**TR 111:2023**
(ICS 35.020; 35.240.67)

TECHNICAL REFERENCE

# Securing cyber-physical systems for buildings

Singapore Standards Council

**TR 111:2023**
(ICS 35.020; 35.240.67)

TECHNICAL REFERENCE

# Securing cyber-physical systems for buildings

Published by Enterprise Singapore

ISBN 978-981-5118-71-1

## Contents

Page

**Tables**

**Figures**

## Foreword

This Technical Reference (TR) was prepared by the Working Group on Securing Cyber-physical Systems for Buildings set up by the Technical Committee on Building Maintenance and Management under the purview of the Building and Construction Standards Committee (BCSC).

Modern smart buildings incorporate autonomous building automation systems that manage occupant comfort and safety. These systems are complex and distributed, and may include predictive and automated functions that affect many different areas in a building. For example, setting room temperature, lighting controls, controlling access to different spaces within the building, and even connecting to systems of other buildings in the same cluster. Due to the integration of various building subsystems, the entire system can be vulnerable to cyber attacks if not adequately secured.

This TR is a provisional standard made available for application over a period of three years. The aim is to use the experience gained to update the TR so that it can be adopted as a Singapore Standard. Users of the TR are invited to provide feedback on its technical content, clarity and ease of use. Feedback can be submitted using the form provided in the TR. At the end of the three years, the TR will be reviewed, taking into account any feedback or other considerations, to further its development into a Singapore Standard if found suitable.

It is presupposed that in the course of their work, users will comply with all relevant regulatory and statutory requirements. Some examples of relevant regulations and acts are listed in the Bibliography. The Singapore Standards Council and Enterprise Singapore shall not be responsible for identifying all of such legal obligations.

Attention is drawn to the possibility that some of the elements of this TR may be the subject of patent rights. Enterprise Singapore shall not be held responsible for identifying any or all of such patent rights.

**NOTE**

1. *Singapore Standards (SSs) and Technical References (TRs) are reviewed periodically to keep abreast of technical changes, technological developments and industry practices. The changes are documented through the issue of either amendments or revisions. Where SSs are deemed to be stable, i.e. no foreseeable changes in them, they will be classified as “mature standards”. Mature standards will not be subject to further review unless there are requests to review such standards.*

2. *An SS or TR is voluntary in nature except when it is made mandatory by a regulatory authority. It can also be cited in contracts making its application a business necessity. Users are advised to assess and determine whether the SS or TR is suitable for their intended use or purpose. If required, they should refer to the relevant professionals or experts for advice on the use of the document. Enterprise Singapore and the Singapore Standards Council shall not be liable for any damages whether directly or indirectly suffered by anyone or any organisation as a result of the use of any SS or TR. Although care has been taken to draft this standard, users are also advised to ensure that they apply the information after due diligence.*

3. *Compliance with a SS or TR does not exempt users from any legal obligations.*

# Securing cyber-physical systems for buildings

## 0 Introduction

Building operations are increasingly being driven by digital processes or aided by digital technology. Traditional building management functions in building management or building automation systems are now being supported by systems driven by software and are connected via the Internet. These improvements in building operations also introduce a range of new threats as building systems are built on operational technology (OT) that may not have been designed with information technology (IT) security capabilities in mind.

While it may be tempting to simply transfer IT cyber security measures and practices to cyber physical systems, this does not take requirements and constraints imposed by activities that occur in the physical realm into account. Mitigation measures that work in cyber-only systems may inadvertently cause problems in the operations of cyber-physical systems. And cyber-only measures do not account for physical vulnerabilities. Hence, there is a need for a set of best practices specific to ensuring that the physical assets and operations of a building are not threatened by either cyber and/or physical attacks.

## 1 Scope

This Technical Reference (TR) covers various factors which impact the cyber security of buildings and facilities. The TR also includes asset management (software, computer equipment and automation system), physical and environmental security (card control, fire door, intruder detection system and access), and access control (user access management, network access control, operating system access control and log-in procedures).

## 2 Normative references

The following referenced documents are indispensable for the application of this TR. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

| | |
|---|---|
| IEC 62443-3-3 | Industrial communication networks - Network and system security – Part 3–3: System security requirements and security levels |
| IEC 62443-4-1 | Security for industrial automation and control systems – Part 4–1: Secure product development lifecycle requirements |
| IEC 62443-4-2 | Security for industrial automation and control systems – Part 4–2: Technical security requirements for IACS components |