TECHNICAL CODE

INTERNET OF THINGS – FUNCTIONAL SAFETY REQUIREMENTS

Developed by

Registered by

Registered date: 4 August 2026

© Copyright 2026

MCMC MTSFB TC G058:2026

Development of technical codes

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) ('the Act') provides for a Technical Standards Forum designated under Section 184 of the Act for the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to Section 185 of the Act shall consist of, at least, the requirements for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with Section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by Section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under Section 185 of the Act.

A technical code prepared in accordance with Section 185 shall not be effective until it is registered by the Commission pursuant to Section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8688 8000
Fax : +60 3 8688 1000
Email : stpd@mcmc.gov.my
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

Page

Committee representation ii
Foreword iii
Introduction 1

1. Scope 1
2. Normative references 1
3. Abbreviations 1
4. Terms and definitions 2
5. Functional safety overview 5
   - 5.1 Functional safety for Internet of Things (IoT) system 5
   - 5.2 Functional safety standards 5
   - 5.3 AI IoT (AIoT) functional safety 6
   - 5.4 Challenges in implementing functional safety 6
6. Functional safety principles 7
   - 6.1 Monitoring and control 7
   - 6.2 Fault detection, diagnostics and response 7
   - 6.3 Redundancy configuration 7
   - 6.4 Fail-safe mechanism 7
   - 6.5 Environmental hardened design 7
   - 6.6 Software security 7
   - 6.7 Communications security 8
   - 6.8 Systematic fault prevention and mitigation 8
7. Functional safety lifecycle for Internet of Things (IoT) system 9
   - 7.1 Phase 1: Hazard and risk assessment 9
   - 7.2 Phase 2: Functional safety specification 10
   - 7.3 Phase 3: Design and development 10
   - 7.4 Phase 4: Verification and Validation (V&V) and certification 11
   - 7.5 Phase 5: Operation 12
   - 7.6 Phase 6: Decommissioning and disposal 13

Annex A Normative references 14
Annex B Functional safety use case: Smart traffic light 16
Annex C Functional safety use cases (Industrial) 20
Annex D Internet of Things (IoT) functional safety and security 23
Bibliography 24

Committee representation

This technical code was developed by Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

CyberSecurity Malaysia

International Islamic University Malaysia

Maxis Broadband Sdn Bhd

SIRIM Berhad

Smart Tech Asia Pacific Sdn Bhd

Universiti Kuala Lumpur

Universiti Teknologi MARA

Universiti Tun Hussein Onn Malaysia

Foreword

This technical code for Internet of Things (IoT) – Functional Safety Requirements ('Technical Code') was developed pursuant to Section 185 of the Act by the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB).

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

MCMC MTSFB TC G058:2026

INTERNET OF THINGS – FUNCTIONAL SAFETY REQUIREMENTS

Introduction

The Internet of Things (IoT) has revolutionised the way we live and work, connecting devices to the internet and creating vast networks of data exchange and automation. IoT is transforming and improving efficiency, security, safety, and reliability, from smart homes and industrial systems to healthcare and transportation, However, the rising connectivity and complexity of IoT system introduce new challenges for the IoT systems to function safely on demand. This includes ensuring reliability of safety-critical functions to mitigate risks that could compromise safety for examples communication delays and interoperability across multi-vendor system. Integration of previously isolated applications necessitates interdisciplinary expertise to ensure system safety and reliability.

Technology maturity will provide the path for safe usage of IoT system. For IoT technology to be effectively and safely exploited, it is the responsibility of the organisation to ensure the functional safety lifecycle is implemented in IoT systems.

This Technical Code shall be read together with the following Technical Codes support a full understanding of the applicable requirements.

a) MCMC MTSFB TC G013, Internet of Things (IoT) - Security Management

b) MCMC MTSFB TC G015, Information and Network Security – Incident Management

c) MCMC MTSFB TC G031, Internet of Things – Application Security Requirements

d) MCMC MTSFB TC G045, Internet of Things – Device Security Requirements

1. Scope

This Technical Code establishes functional safety requirements for IoT systems. It specifies standard practices applicable to organisations to ensure the safety of people, assets, and the environment.

In addition, this Technical Code emphasises a systematic approach in identifying and mitigating risks associated with IoT system functional safety lifecycle to ensure efficient, secure, safe, and reliable design, development, deployment, operation, maintenance, and decommissioning of IoT System applicable to any organisations where safety is critical.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

Refer Annex A.

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

ADAS	Advanced Driver Assistance Systems
AI	Artificial Intelligence
ALARP	As Low as Reasonably Practicable

ASIL	Automotive Safety Integrity Levels
CMI	Communication and Multimedia Industry
E/E/PE	Electrical, Electronic, or Programmable Electronic
HAZOP	Hazard and Operability
IEC	International Electrotechnical Commission
ICT	Information and Communication Technology
IoT	Internet of Things
LIDAR	Light Detection and Ranging
OTA	Over-The-Air
SCADA	Supervisory Control and Data Acquisition
SIL	Safety Integrity Levels
SOP	Standard Operating Procedure
V&V	Validation and Verification
XAI	Explainable AI

4. Terms and definitions

For the purposes of this Technical Code, the following definitions apply.

4.1 Artificial Intelligence (AI)

A machine or computer system's ability to perform tasks that would typically require human intelligence. It involves programming systems to analyse data, learn from experiences, and make smart decisions guided by human input. In IoT systems, AI analyses data from devices, makes smart decisions, and automates actions to improve efficiency and safety.

4.2 AI IoT system

An IoT system that uses AI to process data from connected devices, enabling real-time analysis, predictive maintenance, and automated decision-making to enhance safety and performance.

4.3 Automotive Safety Integrity Level (ASIL)

A classification system used to assess the risks associated with safety functions in vehicles. ASIL helps determine how much risk reduction is needed for different car features (i.e. ASIL A, ASIL B, ASIL C, ASIL D), with higher levels (ASIL D) indicating greater safety requirements. This ensures that safety-related systems in vehicles are designed and tested according to the potential harm they could prevent, making cars safer for everyone.

4.4 Certification

Formal process by an independent, accredited third party who assesses and verifies that an IoT system, product, process, or service complies with the defined requirements. This process provides assurance to users and stakeholders that the IoT solution meets established safety, security, and performance standards.

4.5 Communication security

The practices, technologies, and policies to ensure communications between devices, systems, and controllers are reliable, secure, and fail-safe when used within an IoT system or other functional safety applications.

4.6 Failure on demand

The inability of a safety function to respond correctly and successfully during presence of a hazardous situation or event.

4.7 Functional safety

Addresses the safety-related aspect to how a system functions and ensures that it operates correctly and safely, even when faults occur. Functional safety identifies potentially dangerous conditions, situations, or events to enable corrective or preventive actions to avoid or reduce the impact of an accident and incident.

4.8 Functional safety lifecycle

A structured process for ensuring functional safety of the IoT systems. It defines the necessary phases, activities, and safety requirements throughout the entire life of the IoT system, from concept to decommissioning.

4.9 Internet of Things (IoT)

Infrastructure of interconnected objects, people, systems, and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react. IoT provides a global infrastructure of the information society, enabling advanced services by interconnecting the physical and virtual things on existing and evolving, interoperable ICT. Industrial Internet of Things (IIoT) is a subset of IoT focused specifically on industrial environments.

4.10 IoT device

A device with capabilities of communicating, sensing, actuation, data capture, data storage and data processing. IoT devices are generally able to sense, affect and interact with the physical world and cannot be accessed, managed, or monitored without the physical control interfaces. IoT devices also generally lack in security, privacy, and functional safety attributes.

4.11 IoT functional safety

A set of actions, mechanisms, or processes embedded within an IoT system that are specifically designed to ensure the safety of the people, assets, and environment. The application of IoT functional safety is to ensure that IoT system respond correctly to inputs and safely handle faults to prevent hazards.

4.12 IoT security

The practices, technologies, and policies designed to protect the IoT system, and its communication networks to ensure the confidentiality, integrity, and availability of data, services, and resources. The goals are to safeguard data and to ensure operational continuity, preventing unauthorised access to critical infrastructure, and mitigating threats such as ransomware that exploit vulnerable IoT system. IoT security addresses unique challenges like device heterogeneity, limited computational power, and the convergence of physical and virtual risks.

4.13 IoT software

It is a multi-layered, distributed system of programs and protocols that enables the entire lifecycle of an IoT system. This encompasses the embedded firmware on physical devices for sensing and actuation, the software on edge gateways for data aggregation and protocol translation, and the central IoT platform software, or middleware, which provides device management, data processing, security, and application enablement.

4.14 IoT system

A system that enables IoT devices and associated hardware to connect to the internet or communicate over networks, facilitating data collection, exchange, and analysis to achieve specific functionalities or goals. It encompasses a wide range of components including sensors, actuators, connectivity protocols, cloud platforms, and applications, working together to provide connected intelligent solutions for various domains like smart homes, industrial automation, healthcare, and smart cities.

4.15 Organisation

Manufacturer, service provider and/or end-user that designs, installs, and/or operates IoT system with functional safety.

4.16 Random failure

A failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the IoT system.

4.17 Safety Integrity Level (SIL)

It is a way to describe how reliable a safety system needs to be in order to prevent serious harm when something goes wrong. The safety integrity level has four level: SIL 1, SIL 2, SIL 3 and SIL 4 where SIL 4 is the highest integrity level based on IEC 61508. SIL is a measure of required risk reduction, expressed through PFD_{avg} (Probability of Failure on Demand or PFH (Probability of Dangerous Failure per Hour).

4.18 Spurious failure

A safe failure that causes the safety system to unnecessarily shut down or activate protective actions, even though there is no actual presence of hazardous condition.

4.19 Systematic failure

A failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.

4.20 Success on demand

A situation where a safety-related system is activated only in response to a specific demand, such as an emergency or fault condition, and is required to perform its intended safety function successfully at that time.

4.21 Validation and Verification (V&V)

An independent processes and procedures that are used to validate and verify IoT system to meet and comply with IoT functional safety standards, requirements, and specifications by first or second party or independent third party.

5. Functional safety overview

Functional safety aims to mitigate risks from system malfunctions or failures, ensuring the system operates as intended without causing harm. It encompasses measures and processes that detect potentially dangerous conditions and trigger protective actions, thereby reducing the likelihood and impact of hazardous events.

5.1 Functional safety for Internet of Things (IoT) system

As the application of the IoT system extends beyond the existing monitoring and control functions, the need for functional safety in designing and operating IoT system is critically required. Functional safety focuses on the aspect of safety in IoT system that perform as intended to avoid hazardous situations causing harm to people, assets, and environment due to malfunction, and incorrect or misuse of operation. An example of a functional safety feature in IoT is automatically stopping the motor using motor control devices on robotics or machines to avoid hazards.

The differences between IoT functional safety and security are further explained in Annex D.

5.2 Functional safety standards

The IEC 61508 is the foundational standard for functional safety which provides guidance on Electrical, Electronic, or Programmable Electronic (E/E/PE) systems to be reliable and safe in a critical environment across industries.

Figure 1 below shows the IEC 61508, ITU-T Y.4806 and the relevant industry specific safety standards to ensure that potential hazards are identified, and adequate safety measures are implemented. The standards provide the following.

a) Outlines functional safety requirements throughout the lifecycle of electrical, electronic, or programmable electronic (E/E/PE) systems and products.

b) Adopts a rigorous, quantitative approach to risk reduction that is applicable across a wide range of industries.

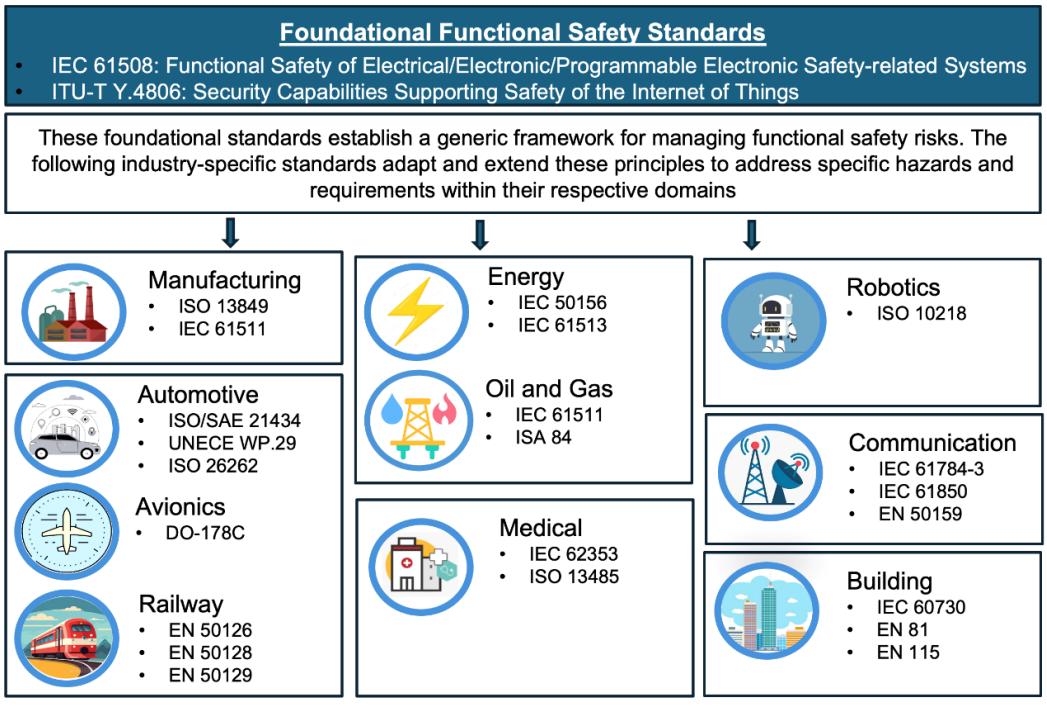

Figure 1. Foundational and Industry-Specific Functional Safety standards

5.2.1 IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

The IEC 61508 standard applies to systems or devices that perform automated safety functions, including components such as sensors, control logic, actuators, and microprocessors. A product, process, or system certified as compliant with IEC 61508 demonstrates conformance with all prescribed safety requirements.

5.2.2 ITU-T Y.4806, Security capabilities supporting safety of the Internet of Things

ITU-T Y.4806 is published by the International Telecommunication Union (ITU-T). It defines a framework of security capabilities such as authentication, access control, secure communication, and fault detection that are necessary to support safety in IoT system, particularly in environments where failure or compromise could cause physical harm.

This standard relates to IoT functional safety by emphasising that security is a prerequisite for safety in an IoT system. Since IoT devices are often exposed to cyber threats, a compromised device can lead to unsafe conditions. Therefore, the security measures outlined in ITU-T Y.4806 help ensure that IoT-based safety functions remain reliable and resilient.

5.3 AI IoT (AIoT) functional safety

An AI IoT (AIoT) system uses AI to process data from connected devices, enabling real-time analysis, predictive maintenance, and automated decision-making to enhance safety and performance.

AIoT functional safety is to further reduce risks of failure on demand. Safety-critical AIoT systems shall follow a documented functional safety lifecycle integrating NIST AI Risk Management Framework and IEC 61508.

5.4 Challenges in implementing functional safety

As IoT system become more complex with more connected devices, proper functional safety measures are needed. For example, the autonomous driving challenge will lead to a more dynamic environment from a safety perspective. The rapid growth of AI and data collection through the cloud increases the need for safety-critical software updates.

The implementation of functional safety has several challenges as discussed in Table 1 below, which should be considered and mitigated as described in Phase 1 of section 6.

Table 1. Challenges in implementing functional safety

No	Challenges	Description
1	System complexity	IoT system combines hardware, software, and network, making it hard to ensure safety and reliability.
2	Interoperability	Devices from different manufacturers may not follow the same safety standards, making integration difficult.
3	Data integrity and privacy	Large data volumes require accuracy. Data loss or tampering can lead to unsafe actions.
4	Real-time requirements	Some applications require fast response. Delays or errors can be dangerous.
5	Regulatory challenges	The absence of a dedicated framework, low industry readiness and adoption, limited local testing capacity and the need for alignment with international standards.

Table 1. Challenges in implementing functional safety (*continued*)

No	Challenges	Description
6	High infrastructure cost	Safety systems require certified hardware, tools, expertise, testing, and maintenance making them less affordable.
7	Scalability	As systems grow, maintaining functional safety and re-certifying components becomes harder, especially with varied vendors.

6. Functional safety principles

Functional safety is about reducing the risks of simple and complex systems that safely operate and function in the event there is any malfunction that can be caused by either random failures or systematic failures. The functional safety principles for IoT systems incorporate various safety functions and mechanisms to detect and automatically mitigate hazards to ensure secure and safe operation.

The organisation shall ensure the following principles are applied in the IoT system.

6.1 Monitoring and control

IoT system shall continuously monitor safety-related parameters and should control parameters to respond and mitigate the risks immediately. Refer to Annex B and Annex C.4 for example.

6.2 Fault detection, diagnostics and response

The IoT system shall have fault detection features, which is a critical component of IoT functional safety that identifies hardware, software, or network failures. It monitors the IoT system logs, health monitoring tools and diagnostics logs of abnormal behaviour before any potential failures and triggers predefined responses to prevent accidents or incidents. Refer to Annex C.3 for example.

6.3 Redundancy configuration

The IoT system shall have redundancy configuration by deploying duplicate systems, components, or pathways to maintain critical functionality to address random failures. Refer to Annex C.4 for example.

6.4 Fail-safe mechanism

The IoT system shall have fail-safe mechanisms to ensure that when a system or components fails, it does so in a predictable manner that avoids creating hazards. Fail-safe design shall be considered in both hardware and software architecture. Refer to Annex C.3 for example.

6.5 Environmental hardened design

IoT system shall be designed to be physically secured and resistant to environmental challenges such as heat, radiation, water ingress, vibration and physical tampering. Refer to Annex C.1 for example.

6.6 Software security

IoT system shall be designed with software security features to prevent malfunctions that could cause harm or damage. This includes safeguarding against cyberattacks, data breaches, and operational failures that could lead to unintended consequences.

Software security features shall include the following.

a) Secure coding practices

b) Task isolation for critical vs. non-critical functions

c) Real-time constraint adherence

d) Comprehensive error handling

e) Strong authentication

f) Secure network connections

g) Encryption of data in transit and at rest

6.7 Communication security

IoT system shall be designed with communication security features to secure the transmission of data to avoid manipulation, falsification or loss of information during transmission or processing. In the case of the IoT system is on TCP/IP stack, IPv6 should be recommended as it enhances security features and larger address space, to ensure secure and efficient data exchange. The communication security features shall protect from tampering, ensure authenticity, and maintain the trustworthiness of data used in functional safety.

Communications security shall involve a multi-layered approach such as the following.

a) Secure data transmission through encryption

b) Secure protocols

c) Message integrity

d) Timeout/retransmission mechanisms

e) Robust authentication and authorisation mechanisms

f) Regular monitoring and maintenance to address vulnerabilities

g) Consideration of physical security measures to protect devices

The IoT systems shall be designed in compliance with MCMC MTSFB TC G044 and MCMC MTSFB TC G045.

6.8 Systematic fault prevention and mitigation

IoT system shall be designed to address systematic failures which are caused by design flaws, process inadequacies, software bugs, configuration errors, or human mistakes and shall be corrected by considering any of the following.

a) Applying the functional safety lifecycle

b) Using proven and certified devices and systems

c) Independent safety assessments

d) Train and certify personnel in safety-related field

e) Diverse technology to address common mode failure

Refer to IEC 61508 for further details and Annex C for example.

7. Functional safety lifecycle for Internet of Things (IoT) system

Organisations should apply the IoT system functional safety lifecycle to manage its associated safety risks. Figure 2 illustrates the six (6) phases of the functional safety lifecycle.

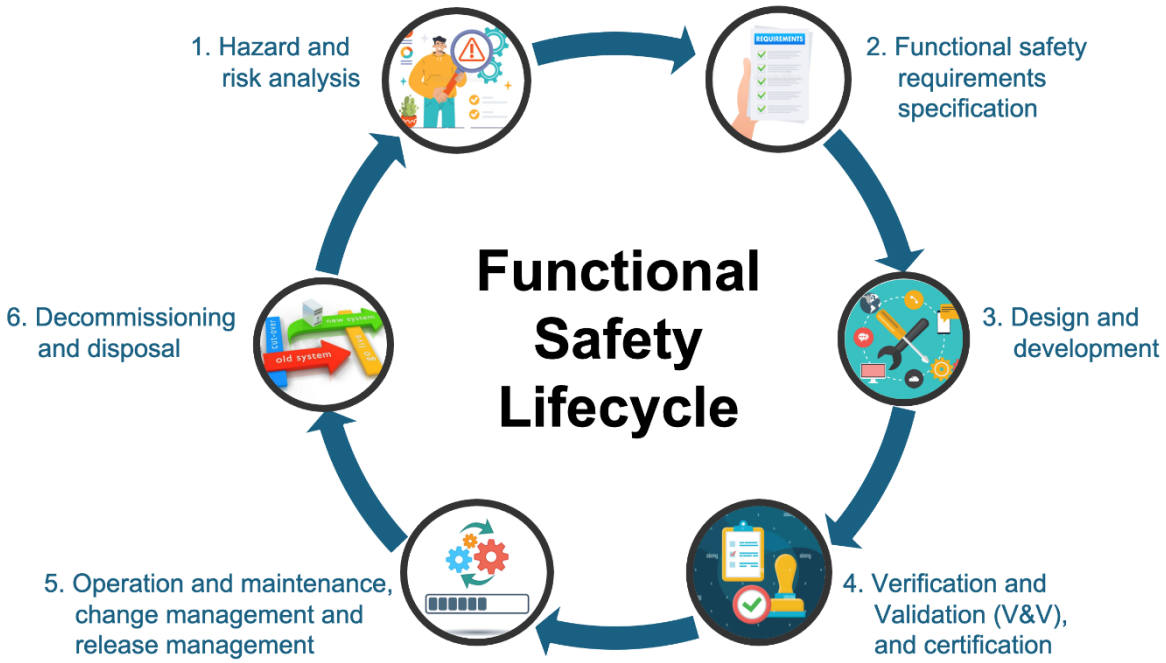

Figure 2. Functional safety lifecycle

Each phase of the functional safety lifecycle is described below.

7.1 Phase 1: Hazard and risk assessment

This phase is to determine the hazards and hazardous events of the IoT system to be deployed, sequence of events leading to the hazardous event, risks associated with the hazardous event, and requirements for risk reduction (requirement for SIL class) and safety functions by taking into consideration the IoT system's component failure rate. This is assumed that the hazard and hazardous event of the process have been determined prior and the design of the related IoT devices has been finalised.

The organisation shall identify and evaluate different types of risks and potential hazards caused by IoT system to people, environment, and assets in order to determine the functional safety requirements for the IoT system.

The risk assessment of IoT system functional safety shall include the following.

a) Failure on-demand of the IoT system during presence of hazard

b) Spurious failure of IoT system when there is no presence of hazard

These risks shall be identified early during hazard and risk assessment to ensure they are mitigated. The identified risks should be reduced to As Low as Reasonably Practicable (ALARP). There are various techniques and approaches used in different industries to weigh the risks versus costs such as Hazard and Operability Study (HAZOP) and What-if Analysis.

The common types of hazard and risks assessment should include:

a) Random or systematic failures of the hardware or software;

b) Human error;

c) Communication error or loss of communication;

d) Communication security;

e) Loss of electricity supply;

f) Improper/Insecure end-of-life decommissioning;

g) Maintenance error/breakdown (e.g., diagnostics, firmware updates);

h) Incorrect specifications of the system, including in the hardware and software;

i) Environmental circumstances for example: temperature, weather, electromagnetic interference, or mechanical phenomena;

j) Cybersecurity threats; and

k) AI risks in IoT systems such as misinterpretation of sensor data, unintended system behaviour due to model drift, or failure to respond correctly to edge cases.

7.2 Phase 2: Functional safety specification

This phase is to define specific safety functions and its safety limits. The specification shall draw upon and incorporate the analysis from the previous phase, namely:

a) Hazard analysis - Hazards resulting from potential system malfunctions; and,

b) Risk assessment - Evaluate each hazard's severity and likelihood.

The IoT system safety criticality level shall be determined from the maximum severity of the risk assessment.

The organisation shall define and document functional safety requirements to address the hazards and risks identified in Phase 1. For example, in the case of communication loss, the safety requirement may demand redundant communication links, timeout detection, and fail-safe transitions. As such, the safety integrity will have to be ensured all along the supply chain like development, verification, update, deployment, etc.

These functional safety specifications shall be detailed and traceable to ensure that all identified risks and challenges are systematically addressed and managed. It shall include:

a) Hardware, software, communication, and cybersecurity;

b) Alignment with sector-specific standards such as IEC 61508, ISO 26262, IEC 62304. Refer to Annex A for the list of reference standards including industry-specific standards; and

c) Categorisation according to relevant industry domains and mapped to the appropriate safety criticality level such as SIL and ASIL.

7.3 Phase 3: Design and development

The IoT system shall be designed and developed in accordance with the functional safety specifications defined in Phase 2. The design and development considerations should include the following:

a) Protective layers: sensors, actuators, logic solvers, relays, and interlocks;

b) Redundancy and diagnostics;

c) Fail-safe behaviour in case of fault detection;

d) Modular and verifiable architecture for ease of validation; and

e) Hardware safety integrity requirements based on IEC 61508.

The organisation shall ensure functional safety and security standard practices are followed based on the following principles.

a) The design and development process shall be integrated with secure practices to ensure cyber resilience covering all security layers including connectivity, access, and infrastructure. The security management guidelines for Internet of Things (IoT) should be referred to MCMC MTSFB TC G013:2018.

b) Functional safety system shall be unaffected by the actions of cybersecurity implementation. For example, system patching shall not affect functional safety.

7.4 Phase 4: Verification and Validation (V&V) and certification

The IoT system shall meet the functional safety requirements through rigorous Verification and Validation (V&V). The needs of certification shall be discussed among the interested parties.

7.4.1 Verification and Validation (V&V)

After design and development, the V&V shall be performed according to ISO/IEC 17029 to ensure that the IoT system can execute the functional safety as designed. Any findings of the V&V exercise shall be rectified immediately.

The V&V shall include, according to the domain the following:

a) Unit, system and stress testing;

b) Integration and communication testing;

c) Simulation and fault injection;

d) Functional testing;

e) Cybersecurity testing;

f) Documentation and traceability; and

g) Formal verification (where feasible)

7.4.2 Certification

In the case of certification is needed for the IoT system, it shall be performed by an independent and accredited third-party according to ISO/IEC 17065 to ensure the credibility of the IoT system. The independent certification ensures the functional safety and security measures implemented in accordance with the design requirements.

The IoT system certification should comply with standards for specific industry such as IEC 61508 for general industry and ISO/SAE 21434 for automotive.

The organisation may also comply with ISO/IEC 15408 to ensure the security of the system, complementing the functional safety requirements specified by relevant standards such as IEC 61508 or ISO 26262, thereby achieving a comprehensive approach to system safety and security certification strategy.

IoT devices or systems utilising communication technologies operating within frequency ranges subject to regulation by the Malaysian Communications and Multimedia Commission, including but not limited to radio frequency technologies, shall obtain all required equipment, EMC, and spectrum-related approvals and shall comply with all applicable Technical Codes prior to IoT system functional safety certification.

7.5 Phase 5: Operation

The IoT system shall be operated, maintained and regularly updated to ensure the system will continue to function and comply with the functional safety requirements.

7.5.1 Operation and maintenance

Safety manual/SOP shall be established to conduct the operation and maintenance. The verified, validated and certified IoT system shall be transitioned into operation and maintenance phase which shall oversee and manage the following.

a) Daily operation.

b) Perform regular system diagnostics.

c) Execute maintenance and repair to ensure system availability and reliability.

7.5.2 Change management

Any modifications to the IoT system such as hardware, software, or functional safety shall undertake a formal change management done by competent personnel. This includes evaluation of safety impacts, approvals, and rollback plans. The organisation may refer to relevant Technical Codes for guidelines on change management.

7.5.3 Release management

Approved changes that have been implemented to the IoT systems shall follow a structured release management process to ensure safety, reliability, and system integrity.

a) Planning and risk assessment: Identify potential impacts of the changes, evaluate associated risks, and develop a plan to address possible issues before deployment.

b) Regression testing: Conduct comprehensive testing to ensure that new changes do not adversely affect existing functionalities and performance.

c) Re-verification and re-validation: Reconfirm that the updated system meets all safety requirements and validation criteria, ensuring continued compliance and safety integrity.

d) Documentation and version control: Maintain detailed records of changes, test results, and system versions for traceability, accountability, and future reference.

7.5.4 Incident management

The organisation shall establish an incident management system to effectively respond and address incidents. Incident management is a process initiated by the organisation’s operation team to respond and address unplanned events that affect functional safety.

The two (2) main objectives of incident management are:

a) Identify and rectify issues to restore normal operation as fast as possible; and

b) Mitigate the adverse effect of critical incidents on business operations.

In summary, the incident management process should encompass the following key steps to ensure effective response and resolution.

a) Plan and prepare: Develop contingency plans and establish procedures in advance to respond promptly and effectively to incidents.

b) Handling an incident: Detect, assess, and respond to incidents in real-time to minimise impact and restore normal operations as quickly as possible.

c) Information sharing: Communicate relevant incident details securely and transparently with stakeholders to support coordinated efforts and informed decision-making.

d) Post-incident activities: Conduct investigations, document lessons learned and implement corrective actions to prevent recurrence and improve future response capabilities.

The detailed requirements of incident management can be referred to MCMC MTSFB TC G015.

7.6 Phase 6: Decommissioning and disposal

The organisation shall decommission and dispose of an IoT system that has reached the end of its useful life in accordance with the following steps.

a) Perform an impact analysis/assessment of the proposed decommissioning or disposal activity so that it will not affect the functional safety of the IoT System.

b) Safely decommission the IoT system in a controlled manner to prevent hazards to persons, property, or the environment.

c) Ensure ethical, secure and environmentally responsible disposal of IoT system including:

   i) Secure erasure, anonymisation, or irreversible destruction of all personal data and sensitive information, including Personally Identifiable Data (PID), in accordance with the Personal Data Protection Act 2010 (Act 709);

   ii) Environmentally responsible recycling, reuse, or safe destruction of hardware components such that no residual safety, security, or environmental risk remains from obsolete or decommissioned systems;

   iii) Handling, storage, transportation, treatment, and disposal of electronic waste and other scheduled wastes in compliance with Section 34B of the Environmental Quality Act 1974 (Act 127) and the Environmental Quality (Scheduled Wastes) Regulations 2005; and

   iv) Compliance with applicable regulatory, environmental, social, and governance (ESG) requirements for the disposal of electronic components, including batteries and printed circuit boards, through licensed waste management providers.

Annex A
(normative)

Normative references

Act 127, *Environmental Quality Act 1974*

Act 709, *Personal Data Protection Act 2010*

The Environmental Quality (Scheduled Wastes) Regulations 2005

MCMC MTSFB TC G009, *Information and Network Security – Requirements*

MCMC MTSFB TC G013, *Internet of Things (IoT) - Security Management*

MCMC MTSFB TC G015, *Information and Network Security – Incident Management*

MCMC MTSFB TC G022, *Internet of Things (IoT) - High-Level Functional Architecture*

MCMC MTSFB TC G031, *Internet of Things (IoT) - Application Security Requirements*

MCMC MTSFB TC G042, *Information and Network Security-Malaysia Critical Security Controls (MYCSC)*

MCMC MTSFB TC G044, *Internet of Things (IoT) – Baseline Security Requirements for Consumer Devices*

MCMC MTSFB TC G045, *Internet of Things (IoT) - Device Security Requirements*

MCMC MTSFB TC G050, *Internet of Things (IoT) – Baseline Security Assessment for Consumer Devices*

IEC 50156, *Electrical equipment for furnaces and ancillary equipment*

IEC 60730, *Automatic electrical controls - Part 1*

IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*

IEC 61511-1, *Functional safety - Safety instrumented systems for the process industry sector - Part 1*

IEC 61513, *Nuclear power plants - Instrumentation and control for systems important to safety*

IEC 61784-3, *Industrial communication networks – Profiles – Part 3-19: Functional safety fieldbuses*

IEC 61850, *Communication networks and systems for power utility automation*

IEC 62304, *Medical device software — Software life cycle processes*

IEC 62351, *Power systems management and associated information exchange - Data and communications security*

IEC 62353, *Medical electrical equipment - Recurrent test and test after repair of medical electrical equipment*

IEC 82304-1, *Health software - Part 1: General requirements for product safety*

ISO 10218, *Robotics - Safety Requirements*

ISO 13485, *Medical devices — Quality management systems — Requirements for regulatory purposes*

ISO 13849-1, *Safety of machinery — Safety-related parts of control systems*

ISO 14971, *Medical devices — Application of risk management to medical devices*

ISO 26262-9, *Functional safety Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses*

ISO/IEC 15408-1 - *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security*

ISO/IEC 17065 - *Conformity assessment - Requirements for bodies certifying products, processes and services*

ISO/IEC 20924, *Internet of Things (IoT) and digital twin - Vocabulary*

ISO/IEC 23894, *Information technology — Artificial intelligence — Guidance on risk management*

ISO/IEC 24029, *Artificial Intelligence (AI) — Assessment of the robustness of neural networks*

ISO/IEC TR 5469, *Artificial Intelligence - Functional Safety and AI Systems*

ISA 84, *Standard for safety instrumented systems*

ISA/IEC 62443, *Industrial network and system security*

ITU-T Y.4000, *Overview of the Internet of Things*

ITU-T Y.4100, *Common requirements of the Internet of Things*

ITU-T Y.4806, *Security Capabilities Supporting Safety of the Internet of Things*

EN 81, *Safety rules for the construction and installation of lifts*

EN 115, *Safety of escalators and moving walks*

EN 50126, *Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*

EN 50129, *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*

ETSI EN 303 645, *Cybersecurity Standard for Consumer IoT Devices*

UNECE WP.29, *World Forum for Harmonization of Vehicle Regulations*

NIST AI 100-1, *Artificial Intelligence Risk Management Framework*

NISTIR 7628, *Guidelines for Smart Grid Cybersecurity*

DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*

Annex B
(informative)

Functional safety use case: Smart traffic light

Overview

Smart traffic light systems are safety-critical IoT systems deployed to manage traffic flow, reduce congestion, and improve road safety. Unlike traditional standalone traffic lights, smart traffic lights integrate sensors, communication networks, central management platforms, and remote-control capabilities.

Traffic signals, once standalone devices, are now part of interconnected systems. Modern traffic controllers as illustrated in Figure A.1 not only follow pre-set schedules but also analyse sensor data, communicate with nearby intersections, and support remote control for improved traffic management.

This Annex illustrates how the **IoT functional safety lifecycle** can be applied to a **smart traffic light system**, demonstrating how safety risks are identified, mitigated, verified, and managed throughout the system's lifecycle — from concept to decommissioning.

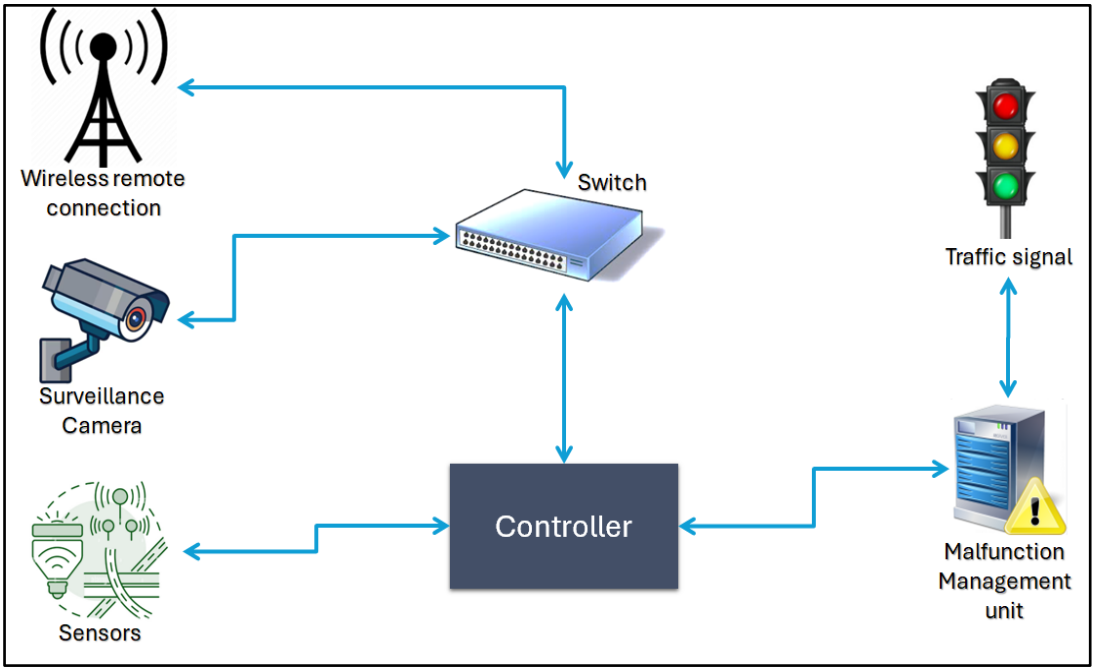

Figure B.1 - Smart traffic lights system

Phase 1: Hazard and Risk Assessment

In this phase, the organisation identifies hazards arising from malfunctioning behaviour of the smart traffic light system and evaluates the associated risks to road users, operators, and infrastructure.

Typical hazards include:

- Conflicting signal outputs (e.g. simultaneous green lights for intersecting roads)

- Traffic lights stuck in a fixed state (e.g. permanent red or green)
- Loss of communication between intersections or the central control system
- Incorrect sensor data leading to unsafe signal timing
- Cyber intrusion resulting in unauthorised signal manipulation
- Power failure or controller hardware faults

Risk assessment considerations:

- Severity of potential accidents (e.g. collisions, injuries, fatalities)
- Likelihood of occurrence
- Ability to detect and control the hazard

The organisation determines the required **risk reduction level** (e.g. SIL) and identifies where **fail-safe behaviour** is necessary. Risks should be reduced to **As Low As Reasonably Practicable (ALARP)**.

Phase 2: Functional Safety Specification

Based on the identified hazards and risks, the organisation defines **functional safety requirements** for the smart traffic light system.

Examples of functional safety requirements:

- The system shall detect conflicting signal commands and transition to a predefined safe state.
- The traffic light shall revert to **flashing red mode** upon loss of communication or critical fault.
- Independent fault detection shall monitor signal logic and output states.
- Manual override shall be available for authorised traffic operators.
- Safety functions shall remain operational during cybersecurity updates or communication reconfiguration.

Each safety requirement shall be:

- Clearly defined and documented
- Traceable to identified hazards
- Assigned an appropriate safety integrity level (e.g. SIL 2 or SIL 3 depending on risk)

Phase 3: Design and Development

In this phase, the smart traffic light system is designed and developed to fulfil the functional safety requirements.

Design considerations include:

- Redundant signal control logic to prevent single points of failure
- Independent malfunction management units that monitor signal outputs
- Protected layers such as sensors, logic solvers, actuators, and interlocks
- Fail-safe default states (e.g. flashing red) that do not rely on communication links

- Secure interfaces between IoT components and central management systems

Functional safety and cybersecurity shall be integrated so that:

- Cybersecurity controls do not interfere with safety functions
- Safety behaviour remains predictable under fault and attack conditions

Phase 4: V&V and Certification

The organisation verifies and validates that the smart traffic light system performs its safety functions as specified.

Verification and validation activities may include:

- Functional testing of normal and abnormal operating scenarios
- Simulation of fault conditions (e.g. sensor failure, communication loss)
- Fault injection to confirm fail-safe transitions
- Cybersecurity testing to ensure safety is maintained under attack scenarios
- Review of documentation, traceability, and test records

Where required, **independent certification** is conducted by an accredited body to demonstrate compliance with applicable functional safety standards and regulatory requirements.

Phase 5: Operation and Maintenance

Once deployed, the smart traffic light system enters the operational phase, where ongoing safety must be maintained.

Key operational activities include:

- Continuous monitoring of system health and diagnostics
- Regular inspections and preventive maintenance
- Controlled firmware and software updates through formal change management
- Incident management procedures for handling faults, accidents, or near-misses
- Training of traffic operators and maintenance personnel

Any modifications to hardware, software, or safety functions must undergo safety impact assessment, re-verification, and documentation updates to ensure continued compliance with functional safety requirements.

Phase 6: Decommissioning and Disposal

When a smart traffic light system reaches the end of its useful life, it shall be safely decommissioned and disposed of without introducing residual risks.

Decommissioning activities include:

- Impact assessment to ensure decommissioning does not compromise ongoing traffic safety
- Controlled shutdown and isolation of traffic controllers
- Secure removal or transition to temporary safe traffic control modes

Disposal considerations include:

- Secure deletion or irreversible destruction of stored traffic data and personal data
- Environmentally responsible recycling or disposal of hardware components
- Proper handling of electronic and hazardous waste through licensed waste management providers

The organisation shall ensure that **no residual safety, security, or environmental risks remain** after decommissioning.

Summary

This use case demonstrates how applying the **IoT functional safety lifecycle** enables systematic identification, control, and management of safety risks in a smart traffic light system. By following each lifecycle phase, organisations can design, deploy, operate, and retire smart traffic infrastructure in a manner that prioritises public safety, regulatory compliance, and long-term sustainability.

Annex C
(informative)

Functional safety use cases (Industrial)
Selected risks and controls in various IoT domains

This Annex is intended to provide a high-level overview of typical IoT risks and controls. It does not replace system-specific hazard and risk analysis in the functional safety lifecycle.

C.1 Smart grid (e.g., Smart meters)

Items	Descriptions
Risks	a) Overvoltage b) Blackout c) Cyber-attacks d) Coordinated Distributed Energy Resources (DER) attacks
Controls	a) Tamper detection and audit logging b) Network isolation for critical components c) Continuous monitoring and anomaly detection d) Cryptographic firmware signing e) Load-shedding logic with failover
Standard references	a) IEC 61508 b) IEC 62351 c) NISTIR 7628

C.2 Medical Appliances (e.g., Smart insulin pumps)

Items	Descriptions
Risks	a) Overdose b) Data loss c) Network failure d) Unintended physical tampering
Controls	a) Data encryption, integrity checks b) Fail-safe actions c) Alert systems with redundancy d) Self-diagnostic capabilities e) Firmware validation and audit trails
Standard references	a) IEC 62304 b) ISO 14971 c) IEC 82304-1

C.3 Industrial system (e.g., SCADA, Robots, Smart elevator system)

Items	Descriptions
Risks	a) Mechanical injury b) Thermal events c) Loss of life d) Loss of operation e) Data breach f) Cyber-terrorism
Controls	a) Dual-channel safety systems b) Fail-operational modes c) Integrated intrusion detection d) Multi-nodes e) Predictive diagnostics
Standard references	a) IEC 61508 b) ISA/IEC 62443 c) ISO 13849

C.4 Automotive (e.g., ADAS, ECUs)

Items	Descriptions
Risks	a) Sensor failure b) Inaccurate actuation c) Software safety d) Cyber-attacks related loss of control
Controls	a) Redundant sensing (Light Detection and Ranging (LIDAR), Radio Detection and ranging (RADAR)) b) Automotive Safety Integrity Level (ASIL) - certified microcontrollers c) Electronic Control Unit (ECU) watchdogs and failover d) Intrusion detection and prevention systems for in-vehicle networks e) Secure On the Air (OTA) updates f) Anomaly detection for abnormal vehicle behaviour
Standard references	a) ISO 26262 b) ISO/SAE 21434 c) UNECE WP.29 d) ISA/IEC 62443

C.5 Smart Home (e.g., Locks, Thermostats)

Items	Descriptions
Risks	a) Fire b) Unauthorised access c) Privacy breaches
Controls	a) Sensor redundancy b) Local fallback control c) Secure boot and rollback d) Tamper-proof hardware
Standard references	a) IEC 60730 b) ETSI EN 303 645

C.6 Artificial Intelligence (AI)

Items	Descriptions
Risks	a) Opaque AI decisions b) adversarial attacks
Controls	a) Explainable AI (XAI) integration b) Adversarial training and robustness testing for AI models c) Fallback logic for uncertain predictions d) Continuous model validation e) Human-in-the-loop controls
Standard references	a) ISO/IEC TR 5469 b) ISO/IEC 24029 c) ISO/IEC 23894

Annex D
(informative)

Internet of Things (IoT) functional safety and security

Functional safety and security in IoT systems are complementary, working together to create a robust and reliable system. While they share some similarities, their primary focus differs significantly.

The objective of functional safety is to reduce the risk of harm resulting from system faults or breakdowns, guaranteeing that the system functions correctly and safely. In contrast, security addresses threats from malicious actors and unauthorised access, protecting the system from external attacks.

Both are crucial for designing and deploying connected IoT systems, especially in critical applications. It is important to remember that IoT systems cannot achieve functional safety without robust IoT security.

The differences between functional safety and security are summarised in the Table D.1 below.

Table D. 1 - The differences between IoT functional safety and security

Items	IoT Functional Safety	IoT Security
Purpose	To ensure IoT systems operate safely and reliably, including during faults or failures, so that harm to people, property, or the environment is prevented or minimised.	To ensure IoT systems, devices, networks, and data are protected from unauthorised access, misuse, and cyberattacks, maintaining confidentiality, integrity, and availability.
Integration	Functional safety and security are increasingly integrated in IoT systems, as cyberattacks can potentially lead to safety hazards. Secure protocols and communication channels, coupled with fail-safe mechanisms, are crucial for building robust and secure IoT systems.	A secure system that is also functionally safe to prevent unauthorised access and ensure reliable operation, even in the face of malfunctions.
Example	Implementing fail-safe mechanisms, redundancy, and error-checking protocols to prevent harm to people, assets or environment.	Encryption, authentication protocols, secure communication channels, and intrusion detection systems.
Standards	IEC 61508 is a functional safety standard and a key standard for functional safety in various industries, including IoT.	IEC 62443 is a cybersecurity standard that is critical for industrial cybersecurity and IoT. MCMC MTSFB TC G013:2018 – IoT Security Management for general security requirements of IoT Systems for CMI.

Bibliography

[1] ISO/IEC JTC 1, *Internet of Things (IoT)*

[2] IEC TR 63069, *Industrial-process measurement, control and automation - Framework for functional safety and security*

Acknowledgements

Members of the Security, Trust and Privacy Working Group

Working Group Leaders

Thaib Mustafa (Chair)	Smart Tech Asia Pacific Sdn Bhd
Prof Dr Shahrulniza Musa (Vice Chair)	Universiti Kuala Lumpur

Drafting Committee Members

Prof Dr Shahrulniza Musa (Draft Lead)	Universiti Kuala Lumpur
Mr Sharul A Rashid (Co-Draft Lead)	Digital Connect Society
Ms Alisa Rafiqah Adenan (Secretariat)	Malaysian Technical Standards Forum Bhd
Ms Shazwani Salleh	CyberSecurity Malaysia
Dr Zainab Senan Attar Bashi	International Islamic University Malaysia
Mr Andrew Chow	Maxis Broadband Sdn Bhd
Ms Amira Amran	SIRIM Berhad
Ms Nur Hidayah Ibrahim	SIRIM Berhad
Ms Wan Zarina Wan Abdullah	SIRIM Berhad
Mr Thaib Mustafa	Smart Tech Asia Pacific Sdn Bhd
Assoc Prof Ir Dr Yusnani Mohd Yussoff	Universiti Teknologi MARA
Ts Dr Hairulazwan Hashim	Universiti Tun Hussein Onn Malaysia
Mr Amit Kulkarni	*ABL Group*
Mr Zarul Annuar Hamzah	*PETRONAS*
Ir Mohd Kamil Mohd Arshad	*PETRONAS*
Mr Simon Phoon	*Supcon Technology (Malaysia) Sdn Bhd*

Contributors

Mr Chaw Yew Kong	U Mobile Sdn Bhd
Mr Siew Nen Jun	U Mobile Sdn Bhd
Ms Josephine Woo Wai Fun	*United Overseas Bank (UOB)*
Datuk Syahril Aziz	*Secure Insight Sdn Bhd*

Technical Code Review Panel

Mr Pathmanathan Muniandy	Cre8 IoT
Ir Zhafran Abdul Aziz	PETRONAS