

# Abstract of the General Framework for Secured IoT Systems (Draft)

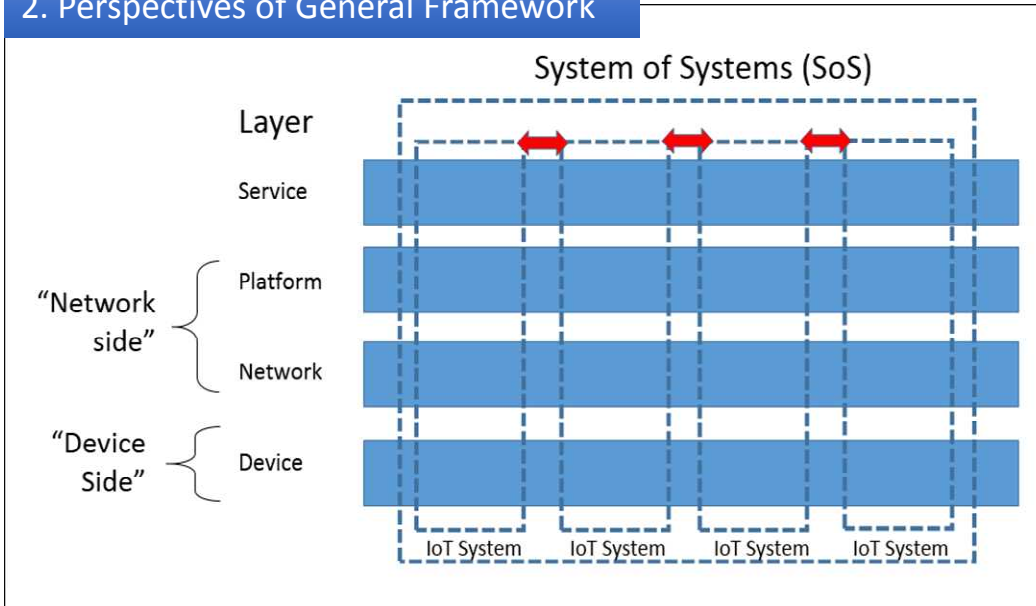
## 1. The Object of the General Framework

### a) Two-Pronged approach

- 1 Clarifying general requirements at each stage of design, development and operation for all IoT systems
- 2 Sector-specific requirements should be added

### b) Clarifying fundamental and essential security requirements for secured IoT systems

## 2. Perspectives of General Framework



## 3. Basic Principles

- a) **Definitions** (including the diversity and the scope) of IoT systems shall be determined and clarified. And also, those systems shall be categorized based on system's characteristics reflecting their inherent risks.
- b) **Essential requirements for ensuring users' safety** shall be determined as well as confidentiality, integrity and availability
- c) **Essential requirements** shall be determined to ensure secured system operation and service resilience in case of system failure, including rules of mission assurance.
- d) **Safety assurance standards, including statutory and customary requirements**, shall be determined for connected things and networks.
- e) Each item from a) to d) above shall be ensured in case of mechanical failure or cyber-attacks.
- f) **Responsibility boundary and information ownership** of IoT systems shall be clarified. Items from a) to f) should be applied to the requirements for other cases such as interconnection of IoT systems.

## 4. Policy Approaches

- a) **Determination of Requirements**
  - Structures, systems and components (SSC's) as well as statutory and regulatory requirements
- b) **Risk Informed Approach**
  - Security measures and implementation means shall be adopted
- c) **Proper application of performance requirements and specific requirements**
- d) **Step-by-step and continuous approach** depending on technological innovation
- e) **Collaboration and determination** of the role-sharing
  - Demarcation of responsibility between each stakeholder
- f) Consideration of other operational rules
  - Protecting personally identifiable information
  - Clarification of certification entities

## 5. Notes

- This framework is described based on IoT systems envisaged at the current stage.
- necessity for preview and update in response to the factors such as advancement of functions of IoT systems along with technological innovation
  - should be revised with reflecting opinions and discussions of multi-stakeholders