymakers, and occupants, will ensure that smart buildings remain a driving force in creating efficient, sustainable, and responsible urban environments.[32][33]

[32] NIST. (2017). *An introduction to privacy engineering and risk management in federal systems.* https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[33] Jansen, W., & Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing.* NIST Special Publication 800-144. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

# 5 DATA PRIVACY, SECURITY & ETHICS FRAMEWORK

As the digital revolution continues to transform our world, smart buildings are increasingly becoming an integral part of modern urban landscapes. These advanced structures leverage cutting-edge technologies to monitor, control, and automate various building functions, enhancing energy efficiency, occupant comfort, and overall functionality. However, with the growing interconnectivity of devices and systems, the challenges of ensuring data privacy, security, and ethical considerations within smart buildings are becoming increasingly complex.

The "People, Process, Technology" (PPT) framework, inspired by Harold Leavitt's "Diamond model" from 1956, provides a comprehensive approach to addressing these challenges in smart buildings. To further enhance the effectiveness of the PPT framework in the context of smart buildings, two complementary approaches, the Top-Down and Bottom-Up approaches, are introduced. A smart building system architecture lies at the core of the framework and should be assessed from both bottom-up and top-down perspectives to establish a comprehensive data privacy, security and ethics strategy (see Figure 16). These approaches provide a structured methodology for evaluating the necessary security levels and establishing fitting security measures and risk mitigation strategies tailored to the unique requirements of each smart building.

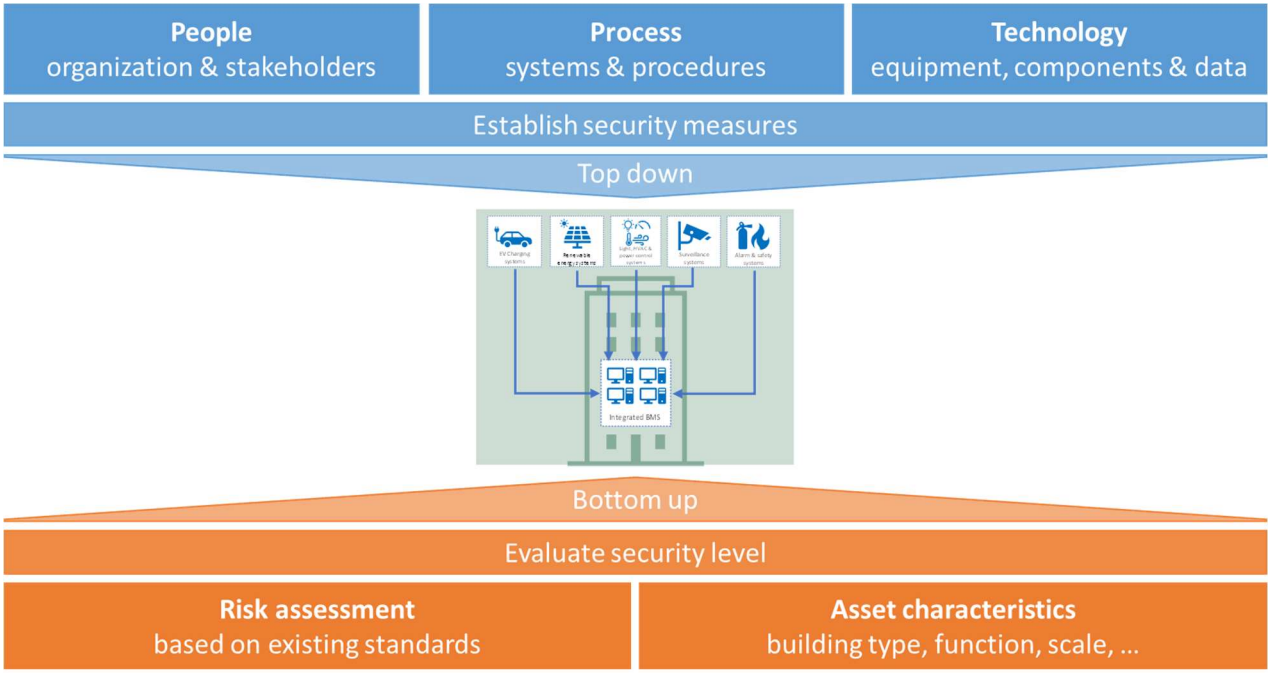


*Figure 16: The data privacy, security, and ethics framework guides stakeholders to evaluate real estate assets bottom-up, including the inherent characteristics and risk levels before establishing appropriate security measures top-down.*

The Top-Down approach focuses on implementing the PPT framework based on the evaluation conducted in the Bottom-Up approach, which involves assessing the asset or series of assets and their system architecture to determine the necessary security level. This comprehensive approach enables stakeholders to prioritize and address potential risks and vulnerabilities effectively, taking into account the building's specific characteristics, such as its function, size, and level of "smartness."

In this context, the Smart Readiness Indicator (SRI) serves as a valuable tool for assessing the required security level of a building, as the smarter the building, the higher the security level required. By considering the SRI, stakeholders can make informed decisions regarding the necessary security measures to protect their assets and uphold data privacy, security, and ethical considerations.

The following chapters we will delve deeper into the PPT framework, the Top-Down and Bottom-Up approaches, and their applications in the realm of smart buildings. The subsequent chapters will outline the key principles and strategies for ensuring the privacy, security, and ethical management of smart buildings, covering topics such as risk assessment, data ownership and protection, supply chain security, and the role of stakeholders in maintaining a secure and ethical environment.

By embracing and implementing this comprehensive framework for data privacy, security, and ethics in smart buildings, stakeholders can effectively safeguard their assets, ensure the well-being of occupants, preserve the integrity of building systems, and foster a responsible and ethical approach to technological advancement in the built environment, all while taking into account the crucial interplay of people, processes, and technology.

## 5.1 The framework

In this chapter, we introduce the framework for data privacy, security, and ethics in smart buildings, emphasizing its foundation on the "People, Process, Technology" (PPT) model and the integration of the Top-Down and Bottom-Up approaches. The "People, Process, Technology" (PPT) framework, inspired by Harold Leavitt's "Diamond model" from 1956, provides a comprehensive approach to address the complex challenges of data privacy, security, and ethics in smart buildings. By considering the interconnected aspects of people, processes, and technology, the framework aims to create a holistic and balanced approach to safeguarding smart buildings from potential threats and ensuring the ethical management of data.

By gaining a comprehensive understanding of the framework and its core principles, stakeholders will be better equipped to make informed decisions and implement effective strategies for safeguarding their assets and upholding the highest standards of data privacy, security, and ethics in the rapidly evolving world of smart buildings.

### 5.1.1 Bottom-up Approach - Evaluating the Necessary Security Levels

In the Bottom-up approach, the primary focus is on evaluating the necessary security levels for a given smart building or a series of assets or asset portfolios. This approach involves a detailed examination of the asset characteristics and conducting risk assessments, which in turn helps to determine the required security measures. The Bottom-up approach can be divided into two main components:

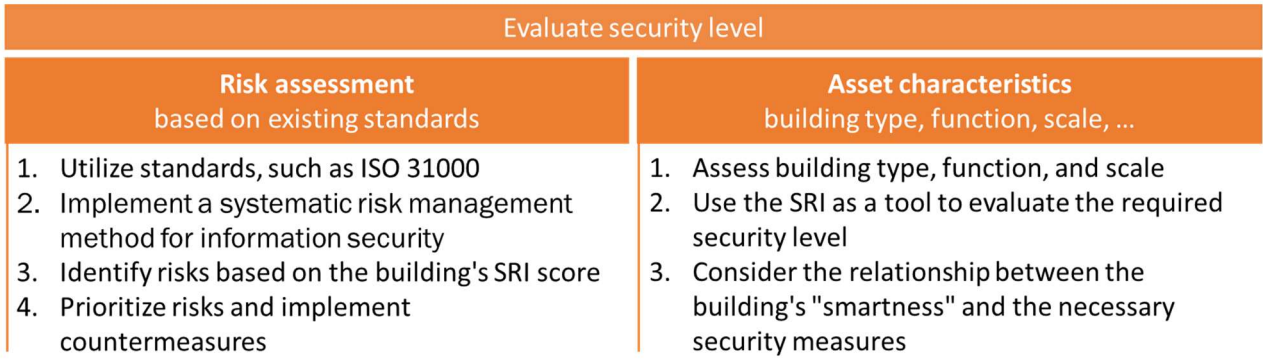


*Figure 17: The Bottom-Up approach showing the main components and their sub-components for evaluating the necessary data security levels.*

#### Risk Assessment: Reference to Existing Standards

1. Utilize standards like ISO 31000 for risk assessment: ISO 31000 is an internationally recognized standard for risk management. It provides a comprehensive framework for identifying, assessing, and managing risks in various contexts, including smart buildings. By adopting this standard, stakeholders can ensure a systematic and consistent approach to risk assessment.

2. Implement a systematic risk management method for information security: Organizations should adopt a structured risk management process to identify, analyse, evaluate, and treat information security risks. This process should involve regular reviews and updates to ensure that risks are appropriately managed and mitigated as the building's environment and threat landscape evolve.

3. Identify risks based on the building's SRI score: Evaluate potential risks using the Smart Readiness Indicator score to prioritize threats and implement appropriate countermeasures.

4. Prioritize risks and implement countermeasures: Develop a plan to address identified risks, prioritizing those with the highest potential impact on the smart building's security and operations.

#### Asset Characteristics: Building Type, Function, Scale, etc.

1. Assess building type, function, and scale: The asset characteristics, such as the building's type, function, and scale, play a crucial role in determining the necessary security levels. For instance, a large commercial building with multiple tenants and complex systems may require a higher level of security than a smaller residential building.

2. Use the Smart Readiness Indicator (SRI) as a tool to evaluate the required security level: The SRI is an assessment tool designed to gauge the necessary security level for a building based on its smartness. In general, the smarter the building, the higher the required security measures. By considering the SRI, stakeholders can make informed decisions regarding the appropriate security measures for their assets.

3. Consider the relationship between the building's "smartness" and the necessary security measures: As the level of "smartness" increases, so does the complexity of the building's systems, leading to higher potential risks. Stakeholders should carefully evaluate the interplay between the building's smart features and the security requirements to ensure a balanced and effective approach to risk mitigation.

In conclusion, the Bottom-up approach to evaluating the necessary security levels for smart buildings involves a comprehensive assessment of both risk and asset characteristics. By combining the insights gained from this evaluation with existing risk management standards like ISO 31000, stakeholders can develop a well-informed and tailored strategy to address the unique security requirements of each building. This approach ensures that smart buildings are not only efficient and comfortable but also secure and resilient in the face of evolving threats.

### 5.1.2 Top-Down Approach - Establishing Fitting Security Measures and Risk Mitigation Strategies

The Top-Down approach focuses on establishing appropriate security measures and risk mitigation strategies based on the evaluation conducted in the Bottom-up approach. This process involves the implementation of the People, Process, and Technology (PPT) framework to address the unique security requirements of each smart building. The Top-Down approach can be divided into three main components, following that framework.

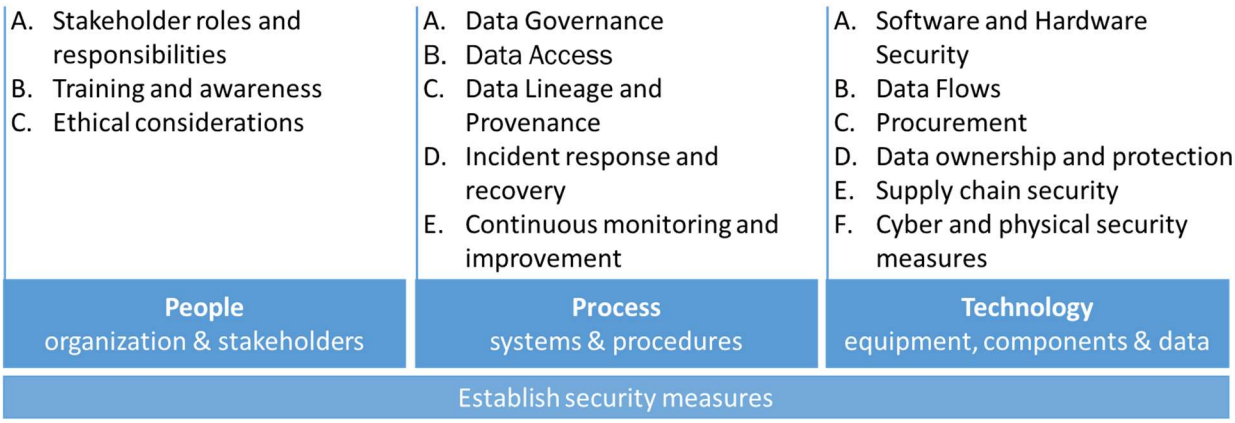


*Figure 18: The Top-Down approach showing the main components and their sub-components for establishing successful data security measures.*

### People: organization & stakeholders

A. Stakeholder roles and responsibilities

1. Building owners and operators: Ensure the implementation of security measures, compliance with regulations, and ongoing maintenance of smart building systems.
2. Facility managers, suppliers and maintenance service providers: Oversee the daily operations of the building and coordinate with IT and security professionals to maintain a secure environment.
3. IT and security professionals: Implement and maintain security measures, monitor potential threats, and respond to security incidents.
4. Occupants and users: Adhere to security policies and guidelines, report any security concerns, and participate in security awareness initiatives.

B. Training and awareness

1. Regular security training programs: Offer training programs that cover essential security topics, such as threat awareness, best practices, and incident response. Some well-known certifications include Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and CompTIA Security+.
2. Promoting a security-conscious culture: Encourage all stakeholders to be proactive in maintaining a secure environment, fostering a culture that prioritizes security and privacy.

C. Ethical considerations

1. Data privacy and protection: Ensure that personal and sensitive data is collected, stored, and processed responsibly, adhering to applicable data protection regulations, such as the General Data Protection Regulation (GDPR).
2. Transparent and responsible data usage: Communicate with stakeholders about data collection, processing, and sharing practices, ensuring that data is used ethically and responsibly.

### Process: systems & procedures

A. Data Governance

1. Establish data governance policies: Develop and implement data governance policies that outline data management principles, data quality standards, and compliance requirements.

2. Assign data governance roles and responsibilities: Designate stakeholders responsible for data governance, ensuring accountability and oversight of data management activities.

B. Data Access

1. Define data access policies: Create policies that specify who can access specific types of data, under what conditions, and for what purposes.
2. Implement access control mechanisms: Employ technical solutions such as role-based access control, multi-factor authentication, and privileged access management to enforce data access policies.

C. Data Lineage and Provenance

1. Track data lineage: Maintain records of data origin, transformations, and movement throughout the smart building systems to ensure traceability and transparency.
2. Document data provenance: Preserve information about the source and ownership of data, enabling stakeholders to assess its reliability and authenticity.

D. Incident response and recovery

1. Developing a comprehensive incident response plan: Create a detailed plan that outlines the roles and responsibilities of stakeholders, communication protocols, and actions to be taken during and after a security incident.
2. Regular testing and updating of the plan: Conduct periodic tests of the incident response plan to ensure its effectiveness and make necessary updates in response to new threats and technologies.

E. Continuous monitoring and improvement

1. Periodic security audits and assessments: Carry out regular security audits and assessments to evaluate the effectiveness of implemented security measures and identify areas for improvement.
2. Updating security measures in response to new threats and technologies: Continuously review and update security measures to maintain their effectiveness in the face of evolving threats and technological advancement

### Technology: equipment, components & data

A. Software and Hardware Security

1. Regularly update software and firmware: Ensure that all software and firmware are updated to the latest versions, including operating systems, applications, and IoT devices, to protect against known vulnerabilities.
2. Secure configuration: Implement secure configurations for hardware and software, following industry best practices and guidelines to minimize potential attack vectors.

B. Data Flows

1. Data flow mapping: Identify and document the flow of data within the smart building, including ingress and egress points, to facilitate risk assessment and mitigation.
2. Data flow protection: Implement appropriate security measures, such as encryption and access controls, at various stages of data flow to ensure the integrity and confidentiality of sensitive data.

C. Procurement

1. Security requirements in procurement processes: Incorporate security requirements and considerations into procurement processes, ensuring that purchased hardware, software, and services adhere to established security standards.

2. Vendor risk assessment: Evaluate potential vendors based on their security posture, track record, and ability to meet the smart building's security requirements.

D. Data ownership and protection

1. Establishing clear data ownership policies: Define and communicate data ownership policies to ensure that all stakeholders understand their responsibilities in protecting and managing data.
2. Implementing robust data encryption and access controls: Employ strong encryption methods and access controls to safeguard sensitive data and prevent unauthorized access.

E. Supply chain security

1. Assessing the security posture of suppliers and vendors: Evaluate the security practices and standards of suppliers and vendors to minimize potential risks and vulnerabilities.
2. Ensuring secure integration of components and systems: Verify that components and systems are securely integrated, minimizing potential weak points in the overall building system architecture.

F. Cyber and physical security measures

1. Network segmentation and firewalls: Implement network segmentation and firewalls to protect critical systems and data from unauthorized access and potential cyberattacks.
2. Access controls and intrusion detection systems: Deploy access controls and intrusion detection systems to prevent unauthorized access and detect any suspicious activities.
3. Secure building management systems (BMS) and IoT devices: Ensure that BMS and IoT devices are secured, regularly updated, and protected against potential vulnerabilities and threats.

In conclusion, the framework for data privacy, security, and ethics in smart buildings, based on the "People, Process, Technology" (PPT) model and incorporating the Top-Down and Bottom-Up approaches, offers a comprehensive and holistic methodology for safeguarding intelligent structures. By addressing the interconnected aspects of people, processes, and technology, the framework enables stakeholders to proactively manage the complex challenges associated with the increasing interconnectivity of devices and systems within smart buildings. As we continue to advance in the digital age, embracing this dynamic framework will be crucial for the successful implementation of secure, ethical, and privacy-preserving smart building systems.

Through continuous improvement and adaptation in response to evolving threats and technological advancements, stakeholders can ensure the well-being of occupants, preserve the integrity of building systems, and foster a responsible and ethical approach to the ongoing digital revolution in the built environment. As the landscape of threats and technologies continuously evolves, it is imperative for stakeholders to remain vigilant and adaptive, ensuring that the framework is updated and improved to counter emerging challenges. The successful implementation of the PPT framework in smart buildings will not only promote a secure and ethical environment but also contribute to the overall resilience and sustainability of the built environment. Ultimately, this comprehensive approach will play a critical role in fostering trust and confidence in smart building technologies and their potential to transform our urban landscapes for the better.

# 6 RECOMMENDATIONS OR "HOW TO BUILD MORE CYBER RESILIENCE"

In the context of the data privacy, security, and ethics framework discussed in the previous chapter, this section focuses on actionable recommendations to enhance cyber resilience in smart buildings. This chapter highlights essential steps that building owners and operators, facility managers, suppliers and maintenance service providers and other stake-holders should consider to mitigate potential threats and vulnerabilities, ultimately creating a more secure, sustainable, and resilient cyber-physical ecosystem within the built environment. These recommendations will serve as a valuable guide for stakeholders to follow as they navigate the complex landscape of data privacy, security, and ethics in the realm of smart buildings.


*Figure 19: Ten step recommendation to enhance cyber resilience in smart buildings*

- **Step 1: Conduct a comprehensive risk assessment.** Analyse the smart building's systems, networks, and devices to identify potential vulnerabilities and threats. This initial assessment will help prioritize risks and form the basis for implementing appropriate countermeasures.
- **Step 2: Develop a risk mitigation plan.** Create a plan that ranks identified risks and outlines the appropriate countermeasures to be implemented. This plan should be reviewed and updated periodically to account for new threats and technological advancements.
- **Step 3: Establish clear policies and procedures.** Develop and communicate security policies, procedures, and guidelines for all stakeholders to ensure adherence to best practices and regulatory requirements. This includes data ownership, access controls, and incident response procedures.
- **Step 4: Implement robust security measures.** Deploy state-of-the-art technological solutions, such as network segmentation, firewalls, intrusion detection systems, and encryption, to safeguard critical systems and data from unauthorized access and potential cyberattacks.
- **Step 5: Train and educate stakeholders.** Implement regular training and awareness programs to educate stakeholders about potential security threats, best practices for mitigating risks, and the importance of adhering to security policies. Foster a security-conscious culture that encourages proactive behaviour and vigilance among all stakeholders.
- **Step 6: Monitor and audit security measures.** Conduct periodic security audits and assessments to evaluate the effectiveness of implemented security measures, identify areas for improvement, and ensure compliance with regulatory requirements.

- **Step 7: Develop a comprehensive incident response plan.** Create a detailed incident response plan that outlines the roles and responsibilities of stakeholders, communication protocols, and actions to be taken during and after a security incident. Regularly test and update the plan to ensure its effectiveness in the face of evolving threats.
- **Step 8: Address supply chain security.** Evaluate the security posture of suppliers and vendors, and ensure secure integration of components and systems. Implement stringent security requirements for third-party providers to minimize potential risks and vulnerabilities.
- **Step 9: Encourage collaboration and information sharing.** Promote collaboration and information sharing among stakeholders, including building owners, facility managers, suppliers and maintenance service providers, IT professionals, and occupants, to identify potential threats and improve overall security posture.
- **Step 10: Continuously review and update the data privacy, security, and ethics framework.** As threats and technologies evolve, regularly review and update the data privacy, security, and ethics framework to maintain its effectiveness. Stay informed about emerging threats and best practices, and adapt security measures as needed to ensure the ongoing protection of smart buildings and their occupants.