FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC/IEEE FDIS 24748-9

ISO/IEC JTC **1**/SC **7**

Secretariat: **BIS**

Voting begins on:
2023-02-17

Voting terminates on:
2023-04-14

Systems and software engineering — Life cycle management —

Part 9: Application of system and software life cycle processes in epidemic prevention and control systems

Reference number
ISO/IEC/IEEE FDIS 24748-9:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Institute of Electrical and Electronics Engineers, Inc
3 Park Avenue, New York
NY 10016-5997, USA

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO/IEC documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

ISO/IEC/IEEE 24748-9 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*, in cooperation with the Systems and Software Engineering Standards Committee of the IEEE Computer Society, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE.

A list of all parts in the ISO/IEC/IEEE 24748 series can be found on the ISO and IEC website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Many areas have adopted information-based prevention and control measures during an epidemic and have developed numerous epidemic prevention and control systems and software. Most of the processes in the entire life cycle of the epidemic prevention and control systems are likely to be completed in the event of an epidemic. Compared with the normal state, there can be special situations such as poor communication, caused by the need for personnel to maintain a safe distance, and limited transportation and logistics services. The result can be insufficient infrastructure protection, short delivery cycles, frequent iterative upgrades, and special requirements such as accuracy, disaster tolerance, degradation capability, safety, user capacity and stress testing, and rapid demand capture. In the development process of epidemic prevention and control systems, the application of the life cycle processes specified in ISO/IEC/IEEE 15288 and ISO/IEC/IEEE 12207 can effectively help guide the process management and application of epidemic prevention and control systems.

However, for effective and efficient application of system and software life cycle processes on epidemic prevention and control systems, additional application requirements are needed. Requirements specific to the use of the epidemic prevention and control systems that facilitate effective implementation depend on the nature and severity of the epidemic and are not detailed in this document.

This document is consistent with life cycle processes of ISO/IEC/IEEE 15288 or ISO/IEC/IEEE 12207 for application on epidemic prevention and control systems, to help ensure the correct application of stakeholders' requirements for epidemic prevention and control systems. This document includes the required outputs and associated attributes.

Systems and software engineering — Life cycle management —

Part 9: Application of system and software life cycle processes in epidemic prevention and control systems

1 Scope

This document provides requirements and guidance on the application of system and software engineering processes to systems for epidemic prevention and control.

This document provides guidance that can be employed for adopting and applying system and software life cycle processes within an organization or a project in an epidemic emergency. It includes system of systems considerations in the context of epidemic emergency.

This document applies to acquisition, supply, development, operation, maintenance, and disposal (whether performed internally or externally to an organization) of system or system of systems in an epidemic emergency.

Many of the requirements and recommendations in this document are also applicable to other systems developed rapidly to respond to emergency conditions affecting the public.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC/IEEE 12207:2017, *Systems and software engineering — Software life cycle processes*

ISO/IEC/IEEE 15288:—[1)], *Systems and software engineering – System life cycle processes*

ISO/IEC/IEEE 15289, *Systems and software engineering — Content of life-cycle information items (documentation)*

3 Terms, definitions, and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO, IEC, and IEEE maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

— IEEE Standards Dictionary Online: available at: https://dictionary.ieee.org

1) Under preparation.

NOTE For additional terms and definitions in the field of systems and software engineering, see ISO/IEC/IEEE 24765, which is published periodically as a “snapshot” of the SEVOCAB (Systems and software Engineering Vocabulary) database, and which is publicly accessible at www.computer.org/sevocab.

3.1.1
constituent system
CS
independent *system* (3.1.3) that forms part of a *system of systems (SoS)* (3.1.5)

Note 1 to entry: Constituent systems can be part of one or more SoS. Each constituent system is a useful system by itself, having its own development, management, utilization, goals, and resources, but interacts within the SoS to provide the unique capability of the SoS.

[SOURCE: ISO/IEC/IEEE 21839:2019, 3.1.1, modified — The abbreviated term "CS" has been added.]

3.1.2
emergency
serious, unexpected, and often dangerous situation requiring immediate action

3.1.3
system
arrangement of parts or elements that together exhibit a stated behaviour or meaning that the individual constituents do not

[SOURCE: ISO/IEC/IEEE 15288:—, 3.47]

3.1.4
system-of-interest
SoI
system (3.1.3) whose life cycle is under consideration

[SOURCE: ISO/IEC/IEEE 15288:—, 3.49]

3.1.5
system of systems
SoS
set of *systems* (3.1.3*)* and system elements that interact to provide a unique capability that none of the *constituent systems* (3.1.1) can accomplish on its own

Note 1 to entry: System elements can be necessary to facilitate interaction of the constituent systems in the system of systems.

[SOURCE: ISO/IEC/IEEE 21839:2019, 3.1.4]

3.2 Abbreviated terms

API	application program interface
CWBS	contract work breakdown structure
DT&E	developmental test and evaluation
ESOH	environment, safety, and occupational health
EVM	earned value management
FMECA	failure mode, effects, and criticality analysis
IMP	integrated main plan
IMS	integrated main schedule

IVS	intelligent vision systems
OpsCon	operational concept
PSA	product support analysis
QA	quality assurance
QPS	queries per second
RT	response time
SEMP	systems engineering management plan
SEP	systems engineering plan
SIP	system integration plan
TPS	transactions per second

4 Conformance

4.1 Intended usage

ISO/IEC/IEEE 15288:—, 4.1 or ISO/IEC/IEEE 12207:2017, 4.1 shall apply.

4.2 Full conformance

4.2.1 Full conformance to outcomes

ISO/IEC/IEEE 15288:—, 4.2.1 or ISO/IEC/IEEE 12207:2017, 4.2.1 shall apply with additional outcomes specified in Clause 6.

4.2.2 Full conformance to tasks

ISO/IEC/IEEE 15288:—, 4.2.2 or ISO/IEC/IEEE 12207:2017, 4.2.2 shall apply with additional tasks specified in Clause 6.

4.3 Tailored conformance

ISO/IEC/IEEE 15288:—, 4.3 or ISO/IEC/IEEE 12207:2017, 4.3 shall apply.

In the case of an epidemic, due to the rapid and serious development of the epidemic, the epidemic prevention and control system project should adopt a tailoring process.

5 Key concepts and application

5.1 General

ISO/IEC/IEEE 15288:—, 5.1 or ISO/IEC/IEEE 12207:2017, 5.1 shall apply with the following addition:

For epidemic prevention and control systems, more attention should be paid to the system and process characteristics in the context of an epidemic.

If the epidemic prevention and control system has many constituent systems (CS) and is complex enough to be regarded as a system of systems (SoS) or more than one SoS, then SoS considerations described in ISO/IEC/IEEE 21840 should be taken into account for system life cycle processes.

5.2 System concepts

5.2.1 System

This document refers specifically to systems that are developed, adapted, or deployed during epidemic emergencies, such as pandemics. The systems considered in this document are epidemic prevention and control physical systems, created and utilized to provide products or services in epidemic environments for the prevention and control of epidemics. Annex A includes examples of typical epidemic prevention and control systems. These systems can include the following system elements: hardware, software, data, humans, processes (e.g. processes for providing service to users), procedures (e.g. operator instructions), facilities, services, materials and naturally occurring entities. As viewed by the user, they are thought of as products or services. The systems can be considered as SoS. Clause 6 explains the specific tasks in processes, covering their development, augmentation, implementation, and other stages.

5.2.2 Characteristics of systems for epidemic emergency

5.2.2.1 Joint missions

To bring additional resources to system development, to meet the needs of multiple stakeholders, and to improve interoperability and information sharing, multiple organizations often engage in joint missions during an epidemic emergency. Joint missions can perform system conceptualization, development, implementation, and operation. The goal of joint missions is to share knowledge on epidemic response and preparedness measures implemented in infected regions or countries and to generate recommendations for adjusting epidemic containment and response measures. The system architecture and requirements for components such as database, data sharing, information exchange, system docking using API for external calls, and programming languages should be considered in this context.

EXAMPLE The systems can allow multiple hospitals to share their patient condition status and remaining acceptable capabilities for patients' infectious disease data, used to determine hospital vehicles and patients requiring appropriate care.

5.2.2.2 Infrastructure protection

Infrastructure and facilities are the essential basis for system operation, especially in the context of an epidemic emergency. However, due to the need for epidemic containment, people can suffer social activity limitations and constraints. Thus, transportation and logistics of the supply chain do not work normally, which results in insufficient facilities supply and inadequate infrastructure protection. In this case, the availability and reliable performance related to the epidemic prevention and control system can be greatly affected. An emergency mechanism and solution should be clarified and established.

5.2.2.3 Strengthened data analysis and visualization functions

Systems and methods for visualization of data analysis are valuable to support rapid decision-making based on evidence. In data analysis, generation of descriptive statistics, exploratory data analysis, and confirmatory data analysis methods are utilized. A method comprises accessing a database, analysing the database to identify clusters of data, and generating an interactive visualization, which is used for better risk assessment and decision-making.

In the context of an epidemic emergency, the data analysis of the epidemic prevention and control system and visualization methods should be strengthened, to better present the comprehensive and different dimensions of the epidemic, support epidemic prevention, and control decision-making.

NOTE The D7-R4 method can be applied in case of IVS related processes. D7-R4 stands for a software development life cycle model with seven stages (i.e. discover, dig, describe, design, develop, demonstrate, and deploy) and reviews from four different perspectives (i.e. quality, user/agent experience, ethics, and security).

5.2.2.4 Adequate performance efficiency consideration

For an epidemic prevention and control system, performance efficiency requirements should be considered. Some scenarios can require real-time response. For example, consistent with data privacy regulations, health QR code applications can be used to start an application; biometric recognition such as facial recognition can be used for user authentication for the doctors; infrared temperature measurement can be used for the clients. For load-balancing in an epidemic emergency, a capacity planning process is developed, in which the full-scale stress test is key to ensuring smooth operations. The process stage includes pre-system machine capacity estimation, full-scale stress testing, and traffic control. During the tests, consideration of the parameters should be taken, for instance, TPS, QPS, RT and the number of concurrent users.

NOTE Performance efficiency can be identified as a quality characteristic, including time efficiency and resource efficiency, which are prescribed in ISO/IEC 25010.

5.2.2.5 System resilience capabilities

The system should be capable of working in an unstable environment during an epidemic emergency. In this case, a system resilience plan should be considered in the concept stage. The system should achieve the following capabilities for system resilience.

— In case that internet is not available, the communication should work through other available systems or even through manual ways.

— Key information should be displayed as a priority during poor internet connection.

— Data should be transmitted by other protocols, e.g. Bluetooth.

5.2.2.6 Disaster recovery capacity

Along with a disaster recovery system, preventive measures should be implemented to avoid crisis situations that have the potential to cause irreparable damage and close down operations indefinitely. Disaster recovery is normally achieved through procedures that backup and restore data, systems, and applications from different locations.

During an epidemic emergency, the systems should be able to function in a decentralized manner, without one central owner. Instead, they use multiple central owners, each of which usually stores a copy of the resources which users can access. For instance, a local health QR code is capable of accessing service by decentralized systems.

5.2.2.7 Balancing trade-offs between privacy protection or security and information transparency

Epidemics have created opportunities for greater transparency through the proactive release of information which can help the containment of disease. However, release of information is contradictory to and imposes risk to the public's data privacy and security.

For protecting data privacy, back deduction by algorithm to personal identification and encryption keys is not allowed. In practice, the real-time infected data should not be provided to the general public.

Data security refers to the process of protecting data from unauthorized access and data corruption throughout the system life cycle. Data security includes data encryption, hashing, tokenization, and key management practices that protect data across all applications and platforms. During an epidemic emergency, sensitive information, for instance personal information, motion trajectory, or close contact, should be handled properly with a firewall security module and multi-level permissions for developers.

5.2.2.8 Data correctness

In an emergency there can be a trade-off between timeliness of data collection and correctness (accuracy) of data. For example, infected persons may be requested to give data about private activities during the past several days, including health status parameters, living place, and visited locations. Correct personal detailed data is useful to find the possible route of infection spread. In some cases, it possibly accelerates emergent prevention actions during an infection, increasing the probability of identifying infected people including pseudo infection. However, over time more correct information should be obtained or verified, enabling users to distinguish between actual infections, non-symptomatic carriers, and increases in severity of cases.

Eventually, the verification of individual infection is based on medical evidence. When the infection data is transmitted, the coverage range and correctness should be predicted. Consideration should also be given to the accuracy and interpretation of predicted data from machine learning systems.

Compared with the value of real-time information transmission, the accuracy of information is more important.

NOTE Data correctness is related to data quality characteristics which are prescribed in ISO/IEC 25012.

5.2.2.9 Reduced misalignment of incentives

Misaligned incentives refer to situations where the conflicting incentives of the stakeholder, developer or practitioner involved in life cycle processes hamper achievement of a common intended goal of a system. Putting specific interests ahead of common system interests can turn planned cooperation into opposition and produce poor outcomes, including the failure of epidemic prevention and control. Two of the most common types of misaligned incentives are those in which either a system element's interests are traded off against the system's interests, or long-term interests are traded off against short-term interests.

5.2.3 System structure

ISO/IEC/IEEE 15288:—, 5.2.2 or ISO/IEC/IEEE 12207:2017, 5.2.2 shall apply with the following addition:

The epidemic prevention and control physical system is a complex SoI or SoS, a system element of which can itself be considered as a system, which can comprise the natural system, the governance system, the health system, the logistic system, and the human ecosystem, respectively. Figure 1 illustrates the structure of an epidemic decision system information model, which can be either an SoI or an SoS.

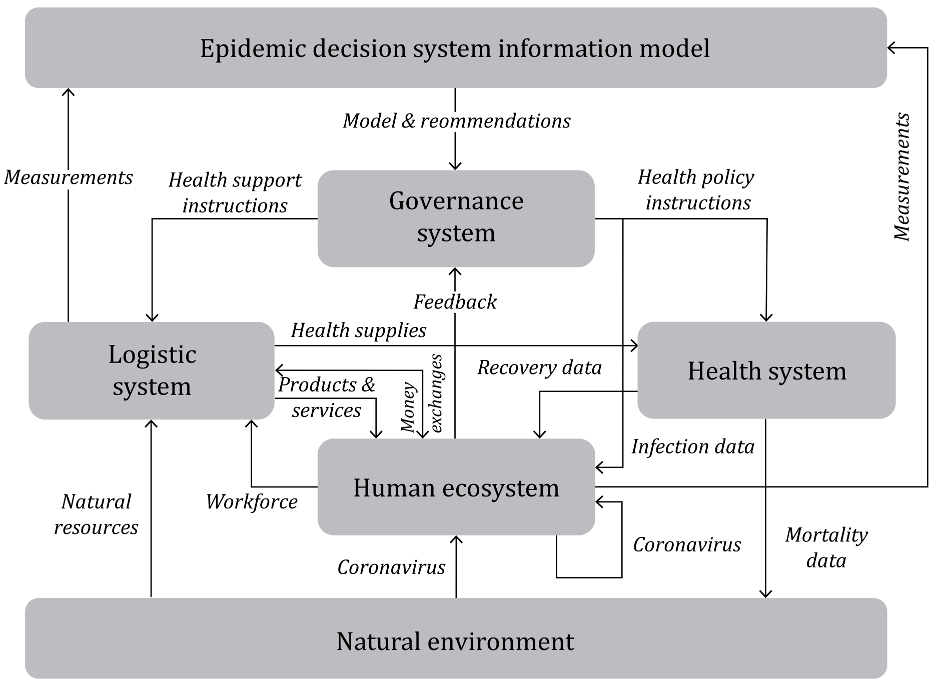

Figure 1 — Structure of epidemic decision system information model

5.2.4 Interfacing, enabling, and interoperating systems

ISO/IEC/IEEE 15288:—, 5.2.3 shall apply.

5.2.5 Concepts related to the system solution context

ISO/IEC/IEEE 15288:—, 5.2.4 shall apply.

5.2.6 Product line engineering (PLE)

ISO/IEC/IEEE 15288:—, 5.2.5 shall apply.

5.3 Organization and project concepts

5.3.1 Organizations

ISO/IEC/IEEE 15288:—, 5.3.1 or ISO/IEC/IEEE 12207:2017, 5.3.1 shall apply.

5.3.2 Organization and project-level adoption

ISO/IEC/IEEE 15288:—, 5.3.2 or ISO/IEC/IEEE 12207:2017, 5.3.2 shall apply.

5.3.3 Organization and collaborative activities

ISO/IEC/IEEE 15288:—, 5.3.3 shall apply.

5.4 Life cycle concepts

5.4.1 System life cycle model

ISO/IEC/IEEE 15288:—, 5.5.1 or ISO/IEC/IEEE 12207:2017, 5.4.2 shall apply.

5.4.2 System life cycle stages

ISO/IEC/IEEE 15288:—, 5.5.2 or ISO/IEC/IEEE 12207:2017, 5.4.1 shall apply. Figure 2 illustrates the interrelationship of the life cycle processes described in this document.

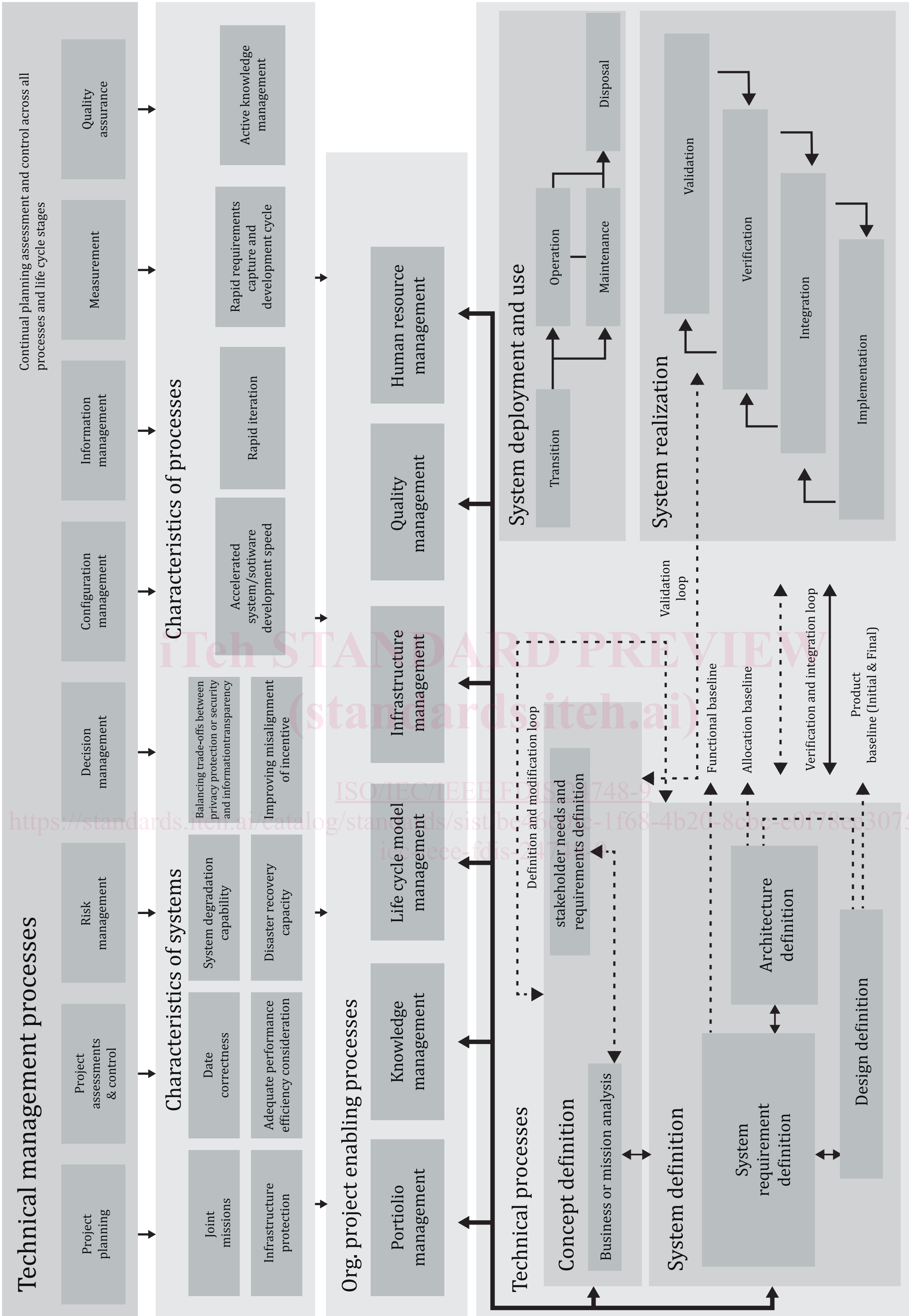

Figure 2 — Interrelationship among processes and system characteristics during an epidemic emergency

5.5 Process concepts

5.5.1 Criteria for processes

ISO/IEC/IEEE 15288:—, 5.6.1 or ISO/IEC/IEEE 12207:2017, 5.5.1 shall apply.

5.5.2 Description of processes

ISO/IEC/IEEE 15288:—, 5.6.2 or ISO/IEC/IEEE 12207:2017, 5.5.2 shall apply with the following addition:

For the application of the epidemic prevention and control systems, each process includes software engineering outputs with attributes. The output shall meet the requirements of ISO/IEC/IEEE 15289.

5.5.3 General characteristics of processes

ISO/IEC/IEEE 15288:—, 5.6.3 or ISO/IEC/IEEE 12207:2017, 5.5.3 shall apply.

5.5.4 Characteristics of life cycle processes for epidemic emergency systems

5.5.4.1 Active knowledge management

System development is a knowledge-intensive activity and its success depends heavily on the developers' knowledge and experience. Especially during an epidemic emergency, inter-disciplinary knowledge is valuable, including system and software, health and medical care, and emergency management.

5.5.4.2 Rapid requirements capture and development cycles

Epidemic changes are usually unpredictable and relatively rapid, which leads to corresponding changes and adjustments in the requirements and definitions of epidemic prevention and control systems. Therefore, rapidly changing requirements are repeatedly captured and modified; and short development cycles are utilized. System development teams attempt to deliver new and modified capabilities in a short timeframe. The short development cycle should follow the guidelines in this document to avoid or minimize system defects and gaps. This kind of situation is challenging for a supplier or system development teams who want to keep up with a fast-paced, ever-changing epidemic emergency.

5.5.4.3 Accelerated system/software development speed

This document aims to deliver guidance for fast system/software construction in quick response to an epidemic emergency. System development should be accelerated to achieve fast and responsive results. Optimization of the processes can use advanced methodologies such as agile development. It supports fast, iterative system/software development that allows developers to fine-tune features in response to feedback.

The new features require careful design, tested development, and thorough testing. The importance of meeting the deadline compromises each process and can result in an extremely fragile application. Thus, the centralized leadership team has to find strategies to maintain the balance between speed and quality. Those strategies can include in-process control and in-use improvement.

5.5.4.4 Rapid iteration

Iterative development is a way of breaking down the system development of a large application into smaller chunks. In iterative development, feature code is designed, developed, and tested in repeated cycles. For each iteration, additional features can be designed, developed, and tested until there is a fully functional system application ready to be in deployment phase. In the context of an epidemic emergency, the rapid change of the epidemic situation and the consequent demand can require frequent iteration of the emergency prevention and control system. The purpose of working iteratively is to allow more flexibility for changes in response to an epidemic emergency.