Building and Construction Authority

An MND Statutory Board

MINISTRY OF DIGITAL DEVELOPMENT AND INFORMATION

Our Ref: BCA\EMEG\GEN\2025\015 Electrical and Mechanical Engineering Group

26 September 2025

See Distribution List

Dear Sir/Madam

CIRCULAR ON THE CYBERSECURITY AND INTEROPERABILITY GUIDELINES FOR CONNECTED LIFT SYSTEMS

- With inputs from GovTech and CSA

This circular informs agencies on the cybersecurity and interoperability compliance standards for the use of Connected Lift systems.

Background

2 Connected Lift systems refer to lifts that are equipped with digital technologies and IoT capabilities, enabling them to communicate with external systems and via network connections[1]. These systems provide near real-time data collection, monitoring, and analytics to improve lift performance, safety, and maintenance.

3 The government recognises the growing cyber-risks associated with the increasingly digital and interconnected nature of Connected Lift systems. These lift systems can be vulnerable to cyber-attacks if not properly secured. Such risks pose public safety concerns as successful attacks could affect lift operations such as overriding emergency protocols, forcing doors to stay open or stalling lifts – potentially trapping users or delaying emergency response.

4 Currently, there are limited prescribed standards or guidelines for Operational Technology (OT) systems[2] like Connected Lift systems, across both industry and the public sector. As a result, agencies and vendors adopt different system setups and configurations, leading to inconsistent approaches to component integration, cybersecurity measures and the type of remote monitoring and diagnostics (RM&D) solutions used.

[1] Features include Remote Monitoring & Diagnostics (RM&D) solutions, safe remote interventions, and/or interfacing with Building Management System (BMS) or Autonomous Mobile Robots (AMRs).

[2] OT systems refer to an arrangement of interconnected computers that is used in the monitoring and/or control of physical processes, that includes: (a) supervisory control and data acquisition systems, distributed control systems, and other control system configuration such as programme logic controllers; (b) a combination of control components, e.g. electrical, mechanical, hydraulic, and pneumatic, that act together to achieve an industrial objective, e.g. manufacturing, transportation of matter, or energy.

5 This fragmented landscape presents several challenges. Agencies and vendors often adopt different configurations and standards, resulting in inconsistent levels of cybersecurity assurance. The absence of common protocols and interfaces also hinders the ability to monitor and respond to threats effectively, weakening situational awareness and slowing incident response. Additionally, the lack of standardisation makes it difficult to scale trusted solutions across estates, leading to high integration costs, duplicated efforts, and operational inefficiencies.

6 To address these issues, the government intends to:

a) Promote interoperability and common technical baselines across Connected Lift systems to reduce complexity, improve coordination, and support secure-by-design deployments.

b) Standardise minimum cybersecurity and system integration requirements, particularly for public sector procurements, to ensure greater consistency and uplift overall security levels.

7 The public sector will take the lead as a first mover, before encouraging broader industry adoption of secure and interoperable solutions.

Compliance Standards for Connected Lift systems

8 This circular stipulates that all Connected Lift systems are to comply with the following standards to prevent unauthorised access, monitoring and control[3].

a) Cybersecurity standards: "TR111:2023 – Securing cyber-physical systems for buildings" and "ISO8102-20:2022 – Electrical requirements for lifts, escalators and moving walks (Part 20: Cybersecurity)"[4] [5].

b) Interoperability standards: "SS 713:2025 – Data exchange between robots, lifts and automated doorways to enable autonomous operations".

9 Connected Lift systems should also ensure that:

a) Systems that allow remote interventions (e.g. remote calling and resetting) for troubleshooting should ensure that these functions do not compromise lift safety by interfering, overriding or bypassing safety systems and controllers.

b) Data transmitted must be secure and encrypted, ensuring it does not contain any WOG or CII data. The data schema for lifts should ensure that lift locations, Permit to Operate (PTO) IDs, and other sensitive information are not captured, to minimize the potential impact in the event of data breach.

[3] Especially systems connected to Critical Information Infrastructure (CII).

[4] ISO8102-20 is preferred over IEC 62443 as it is the latest international standard for lifts, escalators and moving walks.

[5] TR111:2023 clause 7.8.3 states that lift product developers and system developers should adopt best practices from existing standards and guidelines, such as ISO8102-20:2022.

Security Design for Connected Lift Systems

10 Agencies implementing Connected Lift systems are to comply with the default security design to ensure basic cybersecurity hygiene and safeguard against common threats. Where such systems are implemented in more critical or sensitive sites, agencies should adopt enhanced security measures as necessary. Design setups and key considerations for both default and critical infrastructure contexts are detailed in **Annex A**.

Applicability of Instruction Manual for ICT&SS (IM8)

11 MDDI is conducting a review of cybersecurity policy requirements for cyber-physical systems (CPS) in Smart Buildings, including Connected Lifts. Pending this review, Agencies are to reference the standards in paragraph 8(a) for OT specific requirements for Connected Lift and ensure that appropriate controls are implemented to mitigate identified risks.

Clarification

12 Please direct your queries to https://www.bca.gov.sg/feedbackform/ for any clarifications. Thank you.

Yours Faithfully

TEO ORH HAI
GROUP DIRECTOR
ELECTRICAL AND MECHANICAL ENGINEERING GROUP
INVESTIGATION AND ENFORCEMENT DEPARTMENT
BUILDING AND CONSTRUCTION AUTHORITY

JOEL CHUA
DIRECTOR
SMART CITY DIVISION
MINISTRY OF DIGITAL DEVELOPMENT AND INFORMATION

Annex A: Recommended Security Design for Connected Lift systems

	Default	Critical Infrastructure (CI)
Design setup	2 Next-Gen Firewalls (NGFWs) (1 perimeter, 1 OT firewall) a. Public edge pulls data from cloud b. Private edge pulls data from public edge	1 NGFW, 2 data diodes to facilitate data transfer to and from "internal" and "external" networks a. Public edge pulls data from cloud b. Private edge pulls data from public edge
Security consideration	Lower security assurance – NGFW functionally allows bidirectional data transfer, misconfiguration/ software vulnerabilities can cause data leak from control system. NGFW stateful inspection can be used to enforce design, to only allow connections initiated from private edge.	Higher security assurance – data diode enforces very strict separate data flow. However, there is still means for traffic out of control system that may leak sensitive data. Monitoring required to detect and prevent data leaks.
Operational consideration	Maintain minimally 2x key components, e.g. edge and firewall software and signature	Maintain minimally 3x key components, e.g. edge and 2x diodes software/configuration
Cost efficacy	Lower cost	Higher cost

CIRCULAR DISTRIBUTION LIST (via e-mail)

DISTRIBUTION LIST

Director of Infrastructure
School Campus Department
Ministry of Education (MOE)
1 North Buona Vista Drive
Singapore 138675

Chief Civil & Structural Engineer
Building & Infrastructure Group
Housing & Development Board (HDB)
HDB Hub
480 Lorong 6 Toa Payoh
Singapore 310480

Deputy Chief Executive
Infrastructure & Development
Land Transport Authority (LTA)
1 Hamphire Road
Block 8 Level 1
Singapore 219428

Director
Technical Services Division
JTC Corporation (JTC)
8 Jurong Town Hall Road
The JTC Summit
Singapore 609434

Senior Director
Building & Estates Management
People's Association (PA)
9 King George's Avenue
Singapore 208581

Chief Executive
PUB, Singapore's National Water Agency
40 Scotts Road #08-01
Environment Building
Singapore 228231

Chief
Sport Infrastructure Group
Sport Singapore (SportSG)
3 Stadium Drive
Singapore 397630

Assistant Chief Executive & Chief Sustainability Officer
Policy & Planning Group
Singapore Tourism Board (STB)
1 Orchard Spring Lane
Tourism Court
Singapore 247729

Chief Executive Officer
Urban Redevelopment Authority (URA)
45 Maxwell Road, The URA Centre
Singapore 069118

Director
Building and Infrastructure
Defence Science & Technology Agency (DSTA)
1 Depot Road
Defence Technology Tower A
Singapore 109679

Head
Fire Safety and Building Control
Building and Infrastructure
Defence Science & Technology Agency (DSTA)
71 Science Park Drive
Singapore 118253

Manager
Architectural Plans
Building and Infrastructure
Defence Science & Technology Agency (DSTA)
71 Science Park Drive
Singapore 118253

Deputy Chief Executive Officer
Sentosa Development Corporation (SDC)
33 Allenbrooke Road, Sentosa
Singapore 099981

Chief
Health Infrastructure Project
MOH Holdings Pte Ltd
1 Maritime Square #11-25
HarbourFront Centre
Singapore 099253

Director
Smart City Technology Division
Government Technology Agency (GovTech)
10 Pasir Panjang Rd, #10-01
Mapletree Business City
Singapore 117438

Director
Critical Information Infrastructure
Cyber Security Agency (CSA)
5 Maxwell Road Level 3, Tower Block
MND Complex
Singapore 069110