Cyber Security Agency of Singapore

In support of

SMART NATION SINGAPORE
A THRIVING DIGITAL FUTURE FOR ALL

Guide on Conducting Threat Identification and Assessing Effectiveness of Controls for Smart Buildings

March 2026

TABLE OF CONTENTS

1. Introduction

Cyber-physical attacks are when a cyber incident causes real-world, physical consequences by targeting systems that bridge digital and physical domains, such as building controls or infrastructure. The acceleration of digitalisation has significantly broadened this threat landscape, as legacy building IT systems are increasingly interconnected with emerging smart technologies, resulting in new operational and security risks. While such advancements complement Singapore's Smart Nation 2.0 vision of a digitally integrated society, they simultaneously reflect a global trend in which the adoption of smart building systems is redefining the attack surface exposure and thus operational and security risk profiles.

Recent real-world incidents have reinforced these concerns, highlighting how malicious actors have exploited vulnerabilities within building automation and management systems, resulting in operational disruptions, compromised safety, and substantial remediation costs.

In 2021, attackers compromised building automation devices in a German office park, locking out administrators and disabling essential systems such as lighting and motion detection, resulting in major operational disruptions and costly remediation efforts.[1] Similarly, in 2023, publicly exploited vulnerabilities in Building Management System (BMS) products like Schneider Electric's KNX demonstrated the potential for unauthorised access to critical building controls.[2]

In acknowledgement of the emergence of cyber-physical risks, organisations must proactively identify these threats and implement effective controls and mitigation strategies from the outset. To further raise awareness of the growing impact of cyber-physical threats, the Cyber Security Agency of Singapore (CSA) launched its inaugural Securing Smart Cities event at the Singapore International Cyber Week 2024, focusing on the theme "Emergence of Cyber-Physical Risk" to raise awareness of the growing challenges these threats pose for smart urban infrastructure. As a follow up to this inaugural event CSA in support of Smart Nation Singapore have developed this guide.

2. Disclaimer

This guide provides practical guidance for conducting threat identification and selecting effective controls and mitigations for smart buildings. The recommendations are not exhaustive and do not constitute endorsement by CSA or imply compliance with CSA-published policies and regulations.

Organisations are solely responsible for selecting, using, and validating the suitability of this information and assume any liability resulting from such use. Always consult trained cybersecurity professionals before making business-critical security decisions. Risk assessments may guide the selection of mitigations within organisations.

All tables and images included are for illustration and example purposes only, and do not represent comprehensive or definitive models.

3. Acknowledgements

The development of this document has benefited significantly from the inputs and support provided by the following agencies and organisations, as well as the resources listed under References.

1. SMART NATION GROUP - DIGITAL GOVERNMENT (SNDG)
2. THE BUILDING AND CONSTRUCTION AUTHORITY (BCA)
3. INFOCOMM MEDIA DEVELOPMENT AUTHORITY (IMDA)
4. HOUSING AND DEVELOPMENT BOARD (HDB)
5. JTC CORPORATION
6. GARTNER

4. Purpose, Audience & Scope

4.1 Purpose of this Guide

As the adoption of smart building systems continues to grow, the threat landscape inevitably expands alongside it. Malicious actors are increasingly targeting vulnerable building systems, particularly legacy or outdated IT systems that have been integrated with smart devices. These attacks create complex attack surfaces where weaknesses in one component can compromise entire systems, posing significant risks to occupant safety, operational continuity, and business objectives that should deeply concern building operators, facility managers, and other stakeholders.

However, addressing these technological risks is complicated by critical human factors that amplify the vulnerabilities. Facility teams often lack understanding of core cybersecurity principles and concepts, struggling when applying high-level frameworks or implementing checklist-based compliance standards without grasping underlying risks. This skills deficit is exacerbated by broader stakeholder awareness gaps, where decision-makers have limited understanding of cyber-physical threats.

Consequently, even as organisations invest in smart building technologies, the human element necessary to secure these systems effectively remains underdeveloped, creating a dangerous disconnect between technological advancement and security capability.

Why This Guide Matters for Facility Teams

Facility team and building operators are progressively being placed at the frontline of cyber-physical defences due to the increased digitalisation of systems to manage the physical environment.

Furthermore, cybersecurity risks are introduced into building operations through the integration of smart devices, Internet-of-Things (IoT) sensors, and advanced building management systems (BMS), cloud-based platforms, and artificial intelligence-driven analytics. This shift means that facility teams, who traditionally focused on operational reliability and physical safety, now have a critical role in protecting the digital infrastructure of their buildings from cyber threats.

Empowering Non-Cybersecurity Team Members

Facility teams traditionally focus on tasks such as maintaining and monitoring building automation systems, energy management tools and access controls, which have a direct impact on the resilience and safety of smart buildings. When cyber-attacks target these systems, they have the potential to disrupt operations or exploit automation features, which could result in endangerment of lives and damage to property.

Therefore, it has become essential for facility teams to be able to contextualise threat identification, analysis and risk mitigation in terms of cybersecurity. With this understanding, they would be in a better position to effectively identify, respond to, and mitigate cyber-physical risks, thus protecting building occupants, business continuity and sensitive information.

As Singapore's founding father, the late Mr Lee Kuan Yew, once observed, "If you give a man a fish, you have fed him for a day. If you teach him how to fish, you feed him for a lifetime." This guide embraces that philosophy and is specifically designed for practitioners without cybersecurity expertise. It provides practical, step-by-step methods to help non-specialists systematically identify, prioritise, and address security risks in their operating environments.

Key focus areas include:

- Recognising cyber-physical threats within building and automation systems.
- Identifying assets with CPS considerations, including those arising when legacy systems are connected to new smart technologies.
- Working effectively with IT and security partners to address identified threats.

By concentrating on the unique requirements of buildings and facility management teams, the guide empowers professionals to take a proactive approach—rather than reactive— in cyber-physical risk management.

Complementing Existing Resources

Unlike other cybersecurity resources that focus predominantly on IT environments, where prominent publications often provide outcome-driven or compliance-based guidance—such as outlining principles, best practices, and security controls—they seldom offer detailed, step-by-step manuals for practical cyber-physical risk identification in building environments.

Hence, this document is designed to complement and fill that gap, instead of replacing existing standards and best practices. It should be used alongside established resources such as the "Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure" and the "Guide to

Cyber Threat Modelling" [3] released by CSA in 2021, as well as regional and international frameworks. These include but not limited to:

- National Institute of Standards and Technology (NIST) frameworks: including the Cybersecurity Framework (CSF) and NIST SP 800-30 guidelines, widely referenced for cyber risk management [4,5]
- TR 111: Singapore's standard on securing cyber-physical systems for buildings, which provides baseline security principles. [6]
- IMDA's IoT Cybersecurity Guide: offering guidance on securing IoT deployments in diverse contexts, including buildings [7]
- IEC 62443: the international standard for security in industrial control and automation systems [8]
- ISO/IEC standards: such as ISO/IEC 27001 for information security management and ISO/IEC 30141 (IoT Reference Architecture) [9]
- Common Criteria (ISO/IEC 15408): providing an internationally recognised framework for evaluating the security of IT and operational products [10]

Together, these resources offer foundational principles, governance models, and recognised controls. This guide complements them by translating those standards into practical, building-specific methods that facility team and operators can immediately apply to enhance the resilience and safety of their smart building environments.

4.2 Audience & Scope

In addition to the building operators and facility team mentioned in the earlier section, this document may also be of value to a broader range of stakeholders involved in the management and security of smart buildings.

Stakeholders include but not limited to senior executives (CEO, COO, CDO, CISO), business and mission owners, procurement officers, program and security managers, enterprise and security architects, system and facility owners, risk assessors, auditors, and other key personnel responsible for the oversight, operation, security, and risk management of smart buildings within organisations. Consultants, integrators, and service providers engaged in conducting cyber-physical threat identification and mitigation for Smart Buildings on behalf of organisations.

The scope of this guidance is specifically focused on serving as a guide for conducting threat identification and assessing effectiveness of controls and mitigations for Smart Buildings. **Other aspects of risk management, such as ongoing monitoring and reporting, will not be the focus of this document.**

5. Characteristics Of Smart Devices, Cyber-Physical Systems and Smart Buildings

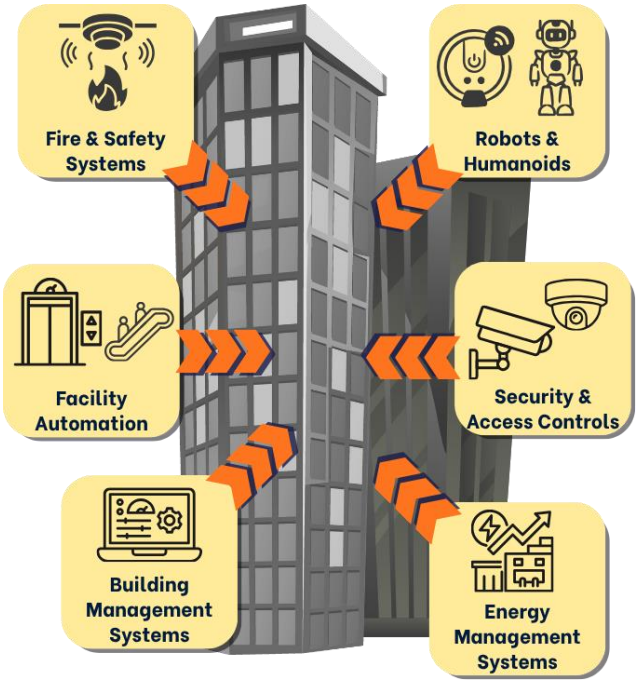

Figure 1. Smart Buildings an Integrated Cyber-Physical System

Sections 5.1 to 5.3 will outline the characteristics of smart devices, CPSs and smart buildings to establish the foundational components of the smart building ecosystem. Characterising these elements upfront provides the necessary context for understanding how CPS categories derive from and depend on these core building blocks. This allows the subsequent sections to build on these identified assets for further discussion and equip readers with the capability to recognise the smart assets more accurately.

5.1 Smart Devices

Smart devices are network-connected components with sensors, basic processing power, and actuators that can collect data, perform specific tasks, and communicate within smart building environments. While many are IoT components, in practice they may also run only on secure intranet or local networks. In such cases, they still act as “things” that provide monitoring and control, without requiring full exposure to the internet. Both Singapore Standards (SS) and international standards from ISO/IEC and NIST continue to recognise these devices as key parts of the cyber-physical ecosystem because they link physical functions with digital intelligence regardless of the connectivity model.

5.2 Cyber-Physical Systems in Smart Buildings

CPS, as defined by NIST, are engineered systems that tightly integrate physical components (such as sensors, actuators, and machinery) with computational elements (including software, networks, and control algorithms) to monitor and control physical processes in real time. CPS may cover beyond a building and over large areas and in this guide, we will focus specially on CPSs within smart buildings.

For example, from temperature sensors and occupancy detectors deployed within the building, CPS in Smart Buildings can make data driven decisions to optimise Heating Ventilation & Air Conditioning (HVAC) or also known as Air Conditioning & Mechanical Ventilation (ACMV) and control lighting for energy efficiency and occupant comfort. It can also integrate security sensors and access controls to intelligently respond to threats by adjusting building access or alerting security personnel. For this document, we will use the term HVAC to refer to ACMV as well.

Due to their real-time control over critical safety and operational functions, failures or cyber-attacks on CPS can cause significant operational disruptions, safety hazards, and potential harm to occupants.

CPS in smart buildings thus comprise interconnected smart devices and digital control platforms that enable adaptive, automated building operations. This integration allows buildings to respond dynamically to environmental changes and occupant needs.

5.3 Smart Buildings

A smart building integrates interconnected CPS and services—such as HVAC, lighting, access control, and energy management—to optimise operational efficiency, occupant comfort, and safety. According to NIST, smart buildings utilise a network of sensors, controls, and automation to collect data and enable intelligent decision-making processes that enhance building performance and user experience. The Cybersecurity and Infrastructure Security Agency (CISA) further highlights that this increased connectivity introduces new cybersecurity challenges that extend beyond traditional IT security scopes.

6. Key Cyber-Physical System Categories In Smart Buildings and Their Smart Device Components

Key CPS categories for smart buildings vary depending on the reference framework. It is important to identify the key CPS so that organisations can classify, prioritise and implement appropriate controls.

Prepared by the Working Group on Securing Cyber-physical Systems for Buildings, Technical Reference (TR) 111:2023 identifies several core CPS key categories—BMS, Building Automation System (BAS), physical systems and entitles, networks and communications, IoT devices, systems access controls, lighting, HVAC, and lifts and escalators—as critical for securing building cyber-physical environments.

Building on foundational cybersecurity guidelines and best practices developed by local and internationally recognised bodies such as Singapore Standards Council, NIST and CISA, this guide proposes a regrouping of the key categories to give focus on prominent common categories with consideration of the evolving threat landscape brought about by digitalisation.

Note: This list is not exhaustive; other specialised or emerging CPS may exist in specific contexts and should be included as part of holistic risk management strategies. The following ten key CPS categories and one miscellaneous category encompassing common smart building systems and their smart device components aims to form a starting point for audiences to develop more detailed assessments.

SN	CPS Category	Description	Common Smart Device Components	Why Cyber-Physical Risks Matter (Safety & Operational Impact)
1	Fire and Safety Systems	Detection and automated response	Smoke detectors, gas sensors,	Directly related to human life safety; cyberattack or

SN	CPS Category	Description	Common Smart Device Components	Why Cyber-Physical Risks Matter (Safety & Operational Impact)
		to fire, smoke, gas leaks, and other hazardous conditions.	sprinkler actuators, alarms	malfunction can cause failure to detect/respond to emergencies, leading to catastrophic harm or loss of life.
2	Autonomous Mobile Robots & Humanoids	Robots performing inspection, physical security, cleaning, delivery, and other facility tasks in shared spaces.	Cameras, gas detectors, thermal sensors, robotic manipulators	High safety risk due to physical presence and mobility; compromised robots could be manipulated to cause harm to occupants, endanger crowds, or exit buildings into dangerous environments (e.g., traffic).
3	Security and Access Control	Monitoring and controlling physical access, surveillance, and alarm systems maintaining security.	Smart locks, biometric scanners, cameras, motion detectors	Physical security breaches can endanger occupants, enable sabotage or theft, and create cascading operational risks; cyber intrusion can disable, or by-pass secured access.
4	BMS	Platforms integrating multiple CPS subsystems for coordinated control.	Sensors/actuators encompassing all subsystems	Centralised controllers are high-value cyber targets; disruption can cascade across multiple systems including safety-critical functions, threatening building resilience.
5	Facility Automation	Automated control of elevators, escalators, and facility logistics like automated doors.	Elevator controllers, automated doors, escalator controllers	Safety-critical equipment controls; cyber compromise could cause mechanical failure, entrapment, or accidents impacting occupant safety.
6	Energy Management Systems	Monitoring and optimisation of power usage and distribution within buildings.	Energy smart meters, smart plugs, power quality sensors	Cyber manipulation can cause power outages, overloads, or damage infrastructure, indirectly impacting safety and operational continuity.
7	HVAC / ACMV Control Systems	Real-time control of heating, ventilation, and air conditioning systems.	Temperature/ humidity sensors, actuators, smart thermostats	Poor climate control risks occupant health (e.g., heat stroke, poor air quality); cyber-attacks can disrupt comfort or exacerbate health hazards (e.g., poor ventilation during emergencies).

SN	CPS Category	Description	Common Smart Device Components	Why Cyber-Physical Risks Matter (Safety & Operational Impact)
8	Lighting Control Systems	Automated lighting controls based on occupancy and daylight.	Occupancy sensors, light sensors, smart bulbs, dimmers	Mostly related to comfort and operational efficiency, but compromised lighting can create visibility issues or panic during emergencies.
9	Water and Environmental Monitoring Systems	Management of water usage, quality, and environmental parameters.	Flow/water quality sensors, CO2 and VOC environmental sensors	Disruptions can compromise occupant health (e.g., water contamination, poor air quality) and damage building operations if water systems fail.
10	Predictive Maintenance Systems	Sensor analytics used to predict equipment failures and schedule maintenance proactively.	Vibration, temperature, pressure sensors	Failure to detect imminent faults may lead to safety-critical system breakdowns; cyber compromises can mask these faults, leading to unexpected failures and safety risks.
11	Other Building Services	Miscellaneous systems that do not belong to a specific category above but presents a cyber-physical risk that are not often regarded or well protected.	Vending Machines, Smart TVs, Parking system, Portable Media devices (Flash Drives etc), Unsecured USB ports & Network ports	Most of these systems do not directly cause safety issues, but real-world cases and research have shown that these devices have been used as entry points or for enterprise espionage and is for the reader to note these possibilities as well.

Table 1: Key CPS Categories

The working example in the following section focuses on these key CPS categories as they are more commonly deployed in smart buildings.

7. How To Conduct Threat Identification on Cyber-Physical Systems

Threat identification for CPS in smart buildings must consider two perspectives. This dual approach is necessary because computational components are tightly integrated with physical processes, all interacting through interconnected networks. Cyber vulnerabilities can lead to real-world physical harm, so threats arising from each CPS category's digital operational context and how it translates to physical world must be considered. This section guides readers, through a clear, step-by-step method to identify threats that affect both cyber assets and physical safety, enabling effective threat identification tailored to smart building CPS environments.

7.1 How to Conduct Threat Identification for Cyber-Physical System in Smart Buildings

Step 1: Define the Scope: Facility teams and cyber teams should begin by clearly defining the scope of the threat identification exercise for your Smart Building. Specify which smart buildings components will be analysed, including physical devices (such as sensors, controllers, and actuators), management software, and network connections that enable communication between building subsystems.

The following steps in this section apply equally to standalone CPS systems that operate independently of a BMS. For example, a connected lift can function as a standalone CPS when deployed independently. However, when the same lift is integrated with other systems such as a BMS, it becomes part of the broader smart building ecosystem.

Step 2: Identify Assets and Resources: Facility teams should identify and track all assets within the smart building with the characteristics like assets that collect or store data, possess control capabilities, or have network access. Cyber teams should assess if these assets are critical components requiring protection from threats. Examples include sensitive data repositories, physical devices such as sensors, actuators, controllers, and critical building infrastructure. Among these, the BMS serves as the central "brain," integrating multiple subsystems like HVAC, lighting, and security for centralised monitoring and control. It is important to clarify whether the BMS acts solely as a dashboard/reporting platform or also exercises direct control over edge devices, as systems with control capabilities pose greater security risks by enabling potential unauthorised manipulation of physical components such as HVAC, lighting, or security controls.

Methods of tracking assets could be through a Cyber-Physical Asset Form or any other suitable type of inventory management and tracker. The following example of an asset tracking form aims to serve as a reference template with suggested fields for comprehensive asset collection and tracking with cyber-physical considerations. Users should adapt this form to their specific context by adding relevant fields or removing unnecessary ones to meet their operational, security, and compliance requirements. By leveraging their operational knowledge, facility teams populate the Cyber-Physical Asset Form systematically to identify, document, and track every asset in the smart building that collects or stores data, has control capabilities, or possesses network access. Facility and Cyber Teams should regularly review and update asset lists as new devices are added or removed.

Cyber-Physical Asset Form		
Standard Asset Information (FM / Procurement to fill)		
Asset Inventory Field	**Description**	**Examples**
Asset ID	Unique identifier assigned to the asset	CPS-FireAlarm-001
Asset Name	Common or operational name	Main Fire Alarm Control Panel
Asset Type/Role	Specify type (e.g., sensor, actuator, PLC, controller, gateway)	Fire Alarm Controller
Manufacturer & Model	Vendor and model details	Honeywell Notifier Model XYZ
Serial Number	Device serial number	SN-123456789
Physical Location	Exact location within the building	Main Lobby, Floor 1
Software/Firmware Version	Current version of software or firmware	v3.2.1

Software/Firmware Hash	Allow verification of authenticity and integrity of Current version of software or firmware	e3b0c44298fc1c149 afbf4c8996fb92427a e41e4649b934ca495 991b7852b855
Last Patch/Update Date	Date of latest security update applied	2025-07-10
Hardware maintenance and maintenance interval	Maintenance Types: Preventive or Predictive, Interval of maintenance (e.g., quarterly, semi-annual, annual)	Preventive: semi-annual
Software maintenance and maintenance interval	Software Patching on software or firmware (e.g., quarterly, semi-annual, annual)	quarterly
Support Contact Information	Vendor support or service desk contacts	support@honeywell.com
Asset Owner	Person or team responsible for the asset	Facilities Team / IT Security Team
Asset Classification	Sensitivity or criticality classification (e.g., public, confidential)	Confidential
Asset Status	Operational lifecycle stage (e.g., active, retired, disposed)	Active
Cyber-Physical Considerations (FM and Cyber Team to fill)		
Has Network Access Capabilities	Does the device have network communication or access? (Yes/No)	Yes
Network Connectivity Details	If yes, what other devices, systems, or services can it connect to?	Building Management System, Emergency Services Network
Network Addressing	IP address and/or MAC address if applicable	IP: 10.10.20.30, MAC: 00:24:D7:89: 5F:1A
Communication Protocols	Protocols supported (e.g., BACnet, Modbus, MQTT, Ethernet)	Ethernet, proprietary Honeywell protocol
Data Collection Capability	Does this asset collect and/or store data? (Yes/No)	Yes, collect and store
Type of Data Collected	Specify the types of data collected (e.g., temperature, occupancy, video)	Fire alarms, system events, status logs
Impact of Data Loss	Describe the impact of losing this data	Loss would impair fire detection and safety alerts, risking occupant safety and compliance
Control Capability	Does this device have direct control over any physical process? (Yes/No)	Yes
Control Description	Describe what physical process(es) this asset controls	Controls fire alarm signalling, emergency evacuation alerts, Fire suppression activation.
Asset Criticality	How critical is the asset to operations/safety? (High/Med/Low)	High
Impact Assessment	Describe the potential impact if this asset malfunctions or is misused	Failure could delay fire detection, alarms and suppression, risking life

		safety and property damage
Known Vulnerabilities	Reference to known vulnerabilities, e.g., CVE IDs	CVE-2020-6972, CVE-2020-6974
Logging and Monitoring	Is the asset's activity logged and monitored? (Y/N)	Yes
Backup and Recovery	Backup frequency and method	Daily automated backups
User Access Controls	Who has access rights? List user groups or roles	Fire Safety Team, IT Security
Notes (CST)	Additional remarks or specific risk considerations	Recently tested for penetration vulnerabilities, patches applied to mitigate CVE-2020-6972 and CVE-2020-6974

Table 2: Cyber-Physical Asset Form

Step 3: Map out all the connected devices: After tracking all your assets, facility teams should map them out as part of an overall smart building diagram on how each CPS is connected or are standalone in your smart building.

Note: The following diagrams below are for illustrative purposes only and depicts an example of a poorly networked smart building. It does not represent all key categories or components of CPS and should not be construed as a comprehensive or accurate model. No liability is assumed for its use.

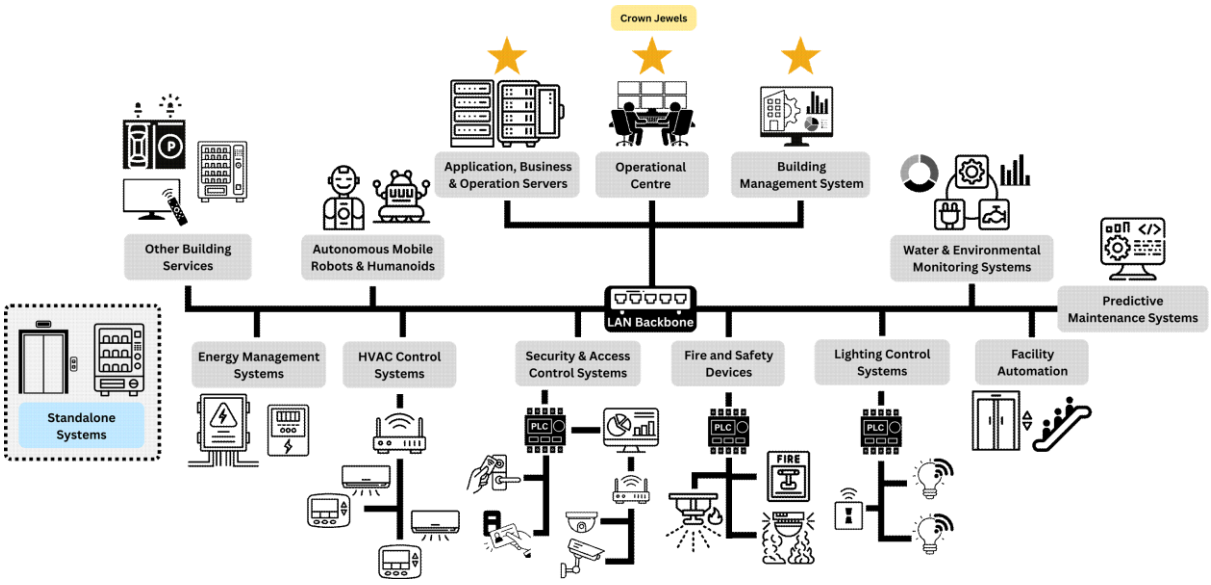

Figure 2: Network Diagram of Connected Devices

Step 4: Highlight Critical Assets and CPS: Facility and cyber teams should mark all critical assets (Crown Jewels) on your network diagram with a ★star. For systems that could have immediate impact to occupant safety should the systems malfunction, misused in a cyber-attack or breached, mark them with a symbol to ensure these areas receive extra attention and precaution during the threat identification process. Facility and cyber teams should also at this stage consider implementing network segregation and isolating systems to reduce lateral movement and remote attack risks where

feasible. It is highly recommended to prepare and update the Emergency Response Plans (ERPs) to handle cyber-physical situations for systems marked as such. [12][13]

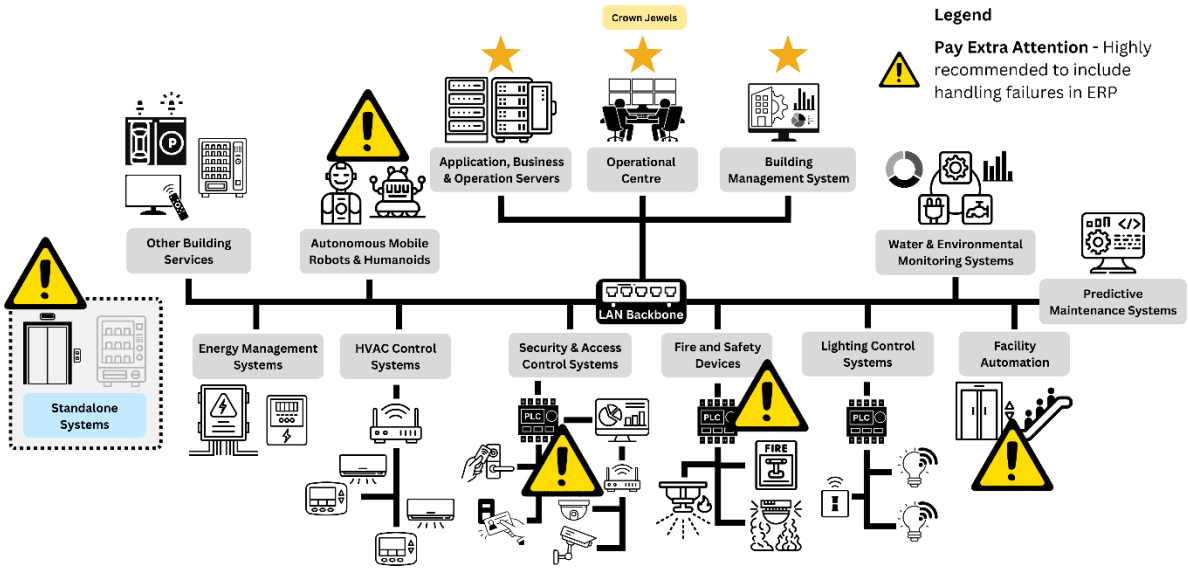

Figure 3: Network Diagram with Highlighted Critical Assets and CPS

Step 5: Analyse Potential Threats and Vulnerabilities: Cyber teams could apply threat modelling methodologies such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) or MITRE ATT&CK for Industrial Control Systems[20] (ICS) to systematically identify potential threats against each component of the smart buildings. This involves analysing possible attack vectors based on the operational use cases and referencing vulnerabilities in CVE databases [11]. By examining sensors, controllers, detection network interfaces, and management software, facility teams can uncover how attackers might exploit weaknesses in building operations and infrastructure.

An example of a STRIDE Analysis for Fire and Safety Systems

STRIDE Analysis for CPS	
Category: Fire and Safety Systems **Background:** **Honeywell Notifier fire alarm system had critical vulnerabilities CVE-2020-6972 (authorization bypass) and CVE-2020-6974 (information disclosure). The system's web server allows remote connection and control but has weaknesses that let attackers bypass authentication and access sensitive information like usernames and password hashes.**	
STRIDE Category	**Cyber-Physical Impact Analysis**
Spoofing: Faking identity to gain access.	Very Severe [19] - Spoofing can lead to false activation or suppression of physical fire alarms, affecting occupant safety directly.
Tampering: Unauthorized data or system modification.	Very Severe- Tampering with system data or controls can physically disable alarms or alter sensor readings, risking fire detection failure.
Repudiation: Denying actions performed.	Moderate - Without tamper-proof logs, physical incident accountability is compromised, indirectly affecting safety response and investigations.

Information Disclosure: Exposing sensitive information.	Moderate- Exposure can lead to loss of sensitive info information like usernames and password hashes but less immediate physical impact unless exploited for attack planning.
Denial of Service: Disrupting service availability.	Very Severe - Disruption of fire alarm systems can cause failure to alert occupants in emergencies.
Elevation of Privilege: Gaining unauthorized higher rights.	Very Severe - Unauthorised control escalation allows attackers to manipulate physical safety functions directly.

Summary of Analysis:
1)The Honeywell Notifier fire alarm system and associated modules (e.g., CPS-24 power supply) are CPS components critical for occupant safety.
2)STRIDE categories Spoofing, Tampering, Denial of Service, and Elevation of Privilege have a direct cyber-physical impact because they can manipulate physical safety functions or disable alarms. (Very Severe Impact)
3)Repudiation and Information Disclosure primarily affect system integrity and confidentiality, thus impacting safety more indirectly. (Moderate impact)
4)Priority will be given to resolve those of **Very Severe and Severe** impact, followed by those of Moderate impact.

Figure 4: STRIDE Analysis for CPS

Step 6: Develop Attack Paths: Cyber teams should construct attack paths that illustrate how an attacker could exploit identified vulnerabilities, especially learning from past real-world cases within the smart buildings. Visualising these attack paths provides a clear map of potential routes an adversary could take, showing how weaknesses in sensors, controllers, or network segments might be chained together to compromise critical building functions or data. This approach helps stakeholders understand the potential impact of various threats on smart buildings operations and prioritise mitigation efforts on the most critical vulnerabilities, chokepoints and uncover real attack paths as adversarial are creative and continuously evolving.

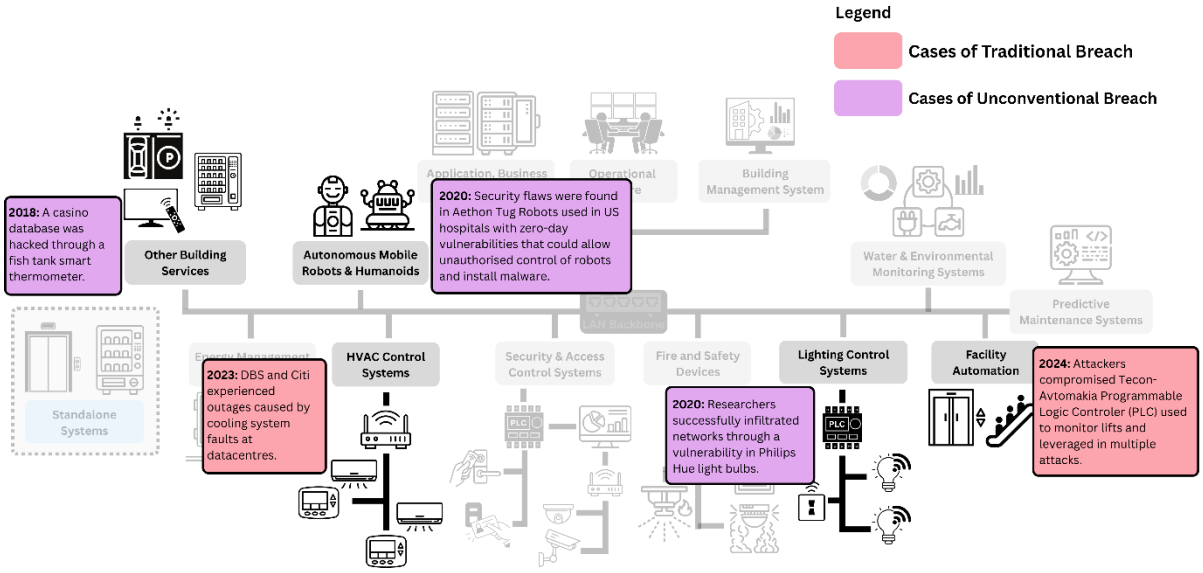

Figure 5: Real Work Cases of Traditional and Unconventional Breaches

The diagram above shows an example mapping of past real-world cases within the smart building context, cases of unconventional breaches show how smart devices or CPS can be exploited in cyber-attacks.

Next, the diagram below shows an example of an attack path being drawn, bringing attention to how unconventional cases where small and often overlooked smart devices like a light bulb could possibility be used in an attack to cause physical harm, disrupt operations, or stage larger attacks.

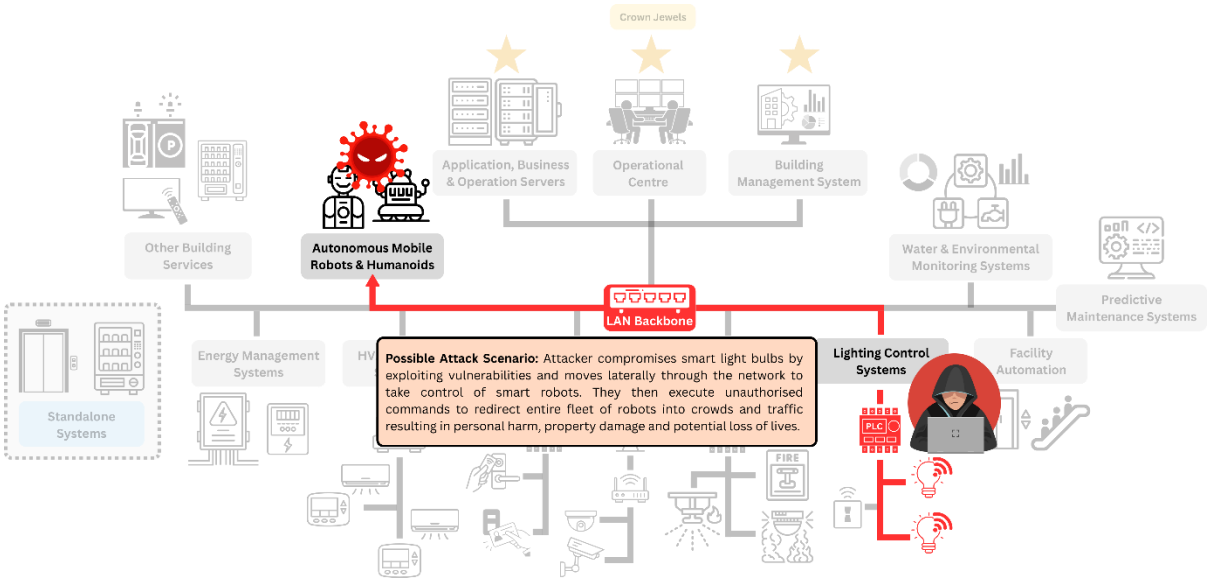

Figure 6: Network Diagram with Attack Path Example

Step 7: Build Threat Scenarios: Cyber teams should create realistic and detailed scenarios that show how various attackers such as cybercriminals, insiders, or nation-states might exploit vulnerabilities in smart building systems to disrupt operations, steal data, or cause damage. These narratives help stakeholders anticipate attacker methods and prioritise defences and incident responses effectively. The threat scenarios should cover details such as threat event, vulnerability, affected assets, consequences and possible impact. When conducting this step, organisations can also align with and refer to the CSA "Guide to Conducting Cybersecurity Risk Assessment for CII" [3], which provides a structured approach for developing such scenarios.

Examples of how to build threat scenarios are provided below. These examples are not exhaustive; it is only a subset of the actual assessment and are intended solely for illustration purposes. They should not be used as definitive threat models or relied upon in place of a full risk assessment tailored to your specific systems and operational environment.

Threat Scenario	STRIDE Threat Categories	Entry Point	Vulnerability	Affected Assets	Consequence	Impact	Key Mitigations	Real World Cases
Attacker takes control of fire and safety systems on an unpatched legacy web application to disable alarms, trigger false alarms, or manipulate sprinklers. Resulting in fire alarms not being triggered during a real fire hazard.	Spoofing, Tampering, Denial of Service, Elevation of Privilege, Lateral Movement	Network interfaces, wireless controls, operator consoles, physical access panels	Weak/absent authentication, unsecured network protocols, lack of encryption, default passwords, unpatched firmware/software	Fire alarms, sprinkler systems, emergency lighting, smoke detectors, control panels, building occupants	Systems failure or false activation causing delayed or inappropriate emergency responses; risk of fire damage, injury, or death	Very Severe — potential for loss of life, significant property damage, business interruption, regulatory penalties	1. Fail-safe defaults (alarms activate on failure) 2. Network isolation 3. Cryptographic integrity verification 4. Regular testing & drills 5. Secure communication channels 6. Continuous monitoring of sensors' health	Attacks on building fire alarm systems via compromised network devices have caused false fire alerts and delayed real response times (various documented ICS attacks)
Attacker takes control of robots via known software flaws and makes unauthorised actuations causing physical harm to nearby occupants.	Spoofing, Tampering, Elevation of Privilege, Lateral Movement	Robot control interface (e.g., network APIs, wireless comms, operator console)	Weak/absent authentication, insecure communication protocols, lack of access control, unpatched firmware/software	Robots, control systems, safety interlocks, human operators, production environment	Robot performs unsafe or malicious movements; physical harm to humans; damage to equipment; interruption of operations	Very Severe — injury, fatalities, regulatory/legal consequences	1. Cryptographic authentication of commands 2. Continuous activity & location monitoring 3. Geofencing and obstacle detection 4. Secure OTA updates 5. Physical safety protocols	Security flaws were found in Aethon Tug Robots used in US hospitals with zero-day vulnerabilities that could allow unauthorized control of robots and install malware [14]
Attacker exploits vulnerabilities in smart light bulbs or their controllers (e.g., Zigbee, Wi-Fi, Bluetooth) to gain a foothold on the building's IoT network and pivot into corporate IT/OT systems to exfiltrate data or disrupt the systems to cause physical harm.	Spoofing, Tampering, Information Disclosure, Elevation of Privilege, Lateral Movement	Smart light bulbs, IoT controllers/bridges, companion mobile apps, vendor cloud services	Insecure wireless protocols (Zigbee exploits, replay attacks), weak/default credentials, lack of encryption, poor firmware patching, overprivileged mobile/cloud APIs	Smart bulbs, IoT gateways, corporate/OT networks connected via shared infrastructure, user mobile devices	Initial compromise of lighting system leads to lateral movement into sensitive IT/OT networks; attacker can exfiltrate data, disrupt operations, or stage larger attacks	Minor — impacts depend on pivot depth: could be nuisance (lights flashing), but also a serious if breach reaches networks	1. Secure device authentication 2. Encrypted communication 3. Activity monitoring 4. Network segmentation 5. Physical security for controllers	Check Point "Lightbulb Attack" (2017): Security researchers hacked Philips Hue smart bulbs by exploiting a firmware flaw [18]

Table 3: Threat Scenario Examples

8. Assessing Effectiveness Of Controls For Cyber-Physical Systems

This section provides a practical guidance to help stakeholders identify and assess the most effective mitigation controls for CPS. The intent is to guide readers in understanding how to evaluate controls not only from a security perspective but also regarding safety, operational feasibility, and business impact. By applying the principles and structured approach outlined here, readers will gain clear methods to prioritise preventive measures, assess detection and response capabilities, and implement layered defences that are proportionate to the unique risks of different CPS categories. Ultimately, this section equips decision-makers with actionable steps to optimise control effectiveness, ensuring that cybersecurity strategies remain aligned with both safety-critical requirements.

8.1 Guiding principles

(These principles are translated into an actionable example in section 8.2)

1. Understand the Specific Risks and Impact of Each CPS Category

As per section 7.1, clearly defining the cyber and physical risks unique to the CPS category. For example, fire and safety systems pose immediate life-and-death risks if compromised, while energy management systems primarily present operational risks that could indirectly affect safety. Understanding the potential impact scope informs control prioritisation.

2. Evaluate the Control's Ability to Prevent the Risk

Ask the fundamental question: Can this control realistically reduce the likelihood of the threat from materialising?

Prevention/protection controls should be the top priority. These controls that block unauthorised access, such as strong multi-factor authentication or network segmentation, are often highly effective preventive/protective measures. Organisations may refer to the CSA "Guide to Conducting Cybersecurity Risk Assessment for CII", which provides a helpful likelihood matrix example to evaluate whether a control can effectively mitigate or reduce the chances of attack entry points.

3. Assess the Control's Capability to Detect and Respond

For risks that cannot be fully prevented, controls must effectively detect attacks or anomalies early to reduce the window of attack or anomaly exposure and enable rapid response or mitigation. This includes intrusion detection systems, real-time monitoring, logging, and alerting mechanisms. Controls should also allow for fail-safe or manual overrides to reduce harm during an incident.

4. Consider Control Feasibility and Operational Impact

The best control strikes a balance between effectiveness, operational feasibility, and appropriate risk acceptance. Overly complex measures that disrupt normal building functions or demand excessive resources can introduce new risks and hinder adoption. Each control should be evaluated to ensure it can be implemented without impeding critical operations or safety procedures. During a cyber incident, affected systems should be promptly isolated. If automated functions fail, facility teams must secure physical access and operate safety-critical systems offline to maintain operational continuity.

5. Layer Controls (Defence-in-Depth)

No single control is foolproof. Employ multiple controls across technical, procedural, and physical domains. For example, network segmentation combined with strong authentication and ongoing monitoring forms a layered defence, or a defence-in-depth approach, that significantly reduces risk.

6. Regularly Validate Control Effectiveness

Effectiveness assessment is not a one-time activity. With an ever-evolving threat landscape and new vulnerabilities announced daily, controls should be tested and validated regularly through vulnerability assessments, penetration testing, and drills. Evaluate if controls are properly configured, remain functional over time, and adapt to evolving threats.

7. Prioritise Controls Based on Business and Safety Impact

Allocate resources first to CPS categories where control failure would cause immediate and severe harm (e.g., Fire and Safety, Autonomous Robots). Lesser-impact systems can be controlled with appropriately scaled measures.

8.2 Example Approach based on the Guiding Principles

Step 1: List controls for each threat scenario (as prepared in Section 7.1 step 7).

Step 2: Evaluate controls for Prevention, Detection, and Recovery in reducing the threat per control, this will help identify which controls that are more effective and should be prioritised first.

- **Prevention/Protection**: Their capability to prevent threat exploitation. Example controls: (Access controls, firewalls, Multi-Factor Authentication (MFA), network segmentation, patch management)
- **Detection & Response**: Their ability to detect and respond rapidly to incidents. Example controls: (SIEM/SOC monitoring, intrusion detection systems (IDS/IPS), threat intelligence, EDR)
- **Recovery**: Their ability to recover and continue business operations. Example controls: (Data backups, disaster recovery plans, business continuity planning, redundancy systems)

Step 3: Prioritise strong prevention controls as CPSs directly impacts human safety and physically processes. Hence, preventing safety incidents is more critical in CPSs than in traditional ICT. No single control is foolproof. Employ multiple controls across technical, procedural, and physical domains to form a layered defence to lower risks.

How to Prioritise

- **First Line of Defence**: Invest in Prevention controls like Fail Safes, Access controls, firewalls, MFA and network segmentation to block common attack vectors.
- **Second Layer**: Enhance Detection & Response capabilities to reduce attacker dwell time and limit damage.
- **Final Safeguard**: Implement Recovery strategies to ensure operations can quickly resume when incidents occur.

Step 4: Continuously monitor and test controls by conducting periodic audits, penetration tests, and simulated scenarios to validate control effectiveness under realistic operational conditions. Testing

both technical and procedural controls can help identify weaknesses, ensures preparedness, and supports continuous improvement which are critical for safety-focused CPS environments.

Step 5: Adjust controls based on most up-to-date findings and evolving threats using test results, incident feedback, and threat intelligence to refine and update controls. Enhancements should be prioritised especially if they address gaps or new risks to maintain an adaptive, resilient defence aligned with current CPS operations and threats.

9. Periodic Review

The Smart building assessment is not a one-off exercise. Smart Building Operators and Stakeholders should regularly revisit sections 7 and 8 to keep the building safe, efficient and secure. Periodic reviews should be conducted at least once a year, and whenever there are major changes to the smart building's systems, usage, or connectivity (e.g. new BMS integration, Smart Lifts, Smart Lighting and Visitor Registration System). This ensures that previous assumptions remain valid, new risks are identified early, and the smart building continues to perform as intended over time.

10. CONCLUSION

As global cities advance their smart infrastructure, the integration of cyber-physical systems in smart buildings offers significant opportunities alongside emerging risks. Cyber-physical attacks that span digital and physical domains can disrupt operations, compromise safety, and impact occupant wellbeing. Facility teams thus become critical frontline defenders in safeguarding digitally integrated buildings, promoting secure, reliable, and efficient environments.

This guide equips facility teams and building operators with practical methods to understand, identify, and mitigate these risks within their environments. By blending foundational cybersecurity principles with building-specific considerations, this guide empowers non-specialists to take a proactive role in protecting smart infrastructure. Emphasizing layered defences prioritizing prevention, detection, and recovery, combined with continuous testing and adjustment, supports resilient operations aligned with evolving threats.

Together with established standards and collaborative partnerships, this guide helps ensure smart building ecosystems remain secure, resilient, and trusted, enhancing operational safety and continuity for all stakeholders.

11. REFERENCES

[1] The Wall Street Journal, "Cyber Attackers Target Building Management Systems" Available https://www.wsj.com/articles/BL-CIOB-1827

[2] Security Bulletin: KNX Systems Publicly Available Exploit, Apr, 2023, [Online]. Available: https://www.se.com/il/en/download/document/SESB-2023-01

[3] CSA publications on "Guide to conducting cybersecurity risk assessment for CII", "Guide to cyber threat modelling**"** https://www.csa.gov.sg/legislation/supplementary-references

[4] (NIST), National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," September 2012. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[5] (NIST), National Institute of Standards and Technology, "Cyber Security Framework 2.0," February 2024 [Online]. Available: https://www.nist.gov/cyberframework

[6] TR 111:2023 (ICS 35.020; 35.240.67) TECHNICAL REFERENCE Securing cyber-physical systems for buildings https://www.singaporestandardseshop.sg/Product/SSPdtDetail/98cf35ec-5e5b-4850-a0f5-04fa148aac29

[7] (IMDA) IMDA IoT Cyber Security Guide Annex C Version 1, Dec 2022 https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-IoT-Cyber-Security-Guide.pdf

[8] IEC 62443: the international standard for security in industrial control and automation systems https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[9] ISO/IEC standards: such as ISO/IEC 27001 for information security management and ISO/IEC 30141 (IoT Reference Architecture) https://www.iso.org/standard/27001 and https://www.iso.org/standard/88800.html

[10] Common Criteria (ISO/IEC 15408): providing an internationally recognised framework for evaluating the security of IT and operational products https://www.iso.org/standard/72891.html

[11] National Vulnerability Database https://nvd.nist.gov

[12] GUIDELINES FOR EMERGENCY RESPONSE PLAN (ERP): https://www.scdf.gov.sg/fire-safety-services-listing/emergency-response-plan

[13] Emergency Response Plan: https://www.ready.gov/business/emergency-plans/emergency-response-plan

[14] The New York Post: "Hospital robots face attacks by hackers after security flaws found" April 14, 2022[Online]. Available: https://nypost.com/2022/04/14/hospital-robots-face-attacks-by-hackers-after-security-flaws-found

[15] Elevator Hacking via PLC: How to Prevent It? 17 Feb 2025 [Online] Available: https://os.kaspersky.com/blog/elevator-exploit

[16] DBS, Citi outages caused by cooling system 'technical issue' at data centre Oct 14, 2023 [Online]. Available: https://www.channelnewsasia.com/singapore/dbs-citibank-service-outage-data-centre-cooling-system-issue-equinix-redone-mobile-3849346

[17] Criminals Hacked A Fish Tank To Steal Data From A Casino Jul 27 2017 [Online] Available: https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino

[18] Researchers Use Smart Light Bulbs to Infiltrate Networks Feb 06 2020 [Online] Available: https://www.trendmicro.com/vinfo/sg/security/news/cybercrime-and-digital-threats/researchers-use-smart-light-bulbs-to-infiltrate-networks

[19] NIST Safety Commission Report https://www.nist.gov/director/nist-safety-commission/nist-safety-commission-reports

[20] MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy

https://www.google.com/search?q=or+MITRE+ATT%26CK+for+Industrial+Control+Systems+(ICS)+to&oq=or+MITRE+ATT%26CK+for+Industrial+Control+Systems+(ICS)+to&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzIwM2owajeoAgCwAgA&sourceid=chrome&ie=UTF-8