Standardization in Cybersecurity

Koji Nakao
Distinguished Researcher, Cybersecurity Research Institute
National Institute of Information and Communications Technology (NICT)
Guest Professor, Yokohama National University
Cybersecurity Advisor, NISC

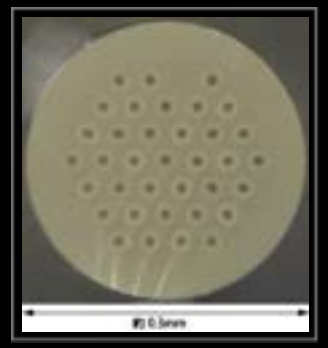
NICT National Institute of Information and Communications Technology

CYNEX CYBERSECURITY NEXUS

Research Topics in NICT

NICT: Sole national research institute in the field of ICT in Japan

Japan Standard Time (JST)
（Leap second on Jan 1, 2017）

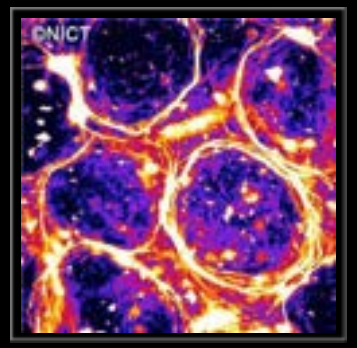


Optical Communication
(Peta bps class multi-core fiber)

Satellite Communication
（Internet Satellite WINDS）

Science Cloud
（Reai-time Web of Himawari-8）

Remote Sensing
（Pi-SAR2 image after 3.11）



Bio/Nano ICT
(Self-organizing bio molecule)

Brain ICT
(Brain-machine Interface)

Multi-lingual Machine Translation
(VoiceTra)

Ultra Realistic Communication
(Electronic Holography)

Cybersecurity
(DAEDALUS)

What is “Cybersecurity”

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1205
(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Overview of cybersecurity

ITU-T Recommendation X.1205: Overview of Cybersecurity

Recommendation ITU-T X.1205

Definition of Cybersecurity in 2008 (X.1205)

3.2.5 cybersecurity:
Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

The general security objectives comprise the following:
- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality.

ISO/IEC 27032: Guideline for Cybersecurity

4.20
Cybersecurity
(Cyberspace security)
preservation of confidentiality, integrity and availability of information in the Cyberspace

NOTE 1 In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

NOTE 2 Adapted from the definition for information security in ISO/IEC 27000:2009.


FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 27032

ISO/IEC JTC 1

Secretariat: ANSI

Voting begins on: 2012-04-26

Voting terminates on: 2012-06-26

Information technology — Security techniques — Guidelines for cybersecurity

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité

Reference number
ISO/IEC FDIS 27032:2012(E)

and networks are protected and resilient against information security risks, network security risks, Internet security risks, as well as Cybersecurity risks.

Figure 1 summarizes the relationship between Cybersecurity and other security domains. The relationship between these security domains and Cybersecurity is complex. Some of the critical infrastructure services, for example water and transportation, need not impact the state of Cybersecurity directly or significantly. However, the lack of Cybersecurity can have a negative impact on the availability of critical information infrastructure systems provided by the critical infrastructure providers.

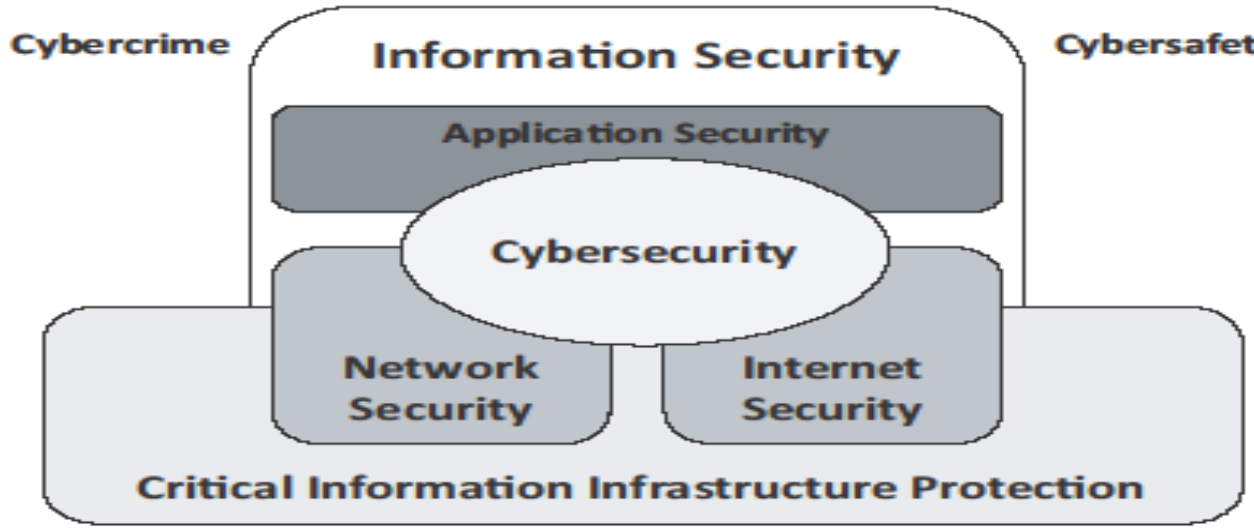


Figure 1 — Relationship between Cybersecurity and other security domains

On the other hand, the availability and reliability of the Cyberspace in many ways rely on the availability and reliability of related critical infrastructure services, such as the telecommunications network infrastructure. The security of the Cyberspace is also closely related to the security of the Internet, enterprise/home networks and information security in general. It should be noted that the security domains identified in this section have their own objectives and scope of focus. To deal with Cybersecurity issues, therefore requires substantial communications and coordination between different private and public entities from different countries and organizations. Critical infrastructure services are regarded by some governments as national security related services, and therefore may not be discussed or disclosed openly. Furthermore, knowledge of critical infrastructure weaknesses, if not used appropriately, can have a direct implication on national security. A basic framework for information sharing and issue or incident coordination is therefore necessary to bridge the gaps and provide adequate assurance to the stakeholders in the Cyberspace.

6.4 General model

6.4.1 Introduction

This clause presents a general model used throughout this International Standard. This clause assumes some knowledge of security and does not propose to act as a tutorial in this area.

This International Standard discusses security using a set of security concepts and terminology. An understanding of these concepts and the terminology is a prerequisite to the effective use of this International Standard. However, the concepts themselves are quite general and are not intended to restrict the class of IT security problems to which this International Standard is applicable.

ISO/IEC TS 27100 (2020) : Cybersecurity – Overview and Concept

3.2
cybersecurity
safeguarding of people, society, organizations and nations from cyber *risks* (3.7)
Note 1 to entry: Safeguarding means to keep cyber risks at a tolerable level.

3.7
risk
effect of uncertainty on objectives
Note 1 to entry: Cyber risk can be expressed as effect of uncertainty on objectives of entities in *cyberspace* (3.5).
Note 2 to entry: Cyber risk is associated with the potential that threats will exploit vulnerabilities in cyberspace and thereby cause harm to entities in cyberspace.

5.2 Cybersecurity

ISO/IEC TS 27100: Cybersecurity – Overview and Concep

The objective of adequate cybersecurity is to maintain an acceptable level of stability, continuity, and safety of entities operating in cyberspace. While it is not possible to always achieve these objectives, cybersecurity aims to reduce cyber risks to a tolerable level.

Areas of concern for cybersecurity include:

a) stability and continuity of society, organizations and nations;
b) property (including information) of people and organizations; and
c) human lives and health.

Cybersecurity with these characteristics is implemented by individual organizations. In cyberspace, organizations need to consider not only themselves, but also other parties who share cyberspace. While an organization needs to manage its vulnerabilities to ensure that the organization does not adversely affect other actors, it needs to work with others to reduce cyber risks. In addition, cybersecurity needs to reduce social and human losses in real space caused by cybersecurity incidents in cyberspace. Therefore, immediate detection and appropriate response of information security incidents are important elements of cybersecurity.

Cybersecurity standards: Objectives, Cyber Risk, Benefits

International CYBER Standards

The aim of the global cyberspace community, developers and interested parties is to develop international CYBER SECURITY and PRIVACY standards to help fight against CYBER CRIME

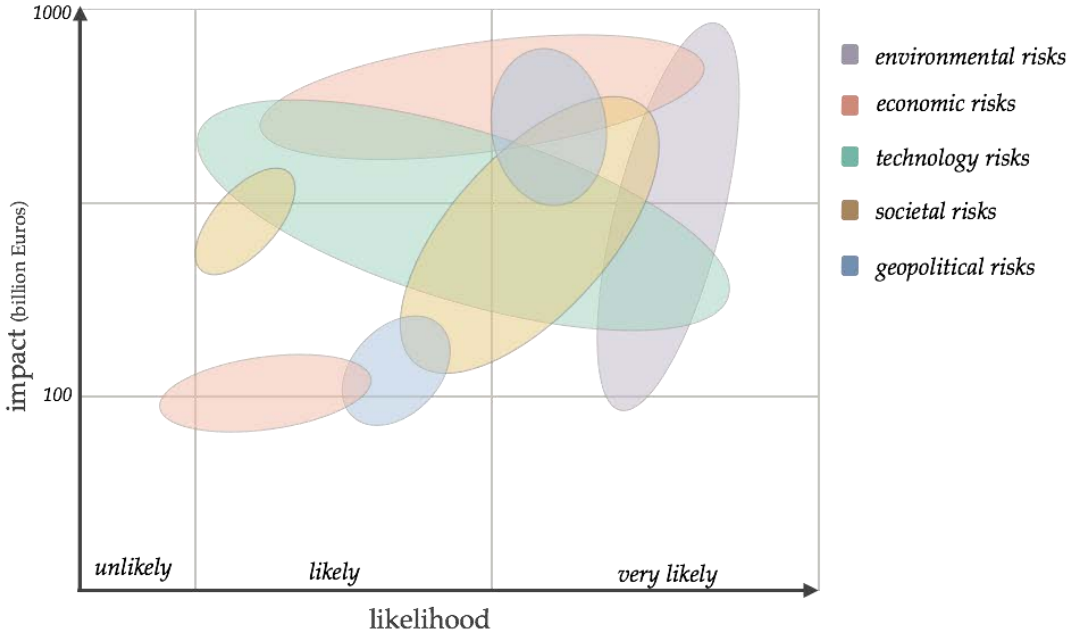
Implementation of international cyber standards can help organisations, governments to:

- *Reduce and minimise the cyber risks*
- *Minimise the impact and destructive effects of cyber attacks*
- *Protect their investment in the IT-based systems, services and infrastructure they use and to protect their sensitive and critical information*

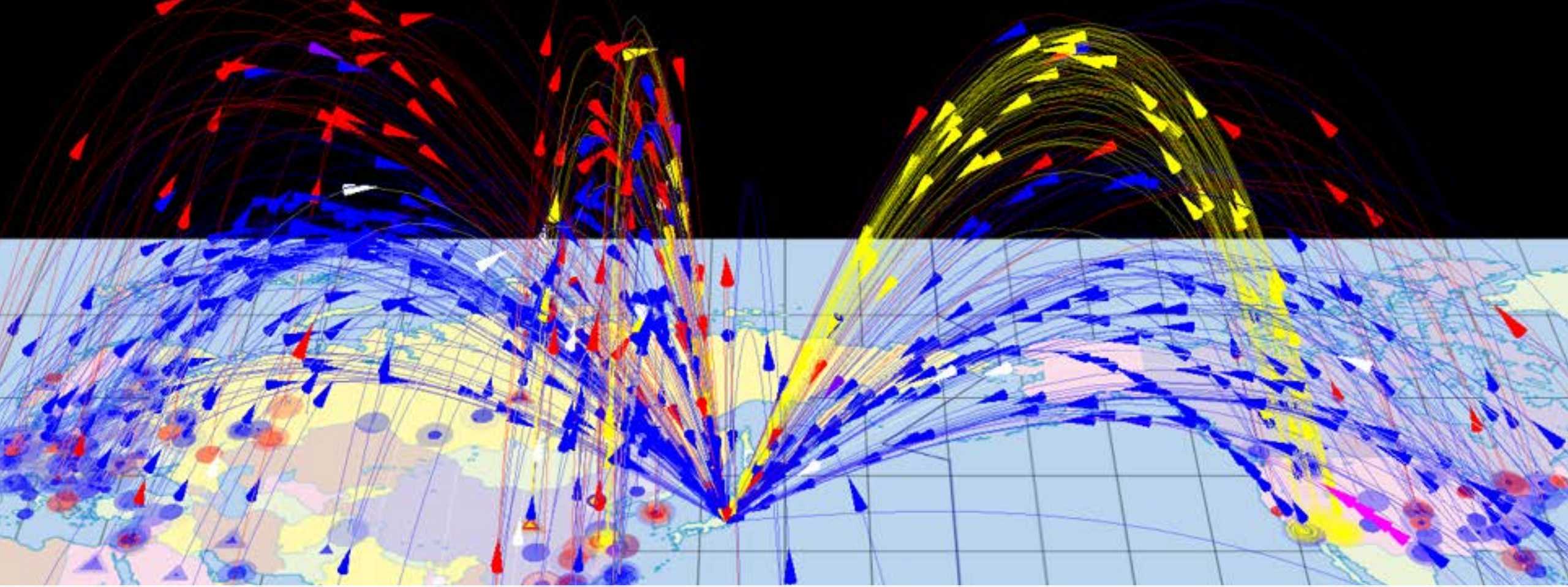
Source: Slides from Dr. Edward Humphrey in ISO workshop

Cyber Security Risk

- **THREATS AND RISKS**
  - Risks to operations, information, people, processes, services, applications, and technology
  - Threats to society and consumers
  - Threats to national infrastructure
- **IMPACT**
  - Financial loss, disruption or damage to systems and services due to the destructive power of cyber attack/incident
  - Leakage, theft, destruction of critical and sensitive information
- **CYBER SECURITY RISK THRESHOLDS**
  - Limiting the disruptive and destructive power and energy of the cyber attack
  - Cyber defence/preparedness, response and recovery



Source: Slides from Dr. Edward Humphrey in ISO workshop



NICTER

- is an **integrated security system** for countering indiscriminate cyberattacks
- based on a large-scale **darknet monitoring**, an automated **malware analysis** and their **correlation**

Some Benefits of Cyber Space Standards

The development of INTERNATIONAL CYBER STANDARDS through cooperation, joint sharing and learning, and consensus building, provides:

- *Improved protection, security and safety for all interested parties*
- *Basis for conformity assessments (certification, testing and inspection)*
- *Basis of mutual understanding and a common language to facilitate communications, innovation, trading and global governance*
- *Complements and supports national cyber policies and programmes*

Source: Slides from Dr. Edward Humphrey in ISO workshop

Players

World Standards Cooperation (WSC)

Regional Standards Bodies

Asia-Pacific

Europe (CEN, CENELEC, ETSI)

Americas

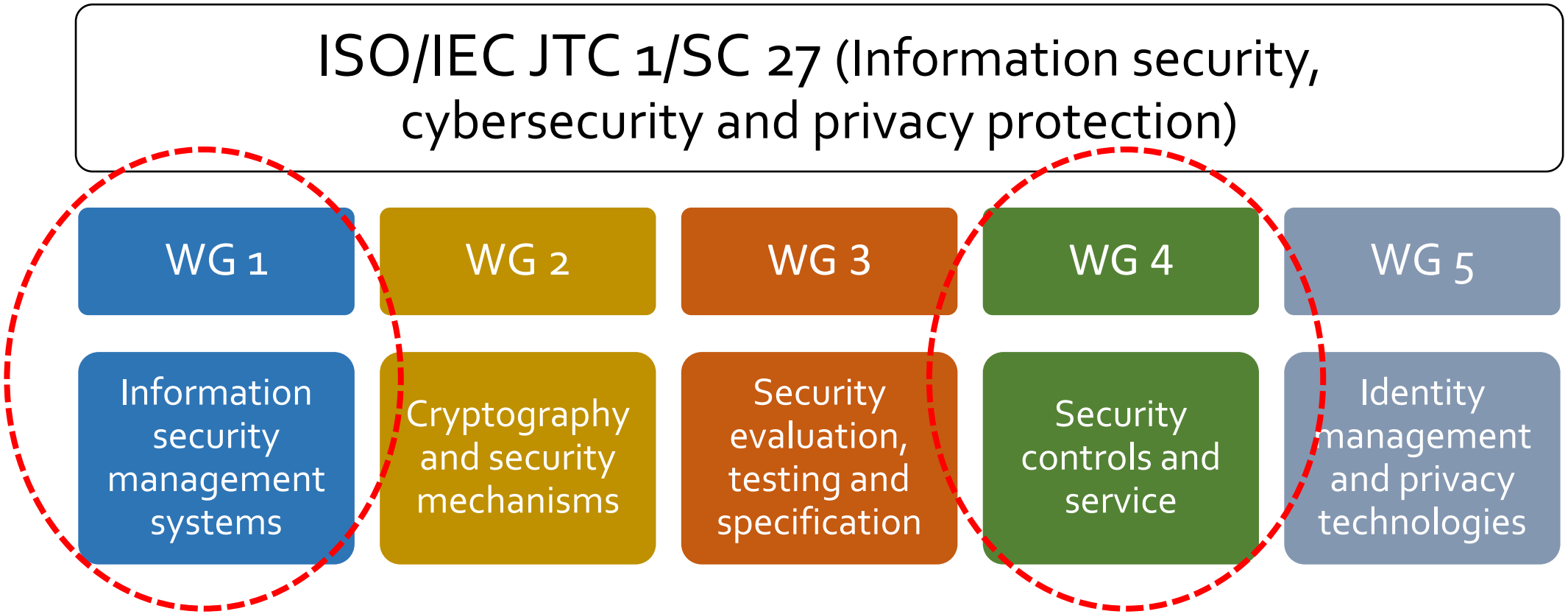
Liaisons (industry groups, consumer groups etc.)

National Standards Bodies (AFNOR, ANSI, BSI, DIN, SAC etc.)

Regulatory Bodies, Government Bodies …

Source: Slides from Dr. Edward Humphrey in ISO workshop

Cybersecurity standards in ISO/IEC JTC1/SC27



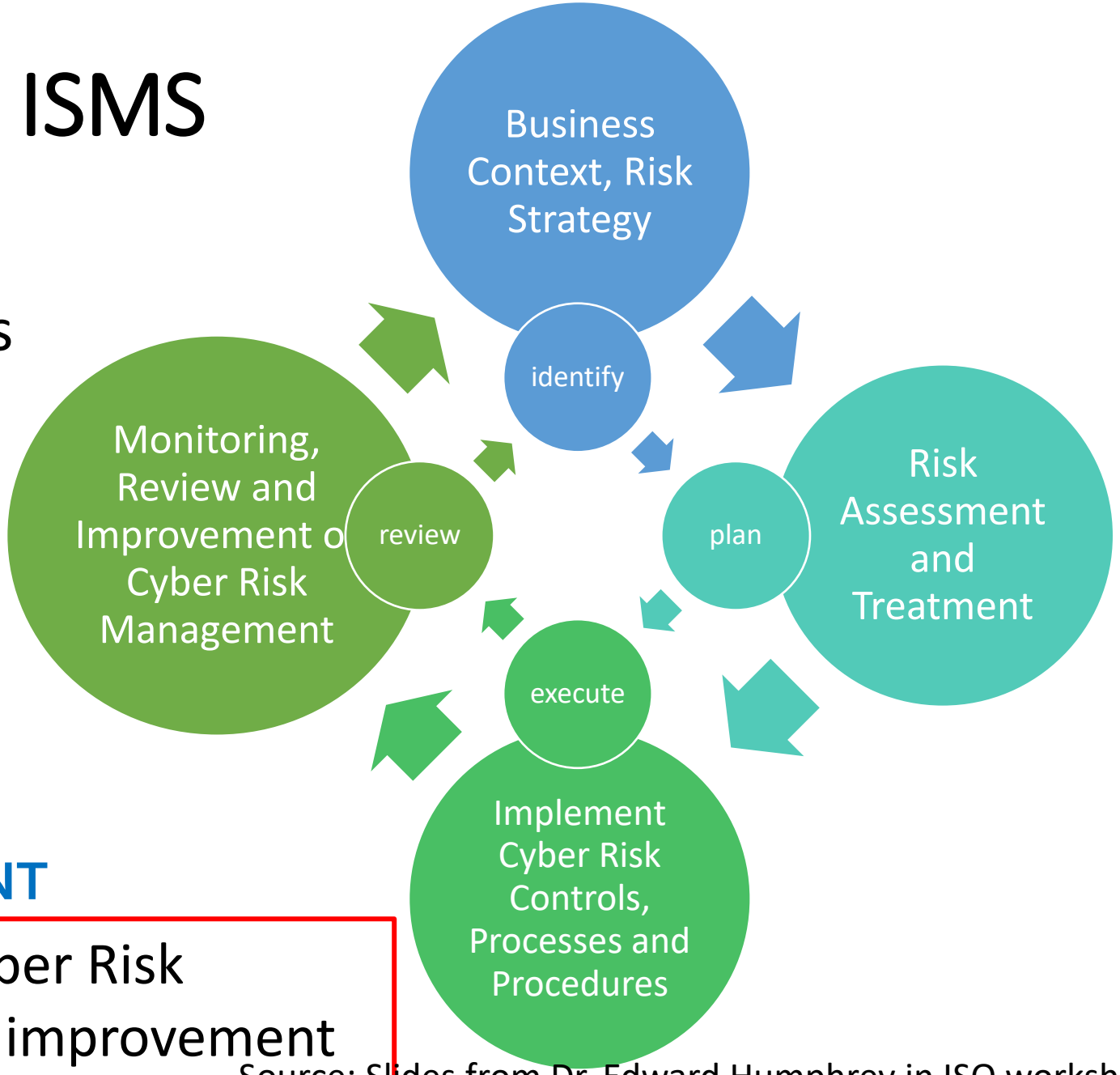
Cover the area of Cyber Security

Source: Slides from Dr. Edward Humphrey in ISO workshop

ISO/IEC 27001 ISMS

The on-going management of cyber risk through the process of continual improvement:

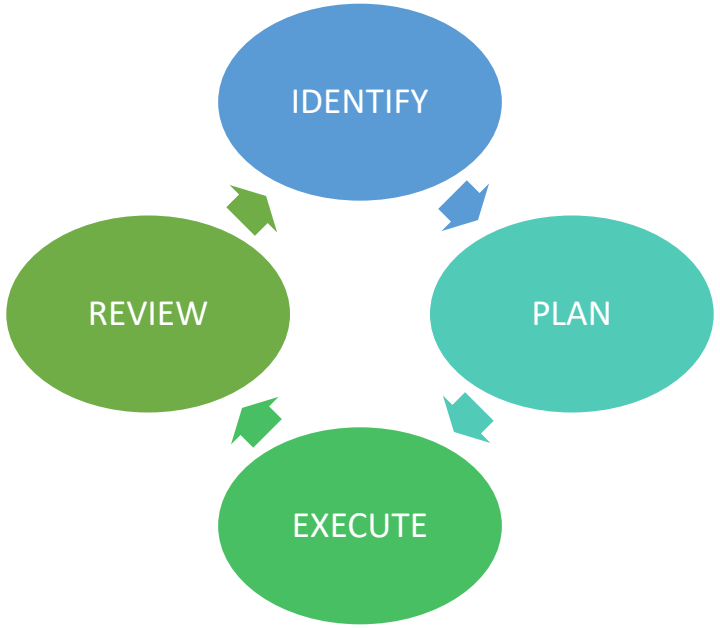
- Anticipate
- Prepare
- Protect
- Reactive & Responsive
- Adaptive *(business plasticity)*
- **CONTINUAL IMPROVEMENT**



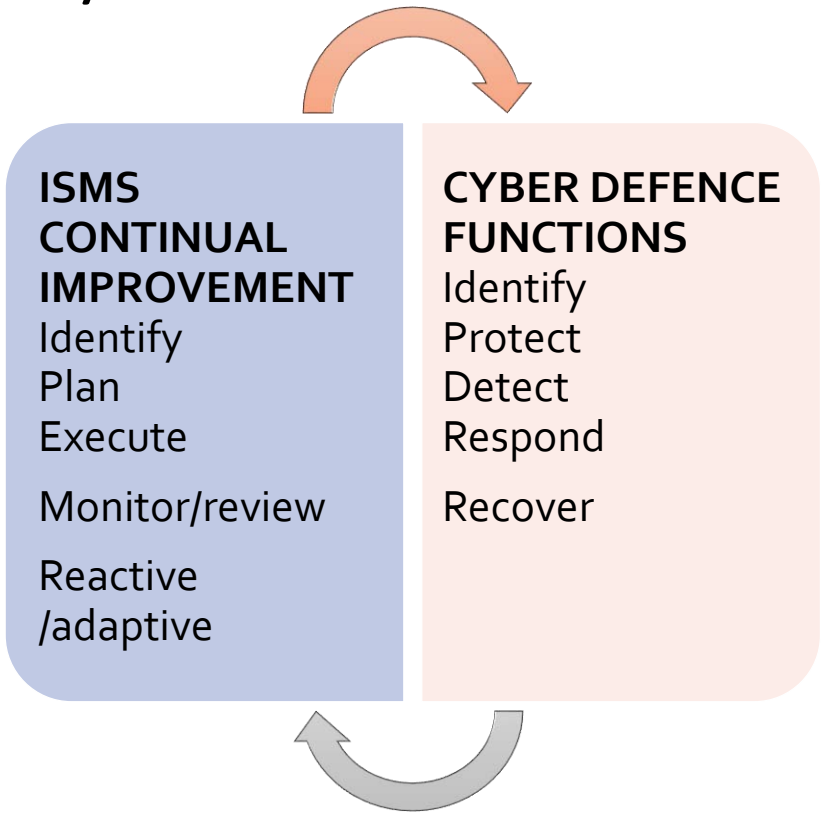
The on-going management of Cyber Risk through the process of continual improvement

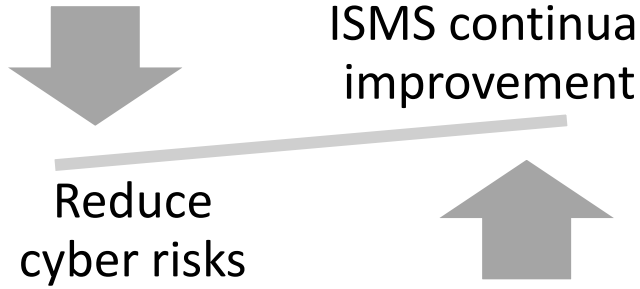
Source: Slides from Dr. Edward Humphrey in ISO workshop

ISO/IEC 27001 ISMS - Managing Cyber Risk



ISMS Continual Improvement Framework





Source: Slides from Dr. Edward Humphrey in ISO workshop

ISO/IEC 27103

IDENTIFY	Business Environment and Context Risk Assessment Risk Management Strategy Governance Asset management
PROTECT	Access Control Aware and Training Data Security Information Protection Policies, Processes and Procedures Maintaining Controls
DETECT	Monitoring and Detection Processes Incident Handling Management Processes
RESPOND	Response Planning and Management Process Continual Improvements Communications
RECOVER	Recovery Planning and Management Processes Continual Improvements Communications

WG 1 Projects related to Cybersecurity

Cybersecurity	
ISO/IEC TS 27100: 2020	Cybersecurity – Overview and Concepts
ISO/IEC 27102:2019	Information security management — Guidelines for cyber-insurance
ISO/IEC TR 27103: 2018	Cybersecurity and ISO and IEC Standards
ISO/IEC TS 27110: 2021	Cybersecurity framework development guidelines

WG 4 Projects 1/11

Guidance for information security controls 1/2	
ISO/IEC 27031:2011 [Revision: DIS]	Guidelines for information and communication technology (ICT) readiness for business continuity
ISO/IEC 27033, Part 1 – Part 6	Network security
ISO/IEC 27034, Part 1 – Part 7	Application security
ISO/IEC 27035, Part 1 – Part 4	Information security incident management
ISO/IEC 27036, Part 1 – Part 4	Information security for supplier relationships

WG 4 Projects 2/11

Guidance for information security controls 2/2	
ISO/IEC 27039:2015	Selection, deployment and operations of intrusion detection and prevention systems (IDPS)
ISO/IEC 27040:2015 [Revision: FDIS]	Storage security

WG 4 Projects 3/11

ISO/IEC 27033, Network security

- Part 1:2015, Overview and concepts
- Part 2:2012, Guidelines for the design and implementation of network security
- Part 3:2010, Reference networking scenarios -- Threats, design techniques and control issues
- Part 4:2014,Securing communications between networks using security gateways
- Part 5:2013, Securing communications across networks using Virtual Private Networks (VPNs)
- Part 6:2016, Securing wireless IP network access
- Part 7: Guidelines for network virtualization security [FDIS]

WG 4 Projects 4/11

ISO/IEC 27035, Information security incident management

Part 1:2023, Principles and processes	[Revision]
Part 2:2023, Guidelines to plan and prepare for incident response	[Revision]
Part 3:2020, Guidelines for ICT incident response operations	
Part 4, Coordination	[DIS]

WG 4 Projects 5/11

Investigation, digital evidence and electronic discovery	
ISO/IEC 27037:2012	Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 27041:2015	Guidance on assuring suitability and adequacy of incident investigative method
ISO/IEC 27042:2015	Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043:2015	Incident investigation principles and processes
ISO/IEC 27050, Part 1 – Part 4	Electronic discovery

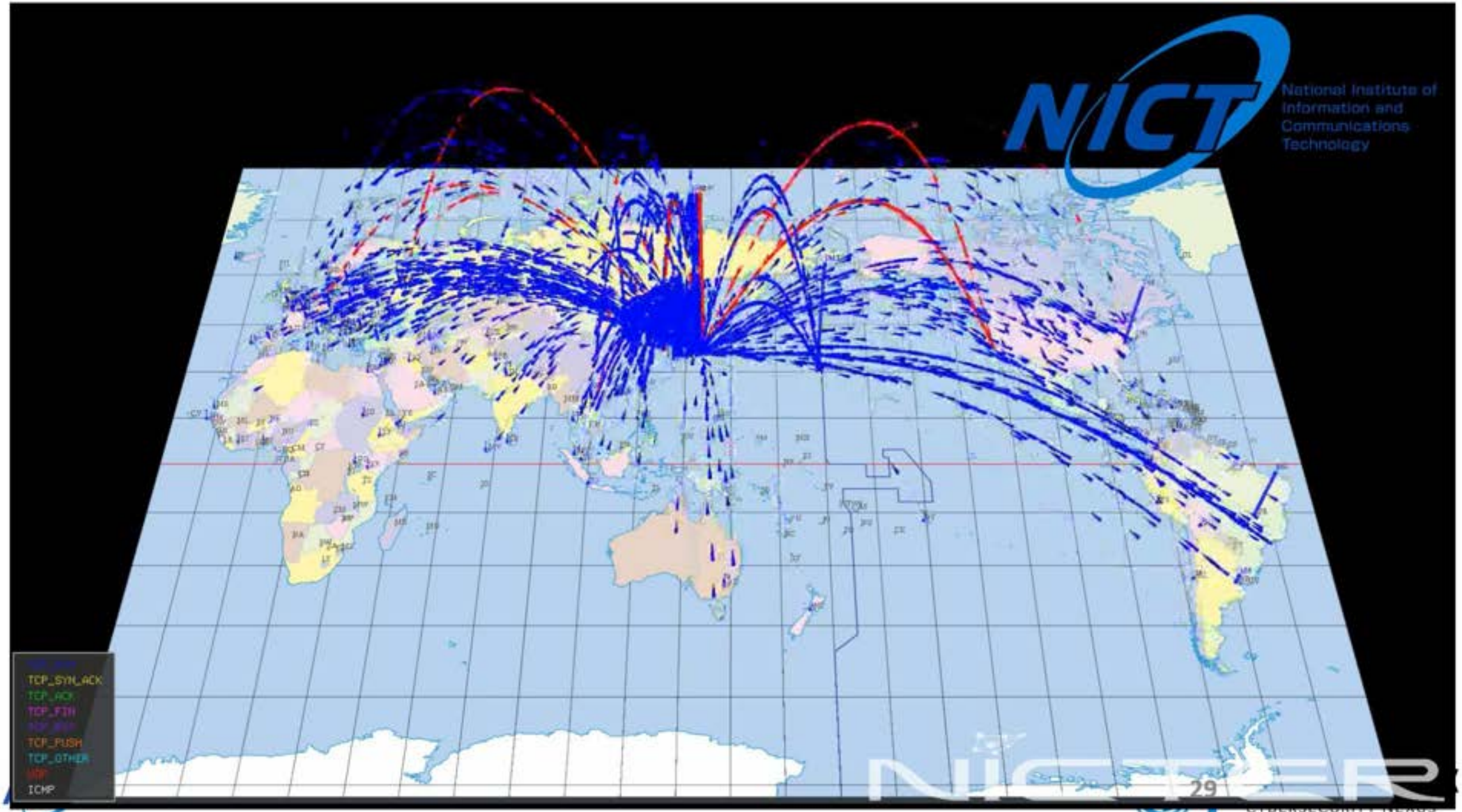
WG 4 Projects 6/11

Cybersecurity	
ISO/IEC 27032:2012 [Revision: FDIS]	Guidelines for cybersecurity Revision: Cybersecurity — Guidelines for Internet security
ISO/IEC 24392 [IS]	Security reference model for industrial internet platform

WG 4 Projects 7/11

IoT security and privacy, CPS	
ISO/IEC 27400:2022	IoT security and privacy – Guidelines
ISO/IEC 27402 [FDIS]	IoT security and privacy – Device baseline requirements
ISO/IEC 27403 [DIS]	IoT security and privacy – Guidelines for IoT-domotics
ISO/IEC 27404 [WD2]	IoT security and privacy – Cybersecurity labelling framework for consumer IoT
ISO/IEC 5689 [PWI→NP]	Security frameworks and use cases for cyber physical systems

- Base documents of SC 41 “Internet of Things and digital twin”
  - ISO/IEC 30141:2018, Internet of Things (IoT) – Reference architecture
  - ISO/IEC 20924:2021, Internet of things (IoT) – Vocabulary


National Institute of Information and Communications Technology
TCP_SYN_ACK
TCP_ACK
TCP_FIN
TCP_PUSH
TCP_OTHER
ICMP

ISO/IEC 27400 – Published

This was initially proposed by Japan based on the guideline produced in IoT promotion consortium of Japan.

- **Title: Cybersecurity – IoT security and privacy – Guidelines**
- Scope

This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

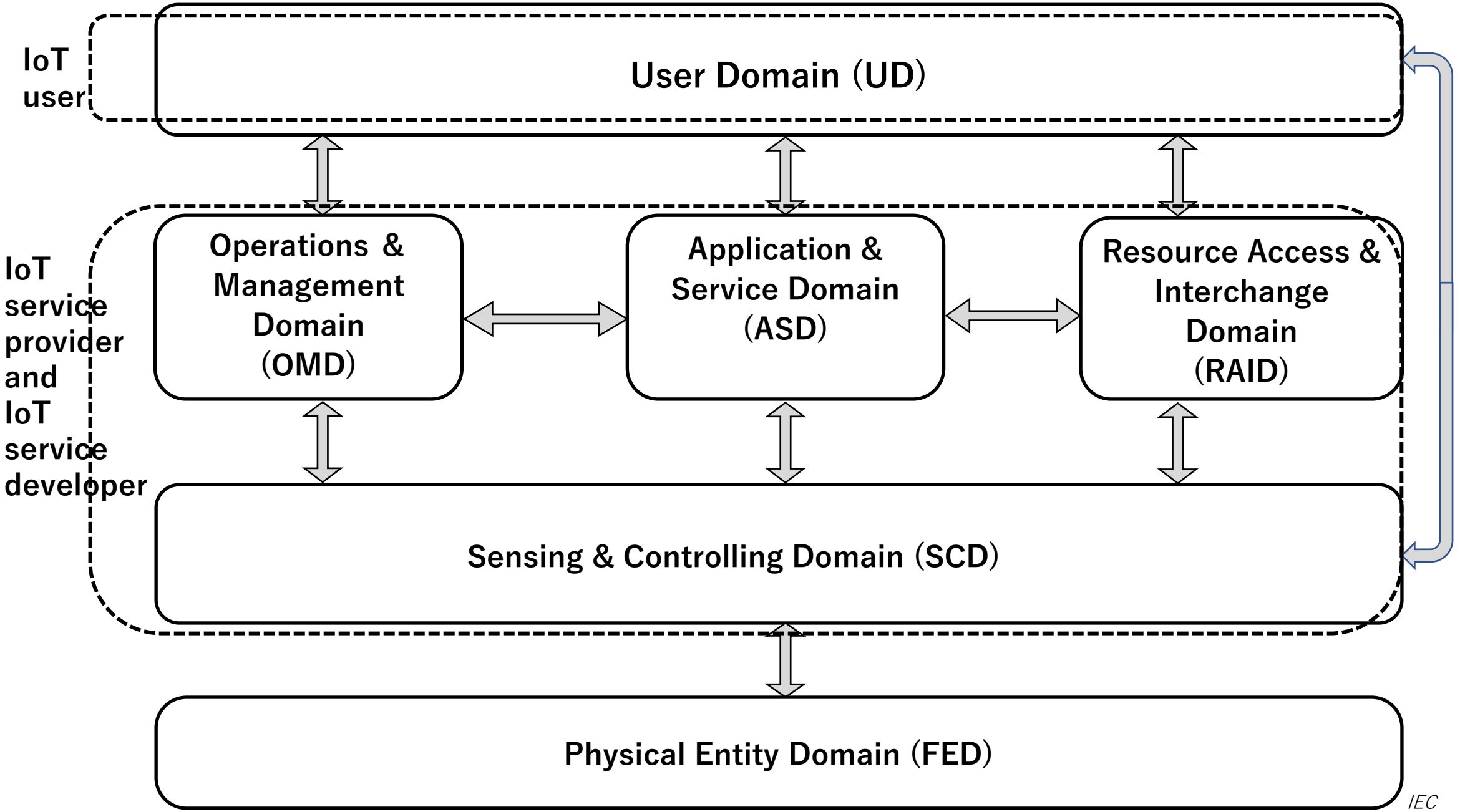
- Main Structure

  Clause 5：IoT concept and reference model

  Clause 6：Risk management for IoT systems

  Clause 7：Security controls and privacy controls

RA (Domain model) used in ISO/IEC 27400 （based on ISO/IEC 30141）



Security Controls in ISO/IEC 27400

Security controls for IoT service developer and IoT service provider

24 controls

- **7.1.2.1 Policy for IoT security**
- **7.1.2.2 Organization of IoT security**
- **7.1.2.3 Asset management**
- **7.1.2.4 Equipment and assets located outside physical secured areas**
- **7.1.2.5 Secure disposal or re-use of equipment**
- **7.1.2.6 Learning from security incidents**
- **7.1.2.8 Secure development environment and procedures**
- **7.1.2.9 Security of IoT systems in support of safety**
- **7.1.2.10 Security in connecting varied IoT devices**
- **7.1.2.11 Verification of IoT devices and systems design**
- **7.1.2.12 Monitoring and logging**
- **7.1.2.13 Protection of logs**
- **7.1.2.14 Use of suitable networks for the IoT systems**
- **7.1.2.15 Secure settings and configurations in delivery of IoT devices and services**
- **7.1.2.16 User authentication**
- **7.1.2.17 Provision of software and firmware updates**
- **7.1.2.18 Sharing vulnerability information**
- **7.1.2.19 Security measures adapted to the lifecycle of IoT system and services**
- **7.1.2.20 Guidance for IoT users on the proper use of IoT devices and services**
- **7.1.2.21 Determination of security roles for stakeholders**
- **7.1.2.22 Management of vulnerable devices**
- **7.1.2.23 Management of supplier relationships in IoT security**
- **7.1.2.24 Information security in IoT devices**

Security controls for IoT user

4 controls

- **7.1.3.1 Contacts and support service**
- **7.1.3.2 Initial settings of IoT device and service**
- **7.1.3.3 Deactivate unused devices**
- **7.1.3.4 Secure disposal or re-use of IoT device**

Privacy controls in ISO/IEC 27400

Privacy controls for IoT service developer and IoT service provider 14 controls

7.2.2.1 Prevention of privacy invasive events

7.2.2.2 IoT privacy by default

7.2.2.3 Collection and use of personal data

7.2.2.4 Verification of IoT functionality

7.2.2.5 Consideration of IoT users

7.2.2.6 Management of IoT privacy controls

7.2.2.7 Unique device identity

7.2.2.8 Fail-safe authentication

7.2.2.9 Minimization of indirect data collection

7.2.2.10 Communication of privacy preferences

7.2.2.11 Verification of automated decision

7.2.2.12 Accountability for stakeholders

7.2.2.13 Unlinkability of PII

7.2.2.14 PII protection in IoT devices

Privacy controls for IoT user 3 controls

7.2.3.1 User consent

7.2.3.2 Connecting with other devices and services

7.2.3.3 Certification/validation of PII protection

Example 7.1.2.10 Security in connecting varied IoT devices

Control-10

An IoT system should be designed and implemented to ensure and maintain security in connecting varied IoT devices.

Purpose

To maintain security of IoT system in connecting varied IoT devices including those not necessarily verified by the IoT service developer or the IoT service provider.

Guidance

…

The IoT service developer and the IoT service provider should design and implement secure IoT system which is prepared for the situation. The IoT system can have the following capabilities as necessary:

a) selectively connect the IoT device using a whitelist; or
b) where applicable, obtain the specifications of the device, e.g., name of provider, model, year of production and conformance to relevant standard, when negotiating with the device for connection, and determine if the connection request is accepted or rejected, or confine the scope of function, service or information to be made available.

ISO/IEC 27402 – FDIS

- **Title: Cybersecurity – IoT security and privacy – Device baseline requirements**

- Scope

This document provides baseline requirements for IoT devices and their developers to support security and privacy controls.

Excluding any of the requirements specified in 5.1 is not acceptable when an organization claims conformity to this document.

Note:
This figure is depicted from "introduction" of ISO/IEC 27402

Security Baseline Requirements in ISO/IEC 27402

5 Requirements

5.1 Requirements for IoT device developers
- 5.1.1 Risk management
- 5.1.2 Information disclosure
- 5.1.3 Vulnerability disclosure and handling processes

5.2 Requirements for IoT devices
- 5.2.1 General
- 5.2.2 Configuration
- 5.2.3 Software reset
- 5.2.4 User data removal
- 5.2.5 Protection of data
- 5.2.6 Interface access
- 5.2.7 Software and firmware updates
- 5.2.8 User notifications

ISO/IEC 27403 – DIS

- **Title: Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics**
- Scope

This document provides guidelines to analyse security and privacy risks and identifies controls that need to be implemented in IoT-domotics systems.

Note:

IoT-domotics:

IoT system composed of networks, devices, services and users typically used in the domicile or as electronic wearables

ISO/IEC 27404 – WD2

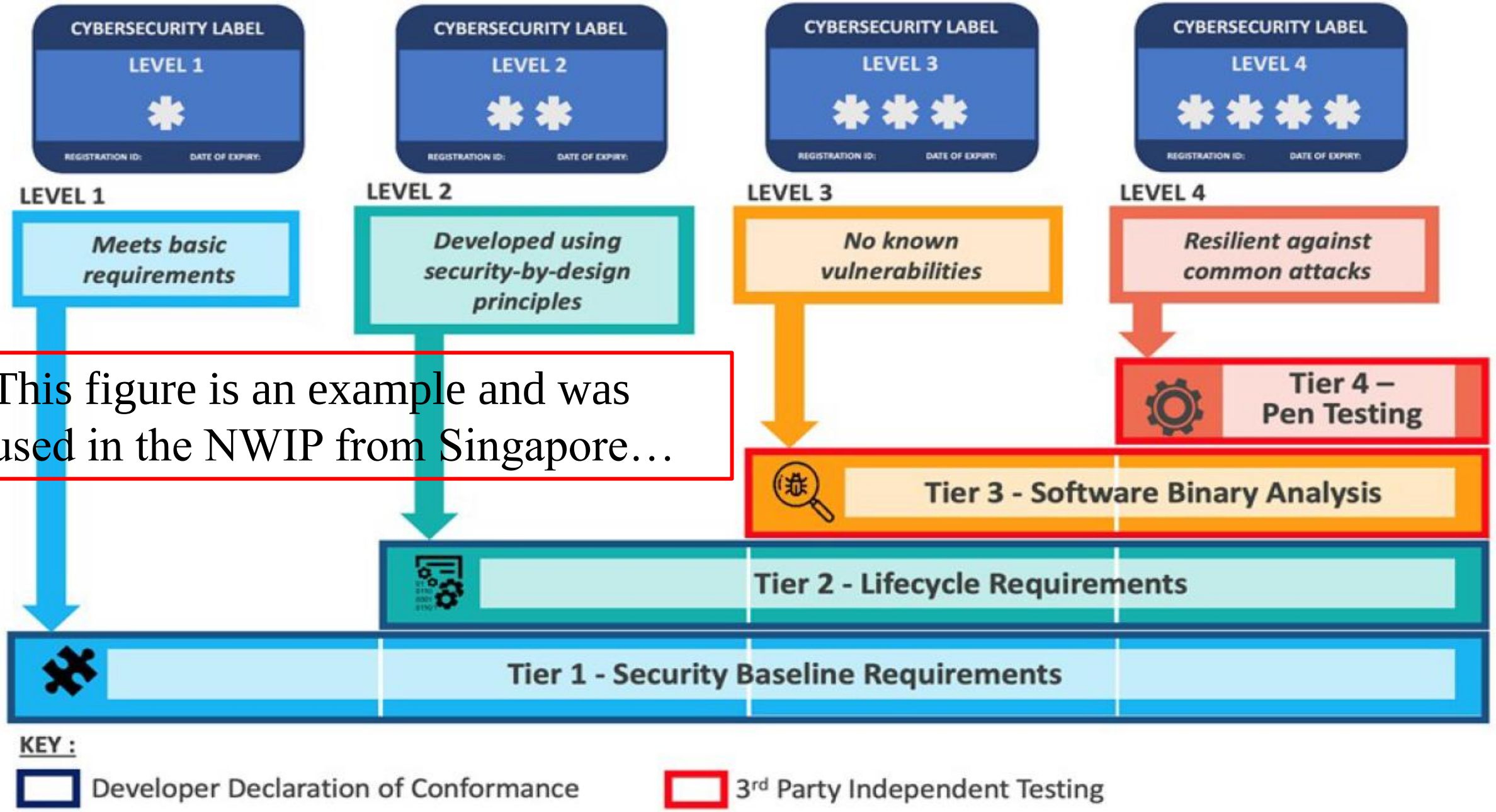
- **Title: Information technology — Security techniques — Cybersecurity labelling framework for consumer IoT**

- Scope

This document defines a cybersecurity labelling framework for the development and implementation of cybersecurity labelling programmes for consumer IoT products and includes guidance on the following topics:

- Risks and threats associated with consumer IoT products;
- Stakeholders, roles and responsibilities;
- Relevant standards and guidance documents;
- Conformity assessment options;
- Labelling issuance and maintenance requirements; and
- Mutual recognition considerations.

The scope of this document is limited to consumer IoT products, such as IoT gateways, base stations and hubs to which multiple devices connect; smart cameras, televisions, and speakers; wearable health trackers; connected smoke detectors, door locks and window sensors; connected home automation and alarm systems, especially their gateways and hubs; connected appliances, such as washing machines and fridges; smart home assistants; and connected children's toys and baby monitors. …..



This figure is an example and was used in the NWIP from Singapore…

Figure 1 — Levels of universal labelling framework and assessment tiers

Approach to global standardization of IoT security

ISO/IEC JTC1/SC27
27400, 27402 (FDIS), and 27404 (WD)

US – CTIA
IoT Cybersecurity Certification,
SP 800-213(NIST)
IoT Device Cybersecurity Guidance for the Federal Government

Common parts
- Terminologies
- Reference Architecture
- Use Cases
- Certification Framework

- Risk Analysis
- Security/Privacy Controls

UK – IASME IoT Cyber Scheme, etc
EU – ETSI, Cyber Security for Consumer IoT: Baseline Req. EN 303 645
EU – ENISA Cybersecurity Certification - EUCC Candidate Scheme

Japan – CPSF (METI), Device Requirements (MIC), IoT device Certification Scheme (under study), etc.

WG 4 Projects 8/11

AI and big data security and privacy	
ISO/IEC 20547-4:2020	Big data reference architecture — Part 4: Security and privacy
ISO/IEC 27045 [PWI]	Big data security and privacy — Processes
ISO/IEC 27046 [CD]	Big data security and privacy — Implementation guidelines
ISO/IEC 27090 [WD4]	Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems
ISO/IEC 5181 [WD]	Information technology – Security and privacy – Data provenance
ISO/IEC 6109 [PWI]	Guidelines for data security monitoring based on logging (Proposed title)
ISO/IEC TS 7709 [PWI]	Security and privacy-preserving guidelines for multi-sourced data processing

- Base documents of SC 42 “Artificial intelligence”
  - ISO/IEC FDIS 22989:2022, Artificial intelligence — Artificial intelligence concepts and terminology
  - ISO/IEC 20546:2019, Big data — Overview and vocabulary
  - ISO/IEC 20547-3:2020, Big data reference architecture — Part 3: Reference architecture

WG 4 Projects 9/11

Cloud computing security and privacy	
ISO/IEC 19086, Part 4:2019	Cloud computing — Service level agreement (SLA) framework — Part 4: Components of security and of protection of PII

- Base documents of SC 38 “Cloud computing and distributed platforms”
  - ISO/IEC 19086, Cloud computing — Service level agreement (SLA) framework
    Part 1: Overview and concepts
    Part 2: Metric model
    Part 3: Core conformance requirements

WG 4 Projects 10/11

Security in virtualization technologies	
ISO/IEC 21878:2018	Security guidelines for design and implementation of virtualized servers
ISO/IEC 27070:2021	Requirements for establishing virtualized roots of trust
ISO/IEC 27071 [IS]	Security recommendations for establishing trusted connections between devices and services

WG 4 Projects 11/11

Other projects for emerging areas	
ISO/IEC 13133 [PWI]	Information technology – Security techniques – Security reference model for digital currency hardware wallet
ISO/IEC 17603 [PWI]	Information security – Security techniques – Confidential computing

PWI 5689 – NP ISO/IEC TS 5689

Title: Cybersecurity –Security frameworks and use cases for cyber physical systems

Scope

This document provides the followings:

CPS conceptual model and its specific characteristics

- a conceptual model of cyber-physical systems (CPS) and its general features;
- specific characteristics of CPS compared to other related concepts;

Concerns and security frameworks

- security concerns as the basis for the discussion of security risks and security controls for the CPS based on the conceptual model;
- several security frameworks to address those security concerns;

Practical use cases for CPS

- use cases based on the respective security frameworks for CPS;
- provision of visibility of use cases into the specific use of the security frameworks, etc.

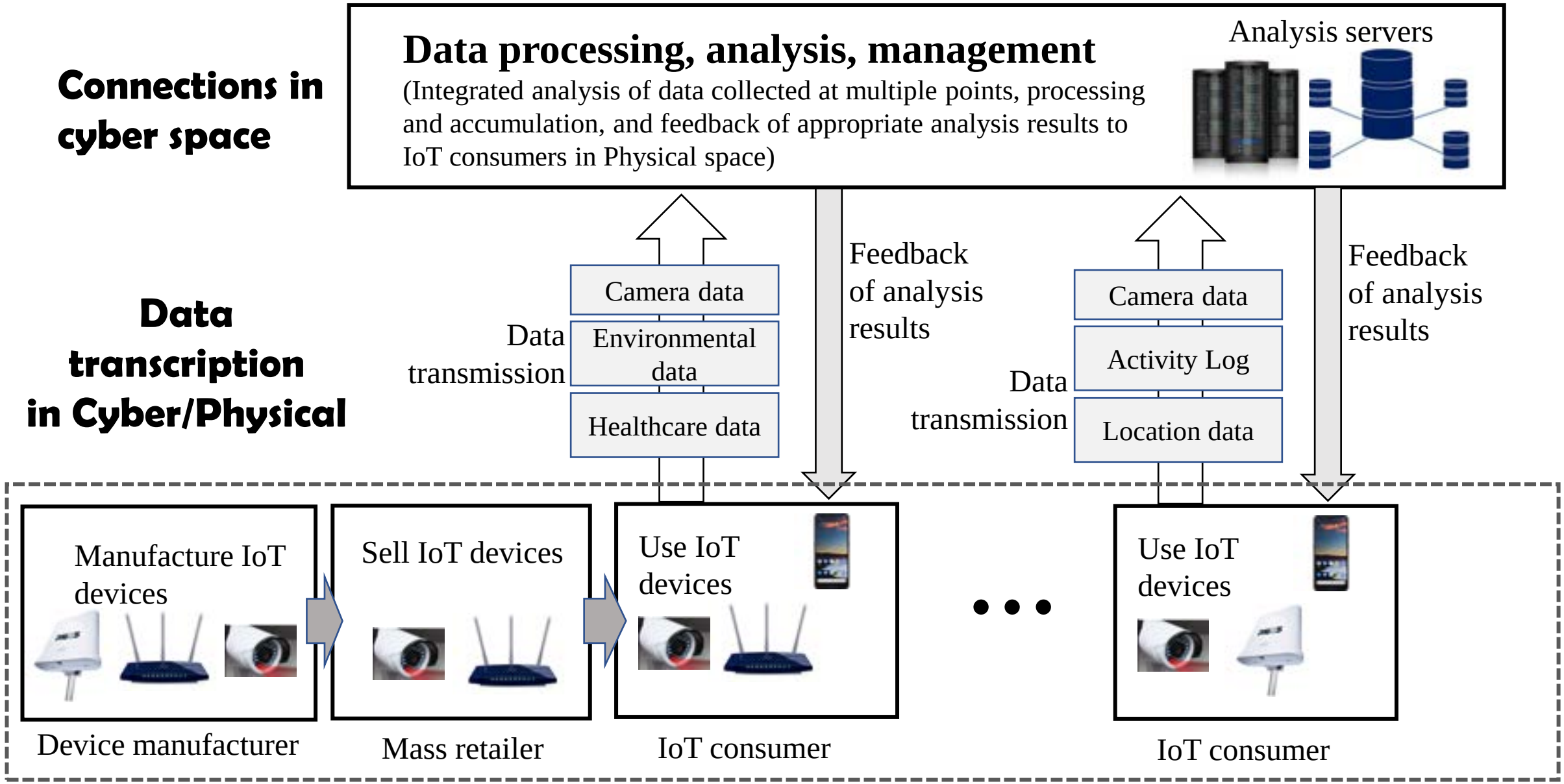


Fig.1 Conceptual Model of CPS (This is not included in the text of 5689)

Figure 3. An example of 3-tier conceptual model with 3 cyber physical systems

The Third Layer

(Connections in cyberspace)

Trustworthiness of data is a key for secured products and services

The Second Layer

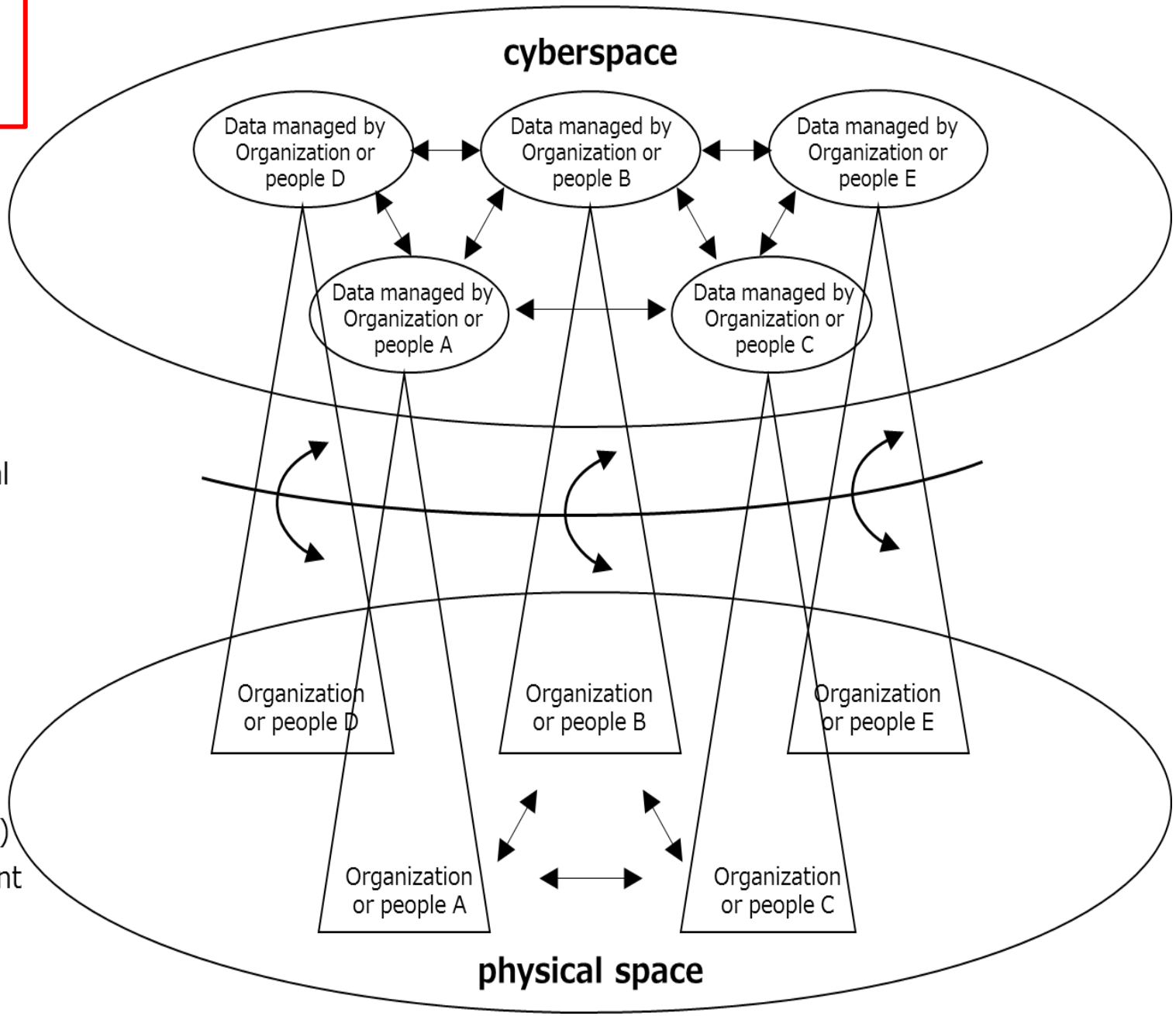
(Mutual connections between cyber & physical space)

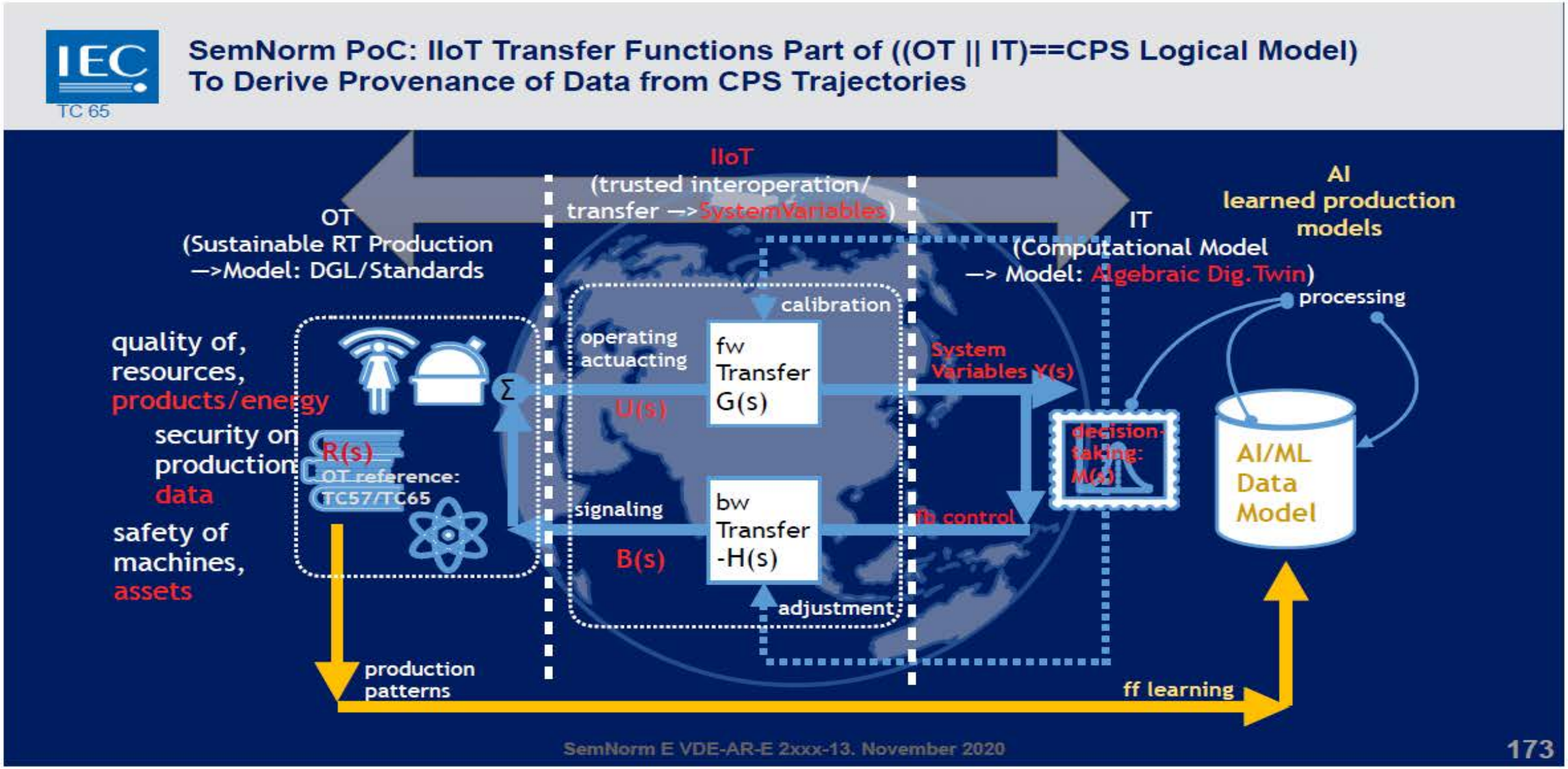
Trustworthiness of "transcription" is a key for normal operation of cyber-physical systems

The First Layer

(Connections among Organizations or people)

Trustworthiness of organization's management is a key for secured products and services

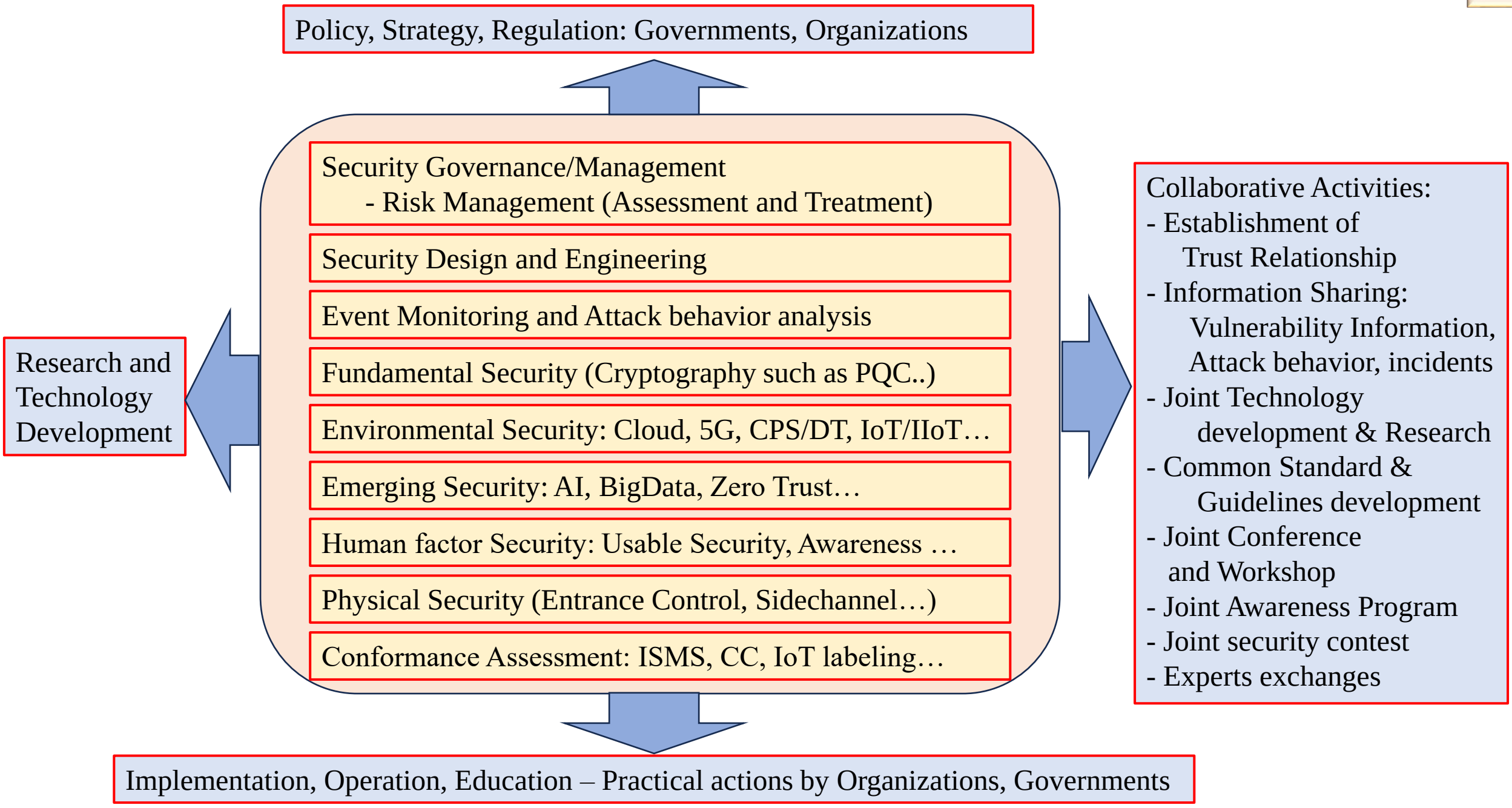




Another Application of CPS framework (will be described in 7.3)

IoT Security Solutions with IoT various stages

1. Security for IoT devices prior to shipment
   ISO/IEC 27400, 27402, 27404, etc.
2. Security Design of IoT system before operation
   ISO/IEC 27400, etc.
3. Security of IoT system (devices) in use (in operation)
   Finding Vulnerable IoT devices, ISO/IEC 27400, etc.
4. IoT system out of life-time
   ISO/IEC 27400, 27402, etc.


Policy, Strategy, Regulation: Governments, Organizations
Security Governance/Management
- Risk Management (Assessment and Treatment)
Security Design and Engineering
Event Monitoring and Attack behavior analysis
Fundamental Security (Cryptography such as PQC..)
Environmental Security: Cloud, 5G, CPS/DT, IoT/IIoT…
Emerging Security: AI, BigData, Zero Trust…
Human factor Security: Usable Security, Awareness …
Physical Security (Entrance Control, Sidechannel…)
Conformance Assessment: ISMS, CC, IoT labeling…
Research and Technology Development
Collaborative Activities:
- Establishment of Trust Relationship
- Information Sharing: Vulnerability Information, Attack behavior, incidents
- Joint Technology development & Research
- Common Standard & Guidelines development
- Joint Conference and Workshop
- Joint Awareness Program
- Joint security contest
- Experts exchanges
Implementation, Operation, Education – Practical actions by Organizations, Governments

Conclusion

1. IoT is not limited to IoT devices. There are various implementation forms as IoT systems and their combinations. Further, its applications in 5G, CPS / DT, smart city, etc. are being actively considered worldwide.
2. With the above environments, ensuring “cybersecurity” is an urgent issue.
3. In this context, active information sharing among ASEAN countries and JP can be an extremely effective means of countermeasures:
   - Sharing is a risk management activity
     - You can get (and provide) early warnings by sharing
   - Collaboration can reduce the cost of defense
     - You can identify actors and threats that you may not have been tracking
   - By sharing information, you can help your suppliers, partners and competitors secure their enterprises
4. Not only sharing information, following activities can also be expected among ASEAN-JP:
   - Improving risk management based on the related standards for new environments such as CPS
   - Joint Research activities: establish a good scheme for the joint research and development and the results can be shared and utilized for each country.
   - Continuous information exchange like this event should be held periodically.

Thank you for listening