INTERNATIONAL STANDARD

ISO/ IEC/IEEE 24748-9

First edition
2023-05

Systems and software engineering — Life cycle management —

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

Ingénierie des systèmes et du logiciel — Gestion du cycle de vie —

Partie 9: Application des processus du cycle de vie des systèmes et du logiciel dans les systèmes de prévention et de lutte contre les épidémies

Reference number
ISO/IEC/IEEE 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 15288:2023, *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

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 15288:2023, 3.47]

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

[SOURCE: ISO/IEC/IEEE 15288:2023, 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 15288:2023, 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 15288:2023, 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 15288:2023, 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 15288:2023, 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 15288:2023, 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 15288:2023, 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.

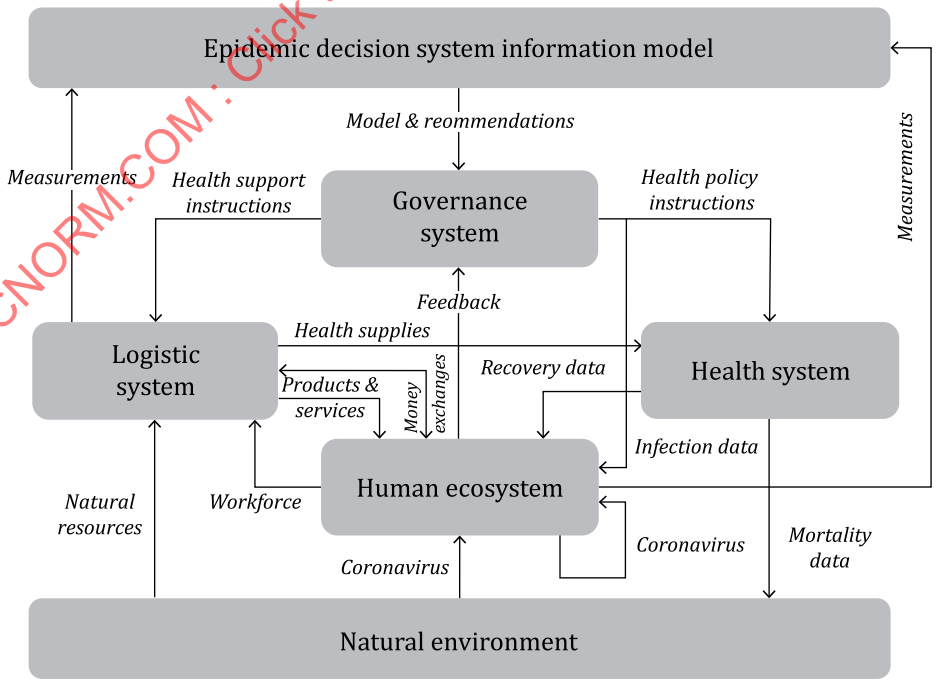

Figure 1 — Structure of epidemic decision system information model

5.2.4 Interfacing, enabling, and interoperating systems

ISO/IEC/IEEE 15288:2023, 5.2.3 shall apply.

5.2.5 Concepts related to the system solution context

ISO/IEC/IEEE 15288:2023, 5.2.4 shall apply.

5.2.6 Product line engineering (PLE)

ISO/IEC/IEEE 15288:2023, 5.2.5 shall apply.

5.3 Organization and project concepts

5.3.1 Organizations

ISO/IEC/IEEE 15288:2023, 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 15288:2023, 5.3.2 or ISO/IEC/IEEE 12207:2017, 5.3.2 shall apply.

5.3.3 Organization and collaborative activities

ISO/IEC/IEEE 15288:2023, 5.3.3 shall apply.

5.4 Life cycle concepts

5.4.1 System life cycle model

ISO/IEC/IEEE 15288:2023, 5.5.1 or ISO/IEC/IEEE 12207:2017, 5.4.2 shall apply.

5.4.2 System life cycle stages

ISO/IEC/IEEE 15288:2023, 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.

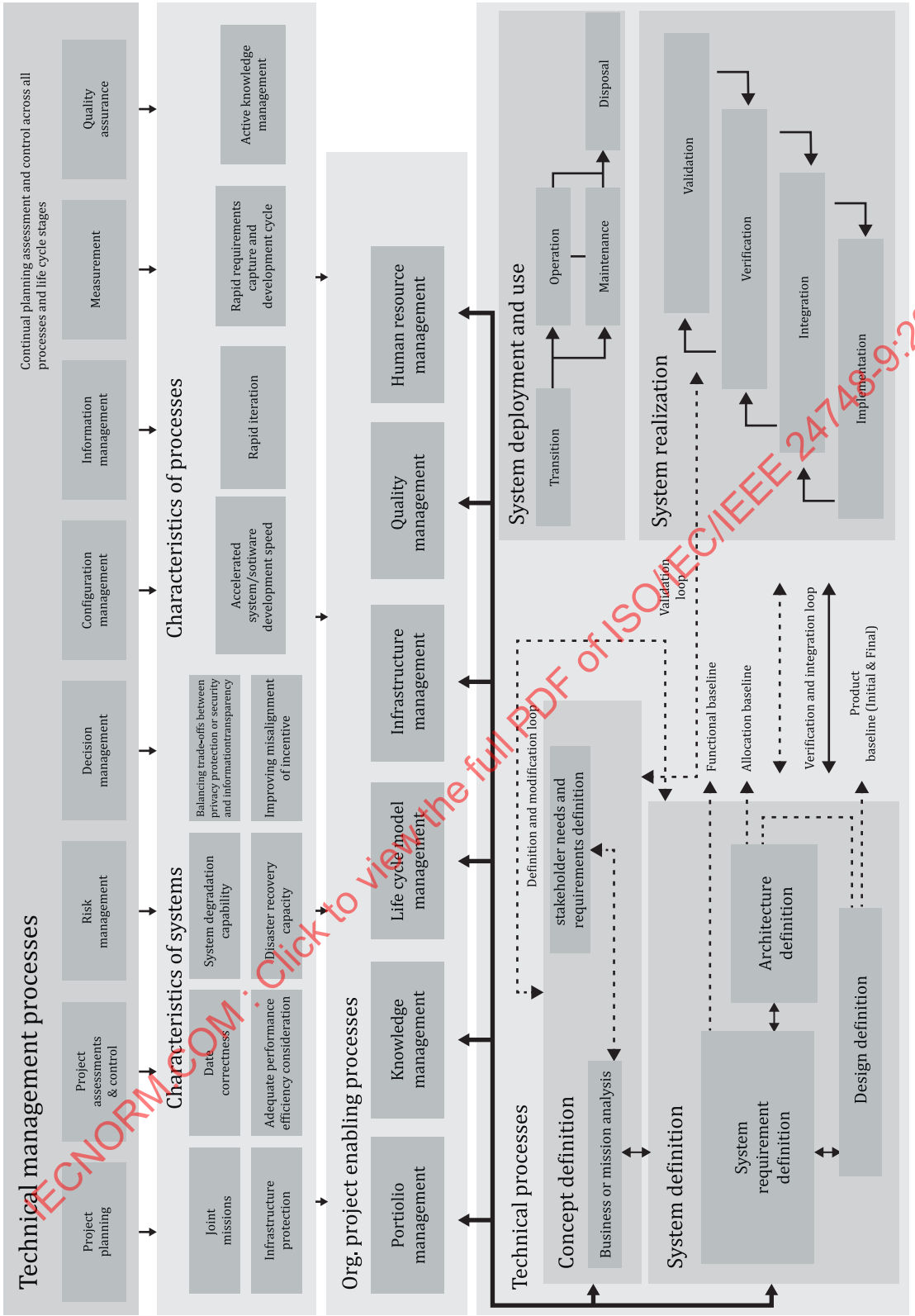

Figure 2 — Interrelationship among processes and system characteristics during an epidemic emergency

5.5 Process concepts

5.5.1 Criteria for processes

ISO/IEC/IEEE 15288:2023, 5.6.1 or ISO/IEC/IEEE 12207:2017, 5.5.1 shall apply.

5.5.2 Description of processes

ISO/IEC/IEEE 15288:2023, 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 15288:2023, 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.

5.6 Processes in this document

5.6.1 General

ISO/IEC/IEEE 15288:2023, 5.7.1 or ISO/IEC/IEEE 12207:2017, 5.6.1 shall apply.

5.6.2 Agreement processes

ISO/IEC/IEEE 15288:2023, 5.7.2 or ISO/IEC/IEEE 12207:2017, 5.6.2 shall apply.

5.6.3 Organizational project-enabling processes

ISO/IEC/IEEE 15288:2023, 5.7.3 or ISO/IEC/IEEE 12207:2017, 5.6.3 shall apply.

5.6.4 Technical management processes

ISO/IEC/IEEE 15288:2023, 5.7.4 or ISO/IEC/IEEE 12207:2017, 5.6.4 shall apply.

5.6.5 Technical processes

ISO/IEC/IEEE 15288:2023, 5.7.5 or ISO/IEC/IEEE 12207:2017, 5.6.5 shall apply.

5.7 System-of-interest concepts

5.7.1 General

The perception and definition of a particular system, its architecture, and its elements depend on a stakeholder's interests and responsibilities. One stakeholder's system-of-interest can be viewed as a system element in another stakeholder's system-of-interest. Furthermore, a system-of-interest can be viewed as being part of the environment for another stakeholder's system-of-interest.

The following are key points regarding the characteristics of systems-of-interest.

— Defined boundaries encapsulate meaningful needs and practical solutions.

— There is a hierarchical or other relationship between system elements.

— An entity at any level in the system-of-interest can be viewed as a system.

— A system comprises an integrated, defined set of subordinate system elements.

— Humans can be viewed as both users external to a system and as system elements (i.e. operators) within a system.

— A system can be viewed in isolation as an entity, i.e. as a product or as a collection of functions capable of interacting with its surrounding environment, i.e. a set of services.

The SoI concept in this document mainly refers to systems in the context of an epidemic emergency whose elements include relevant software, hardware, data, human, infrastructure, and processes, with enabling systems and other systems in the operational environment. Alternatively, hardware or services hosting the system and handling communications with other systems can be viewed as enabling systems or external systems in the operating environment.

5.7.2 Relationships between software and system

This document applies to epidemic prevention and control systems for which software is of primary importance to the stakeholders, since information-based measures can effectively and efficiently help contain infectious diseases. It is based upon the general principles of systems engineering and software engineering. However, it is a fundamental premise of this document that software always exists in the

context of a system. Since software does not operate without hardware, the processor upon which the software is executed can be considered as part of the system, or as an enabler of the software system.

Although software plays an essential role in the epidemic prevention and control aspect, epidemic prevention and control is a quite complex issue since it not only involves relevant hardware, humans, and facilities, but also directly relates to the social effect, economic effect, and other existing systems. From this point of view, the socio-technical system is the SoI, rather than only the software.

5.8 System of systems concepts

5.8.1 General

When the epidemic prevention and control system is complex enough and contains a set of CS, none of which can accomplish the goal of epidemic containment, for example, cross-region or cross-country systems, the SoI can be an SoS or multiple SoS.

An SoS is a set of systems and system elements that interact to provide a unique capability that none of the CS can accomplish on its own, something of great importance in an epidemic emergency. Each component system has its own management, objectives, and resources; and these systems are coordinated in the SoS to achieve the SoS objectives. The SoS is composed of the original SoI, the enabling system and the integrated system of interaction system.

An essential characteristic is that CS within the SoS are operationally independent. That is, the CS can (and do) operate independently to fulfil purposes on their own, separate from the SoS. While CS operate independently from each other for their own purposes, they also operate interdependently with each other and other elements to produce the SoS outputs. CS are never totally independent, yet they are also never totally subservient to the SoS.

Managerial independence suggests that the CS are likely to be managed by various health and other organizations that retain some degree of independence, even though they are interdependent while participating in an emergency response. The implication is that these organizations can have goals and objectives for the CS that differ from those of the SoS. If so, there is likely some degree of independence and interdependence of governance, as well as some degree of independence and interdependence of management.

5.8.2 Differences between systems and SoS

ISO/IEC/IEEE 15288:2023, 5.4.1 shall apply.

5.8.3 Managerial and operational independence

ISO/IEC/IEEE 15288:2023, 5.4.2 shall apply.

5.8.4 Taxonomy of SoS

ISO/IEC/IEEE 15288:2023, 5.4.3 shall apply.

5.8.5 SoS considerations in life cycle stages of a system

ISO/IEC/IEEE 15288:2023, 5.4.4 shall apply.

5.8.6 Epidemic prevention and control system as an SoS

Throughout this document, the relevant pieces of the SoI can be called subsystems, elements, or components. However, in the context of an epidemic prevention and control system in public health emergency, these elements can be existing systems, forming an SoS where the relevant pieces of the system-of-interest are, by definition, systems themselves.

When the epidemic prevention and control system includes software systems, hardware systems, personnel, facilities, communication systems, service systems, and management systems, and each system is managerially and operationally independent, and has interaction with others, then it can be considered as an SoS. In order to meet the goal of epidemic prevention and control, the SoS should offer quick response time, accelerated project development speed, and high efficiency. In this case, a directed SoS can be a good option.

NOTE A directed SoS is centrally controlled. Forming a directed SoS during an epidemic emergency can involve a change of control for the constituent systems. More information for directed SoS can be found in ISO/IEC/IEEE 21841.

5.9 Process application

5.9.1 Overview

ISO/IEC/IEEE 15288:2023, 5.7 or ISO/IEC/IEEE 12207:2017, 5.7 shall apply with the following addition:

The functions of processes are defined in terms of specific purposes, outcomes and the set of activities and tasks that constitute the process.

The iterative use of those processes is important for the progressive refinement of process outputs, for example, the interaction between successive verification actions and integration actions during an epidemic emergency can incrementally build confidence. The recursive use of processes, for example, the repeated application of the same process or set of processes applied to successive levels of system elements in a system structure, can add value to successive systems.

The changing nature of the influences on the system, in this case under epidemic emergency, requires continual review of the selection and timing of process use. Process use in the life cycle can be dynamic, responding to the many external influences on the system, such as an epidemic emergency. The life cycle approach also allows for incorporating the changes in the next stage. The life cycle stages assist the planning, execution, and management of life cycle processes. In the face of this complexity, the life cycle model provides comprehensible and recognizable high-level purpose and structure. The set of processes within a life cycle process group is applied with the common goal of satisfying the exit criteria for a stage or the entry criteria of the formal progress reviews within that stage.

The technical management processes, organizational project enabling processes and technical processes interoperate with each other. The purpose, outcomes and set of activities and tasks should be specific to the epidemic emergency. The organizational project enabling processes enable the input of concept and system definitions of technical processes. Performance of the processes focused on concept and system definition requires input from processes that focus on system realization, deployment, and use. All this should be accomplished across the life cycle. Figure 2 illustrates the interrelationships among these processes.

EXAMPLE 1 During an epidemic emergency, the inter-operative engineering processes facilitate the ability of systems, personnel, and equipment to provide and receive bio-medical related functionality, data, information and services to and from other systems, personnel, and equipment of both public and private agencies, departments, and other organizations, in a manner enabling them to operate effectively and securely together.

EXAMPLE 2 For a vaccination system, a thorough assessment of clinical data is carried out to reach a scientific opinion on whether each vaccine is safe and efficacious. The system helps ensure that vaccine distribution is based on a transparent, ethical framework, incorporating clinical and equitable norms. The distribution approach combines ethical principles for stewardship of scarce resources with equitable access with prioritization for those most in need. The effective communication approach builds on the successful communication and engagement programme delivered throughout the epidemic. Communication efforts have a particular focus on maximizing the public's understanding of the vaccines, including oversight in real world use. The aim is to connect with underserved, hard to reach, vulnerable, and vaccine-hesitant populations, as well as to pursue focused outreach approaches to communities at highest risk. The process of system development is agile and iterative in order to adapt to new knowledge regarding the ability of vaccines to reduce illness and infection, and circumstances as they arise.

Detailed descriptions of life cycle stages in the context of the specific epidemic scenario may also be created in order to minimize stakeholder' risks by establishing the link between the stage and the specific process. Descriptions of stages during epidemic emergencies may include epidemic awareness, risk characterization, epidemiological investigation, surveillance and epidemiological monitoring, laboratory analysis, and management of medical countermeasures, supplies, equipment, and information management systems.

The stage of epidemic awareness may enable the relevant life cycle process to be capable of identifying that a health threat with national or international potential has arisen.

The stage of risk characterization may enable the relevant life cycle process to be capable of identifying the pathogen and its epidemiological characteristics, such as reservoir and potential sources, modes of transmission, risk groups, level and duration of infectiousness, virulence, generation time, and available control strategies.

The stage of epidemiological investigation may enable the relevant life cycle process to be capable of developing case definitions, conducting outbreak investigations and case control studies to validate and analyse case reports, identifying pathogens and sources of exposure, and aiding in risk characterization.

The stage of surveillance and epidemiological monitoring may enable the relevant life cycle process to be capable of identifying outbreaks, characterizing affected population groups, monitoring disease trends, and evaluating the impact of control strategies.

The stage of laboratory analysis may enable the relevant life cycle process to be capable of identifying pathogens, monitoring antimicrobial resistance, and handling large numbers of samples submitted for diagnostic purposes. The stage management of medical countermeasures, supplies, equipment may enable the relevant life cycle process to be capable of procuring, distributing, and managing countermeasures, supplies and equipment, including personal protective equipment.

The stage of information management system may enable the relevant life cycle process to develop, maintain, and govern information flows that support management, operations, planning, logistics, finance, and administration.

5.9.2 Process iteration, recursion, and concurrency

ISO/IEC/IEEE 15288:2023, 5.8.2 shall apply.

5.9.3 Process views

ISO/IEC/IEEE 15288:2023, 5.8.3 shall apply.

5.10 Concept and system definition

ISO/IEC/IEEE 15288:2023, 5.9 shall apply.

5.11 Assurance and quality characteristics

ISO/IEC/IEEE 15288:2023, 5.10 shall apply.

5.12 Process reference model

ISO/IEC/IEEE 15288:2023, 5.11 or ISO/IEC/IEEE 12207:2017, 5.8 shall apply.

6 System life cycle processes

6.1 Agreement processes

6.1.1 Acquisition process

6.1.1.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.1.1.1 or ISO/IEC/IEEE 12207:2017, 6.1.1.1 shall apply.

6.1.1.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.1.1.2 or ISO/IEC/IEEE 12207:2017, 6.1.1.2 shall apply in accordance with the acquirer-supplier agreement.

6.1.1.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.1.1.3 or ISO/IEC/IEEE 12207:2017, 6.1.1.3 shall apply.

6.1.1.4 Acquisition process outputs

One or more of the following acquisition process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) contract, including any special contract requirements; the contract shall contain relevant provisions on how to deal with contract changes and partial realization of the contract caused by force majeure in the epidemic; the agreement (contract) shall contain relevant provisions on how to deal with the failure to deliver supply caused by force majeure in an epidemic emergency;

b) approved change proposals.

Due to the changing methods and timelines of epidemic prevention and control, the modification of related contracts may be more frequent.

6.1.2 Supply process

6.1.2.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.1.2.1 or ISO/IEC/IEEE 12207:2017, 6.1.2.1 shall apply.

6.1.2.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.1.2.2 or ISO/IEC/IEEE 12207:2017, 6.1.2.2 shall apply in accordance with the acquirer-supplier agreement.

6.1.2.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.1.2.3 or ISO/IEC/IEEE 12207:2017, 6.1.2.3 shall apply.

6.1.2.4 Supply process outputs

One or more of the following supply process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) approved change proposals;

b) other deliverables in the list of contract requirements.

6.2 Organizational project-enabling processes

6.2.1 Life cycle model management process

6.2.1.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.2.1.1 or ISO/IEC/IEEE 12207:2017, 6.2.1.1 shall apply.

6.2.1.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.2.1.2 or ISO/IEC/IEEE 12207:2017, 6.2.1.2 shall apply in accordance with the acquirer-supplier agreement.

6.2.1.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.2.1.3 or ISO/IEC/IEEE 12207:2017, 6.2.1.3 shall apply.

6.2.1.4 Life cycle model management process outputs

The following life cycle model management process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) policies and procedures for life cycle models and processes;

b) life cycle models and process evaluation results;

c) life cycle model and process optimization plan and optimization situation.

NOTE The life cycle model management process is often expected to generate outputs that can enable:

— suppliers to perform periodical and iterative development and maintenance with trial operations for evolutionary improvements or to resolve issues in epidemic prevention and control;

— developers to develop and release iteratively and periodically; to obtain and respond to quick feedback on effectiveness of the system operation for epidemic prevention and control from system operators, medical users, and general public users;

— suppliers of existing systems or software to be interfaced or connected with the system to enter maintenance and to provide requested functions for epidemic prevention and control.

6.2.2 Infrastructure management process

6.2.2.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.2.2.1 or ISO/IEC/IEEE 12207:2017, 6.2.2.1 shall apply.

6.2.2.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.2.2.2 or ISO/IEC/IEEE 12207:2017, 6.2.2.2 shall apply in accordance with the acquirer-supplier agreement.

6.2.2.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.2.2.3 or ISO/IEC/IEEE 12207:2017, 6.2.2.3 shall apply with the following addition:

— Add to activity a) "establish the infrastructure", task 2):

In the case of an epidemic, due to restrictions on personnel, transportation, and logistics, an emergency mechanism shall be established for the acquisition and provision of infrastructure resources required

for the system life cycle, such as deployment in advance, purchase of additional spare parts, and opening special logistics channels,

— Add the following tasks to activity b) "maintain the infrastructure":

1) When infrastructure maintenance personnel are unable to perform their duties normally due to activity restrictions or health factors, supplement personnel. Give priority to supplementing personnel who meet the requirements of infrastructure maintenance experience and skills. Train personnel who do not meet the qualifications as soon as possible or hire externally qualified personnel.

2) Establish contingency logistics plans, such as purchasing in advance or opening special logistics channels.

6.2.2.4 Infrastructure management process outputs

The following infrastructure outputs shall be provided:

a) Infrastructure elements are clearly identified;

b) Accessible infrastructure elements are developed or supplied.

NOTE Access to infrastructure is more difficult under epidemic prevention and control conditions, especially when some infrastructure is damaged or expires.

6.2.3 Portfolio management process

6.2.3.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.2.3.1 or ISO/IEC/IEEE 12207:2017, 6.2.3.1 shall apply.

6.2.3.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.2.3.2 or ISO/IEC/IEEE 12207:2017, 6.2.3.2 shall apply.

6.2.3.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.2.3.3 or ISO/IEC/IEEE 12207:2017, 6.2.3.3 shall apply.

6.2.3.4 Portfolio management process outputs

The following portfolio management process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) project definition and authorization certificate;

b) project evaluation.

NOTE The portfolio management process is often expected to generate outputs that provide the following:

— portfolio evaluations that include the system and its life cycle process characteristics for epidemic prevention and control, as identified in 5.2.2 and 5.5.4;

— information and reasons to determine whether the current projects, for epidemic prevention and control are planned to be continued, prioritized, supplemented with the activation of additional support projects, or terminated.

6.2.4 Human resource management process

6.2.4.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.2.4.1 or ISO/IEC/IEEE 12207:2017, 6.2.4.1 shall apply.

6.2.4.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.2.4.2 or ISO/IEC/IEEE 12207:2017, 6.2.4.2 shall apply in accordance with the acquirer-supplier agreement.

6.2.4.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.2.4.3 or ISO/IEC/IEEE 12207:2017, 6.2.4.3 shall apply with the following addition:

— Add the following note to activity a) "identify skills", tasks 1) and 2):

NOTE In the case of an epidemic, the system life cycle process involves cross-professionals from multiple industries and professional fields, such as health care, disease control, and emergency management.

— Add to activity c) "acquire and provide skills":

For the prevention and control requirements in the case of an epidemic, time-bound requirements and mechanisms shall be used to acquire and deploy skilled personnel, such as health care, disease control, and emergency management professionals.

6.2.4.4 Human resource management process outputs

The following human resource management process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) list of required skills;

b) list of skilled personnel;

c) skills management plan, including skills development, training, strengthening, and dynamic acquisition;

d) staff management plan, including dynamic staffing levels, and staff allocation.

6.2.5 Quality management process

6.2.5.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.2.5.1 or ISO/IEC/IEEE 12207:2017, 6.2.5.1 shall apply.

6.2.5.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.2.5.2 or ISO/IEC/IEEE 12207:2017, 6.2.5.2 shall apply in accordance with the acquirer-supplier agreement.

6.2.5.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.2.5.3 or ISO/IEC/IEEE 12207:2017, 6.2.5.3 shall apply.

6.2.5.4 Quality management process outputs

The following quality management process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) organizational quality management policies, plans and schedules;

b) organizational quality evaluation reports supporting participating projects in the epidemic prevention and control system;

c) organizational quality management records and reports;

d) organizational incident records and resolution reports.

NOTE The quality management process generates outputs that support multiple participating projects. Multiple acquirers and suppliers can collaboratively organize quality management with stakeholders during system development, maintenance, and service for epidemic prevention and control.

6.2.6 Knowledge management process

6.2.6.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.2.6.1 or ISO/IEC/IEEE 12207:2017, 6.2.6.1 shall apply.

6.2.6.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.2.6.2 or ISO/IEC/IEEE 12207:2017, 6.2.6.2 shall apply in accordance with the acquirer-supplier agreement.

6.2.6.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.2.6.3 or ISO/IEC/IEEE 12207:2017, 6.2.6.3 shall apply with the following addition:

Add the following note to activity a) "plan knowledge management", task 2):

NOTE A wide range of professional knowledge, skills and knowledge assets can be identified, such as health care, disease control, emergency response and management.

6.2.6.4 Knowledge management process outputs

The following knowledge management process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) list of knowledge assets;

b) knowledge management norms (rules and regulations);

c) data used in knowledge management;

d) epidemic prevention knowledge document.

6.3 Technical management processes

6.3.1 Project planning process

6.3.1.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.3.1.1 or ISO/IEC/IEEE 12207:2017, 6.3.1.1 shall apply.

6.3.1.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.3.1.2 or ISO/IEC/IEEE 12207:2017, 6.3.1.2 shall apply in accordance with the acquirer-supplier agreement.

6.3.1.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.3.1.3 or ISO/IEC/IEEE 12207:2017, 6.3.1.3 shall apply.

6.3.1.4 Project planning process outputs

The following project planning process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) SEMP, aligned with the acquirer's SEP;

b) CWBS;

c) The IMP including the IMS, EVM planning, and other specific planning.

NOTE The project planning process is often expected to generate outputs that support the timely release of a system for recovering critically emergent status of epidemic prevention and control. For example, project planning process outputs can be realized as sprint planning to develop features from the backlog, when highly rapid and iterative development is prioritized.

6.3.2 Project assessment and control process

6.3.2.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.3.2.1 or ISO/IEC/IEEE 12207:2017, 6.3.2.1 shall apply.

6.3.2.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.3.2.2 or ISO/IEC/IEEE 12207:2017, 6.3.2.2 shall apply in accordance with the acquirer-supplier agreement.

6.3.2.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.3.2.3 or ISO/IEC/IEEE 12207:2017, 6.3.2.3 shall apply.

6.3.2.4 Project assessment and control process outputs

The following project assessment and control process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) documented process for assessing system effectiveness, life cycle cost, schedule, and risk;

b) variance reports and corrective actions.

NOTE The project assessment and control process is often expected to frequently monitor the progress in improving epidemic prevention and control.

6.3.3 Decision management process

6.3.3.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.3.3.1 or ISO/IEC/IEEE 12207:2017, 6.3.3.1 shall apply.

6.3.3.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.3.3.2 or ISO/IEC/IEEE 12207:2017, 6.3.3.2 shall apply in accordance with the acquirer-supplier agreement.

6.3.3.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.3.3.3 or ISO/IEC/IEEE 12207:2017, 6.3.3.3 shall apply.

6.3.3.4 Decision management process outputs

The following decision management process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) a decision management strategy;

b) a recommended course of action;

c) documented and implemented decisions.

NOTE The decision management process is often expected to generate outputs that can provide reasonable decision approaches or decision-making methods for improving the effectiveness of epidemic prevention and control.

6.3.4 Risk management process

6.3.4.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.3.4.1 or ISO/IEC/IEEE 12207:2017, 6.3.4.1 shall apply.

6.3.4.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.3.4.2 or ISO/IEC/IEEE 12207:2017, 6.3.4.2 shall apply in accordance with the acquirer-supplier agreement.

6.3.4.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.3.4.3 or ISO/IEC/IEEE 12207:2017, 6.3.4.3 shall apply with the following addition:

Add the following notes to activity c) "analyse risks", task 1):

NOTE 1 In the case of epidemics, the risks of shortages of spare parts and supplies, insufficient workforce for operations and maintenance, and out-of-date or unavailable information can be expected.

NOTE 2 The management requirements and constraints of ISO/IEC 27001 and local laws and regulations form the context for evaluating information and data security risks.

NOTE 3 Implementing new epidemic control systems can impact existing systems. For example, purchasing services can be affected by the need to overcome a shortage of medical supplies for hospitals, individual patients, or general public users. Frequent requests for epidemic-related data can affect local hospitals' information systems. Increased requests for connection to medical equipment can strain logistics systems. In these situations, the risk management process can be performed to identify risks and mitigation.

6.3.4.4 Risk management process outputs

The following risk management process output shall be provided in accordance with the acquirer-supplier agreement: the risk management plan with the following attributes:

a) specifies a process for risk and opportunity identification, such as the risk identification of purchased parts;

b) identified risks that can impact the program or technical solution;

c) project risk assessment.

6.3.5 Configuration management process

6.3.5.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.3.5.1 or ISO/IEC/IEEE 12207:2017, 6.3.5.1 shall apply.

6.3.5.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.3.5.2 or ISO/IEC/IEEE 12207:2017, 6.3.5.2 shall apply in accordance with the acquirer-supplier agreement.

6.3.5.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.3.5.3 or ISO/IEC/IEEE 12207:2017, 6.3.5.3 shall apply.

6.3.5.4 Configuration management process outputs

The following configuration management process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) configuration management plan;

b) evaluation of change control implementation, including the following:

   1) baseline decision making and change control measures;

   2) configuration control, including system recommendations, justification, evaluation, coordination, approval, or disapproval of proposed changes to the baseline;

   3) analysis of proposed changes to the baseline;

c) configuration change management records;

d) configuration item status accounting records.

NOTE Records define the life cycle baselines of the epidemic prevention and control system.

6.3.6 Information management process

6.3.6.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.3.6.1 or ISO/IEC/IEEE 12207:2017, 6.3.6.1 shall apply.

6.3.6.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.3.6.2 or ISO/IEC/IEEE 12207:2017, 6.3.6.2 shall apply in accordance with the acquirer-supplier agreement.

6.3.6.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.3.6.3 or ISO/IEC/IEEE 12207:2017, 6.3.6.3 shall apply.

6.3.6.4 Information management process outputs

The following information management process outputs shall be provided in accordance with the acquirer- supplier agreement:

a) information management products;

b) information items related to epidemic prevention and control.

NOTE The information management process can be applied to produce outputs that can be provided repeatedly and periodically during development and operation of epidemic prevention and control systems. Such outputs can include use cases, planned release schedules, and material to encourage appropriate behavior to prevent the infection from spreading. Stakeholders for information management can include epidemic specialists, doctors, clinical nurses, medical care personnel or staff in municipal offices, epidemic patients, vaccine trial volunteers, and the general public.

6.3.7 Measurement process

6.3.7.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.3.7.1 or ISO/IEC/IEEE 12207:2017, 6.3.7.1 shall apply.

6.3.7.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.3.7.2 or ISO/IEC/IEEE 12207:2017, 6.3.7.2 shall apply in accordance with the acquirer-supplier agreement.

6.3.7.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.3.7.3 or ISO/IEC/IEEE 12207:2017, 6.3.7.3 shall apply.

6.3.7.4 Measurement process outputs

The following measurement process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) measurement reports including measures, analysis results, and initial recommendations;

b) measures and select technical parameters for tracking;

c) measurement data.

The measurement process may generate outputs providing the following:

— quality analysis results, including functional suitability, performance efficiency, operability, and availability of the system in association with improving epidemic prevention and control;

— visualized data and analysis results, including recommended actions and trends in the epidemic prevention and control status appropriate to specific users, e.g. operators, medical care experts or staffs, patients, press, and the general public.

6.3.8 Quality assurance process

6.3.8.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.3.8.1 or ISO/IEC/IEEE 12207:2017, 6.3.8.1 shall apply.

6.3.8.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.3.8.2 or ISO/IEC/IEEE 12207:2017, 6.3.8.2 shall apply in accordance with the acquirer-supplier agreement.

6.3.8.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.3.8.3 or ISO/IEC/IEEE 12207:2017, 6.3.8.3 shall apply with the following addition:

— Add the following task to activity a) "prepare for quality assurance":

1) Confirm that supplier quality assurance requirements are defined and adequate.

If there are multiple suppliers, QA requirements shall apply to each of them. If multiple suppliers are involved in layered supply chains, the QA requirements shall apply to first-level suppliers for their own tasks and also to the tasks performed by their contracted suppliers through application of the acquisition and supply processes.

— Add the following task to activity b) "perform product or service evaluations":

1) Confirm verification of the supplier quality assurance program.

NOTE In the case of an epidemic, the correctness of the epidemic prevention and control system related information transmission is a higher priority than the real-time information transmission.

6.3.8.4 Quality assurance process outputs

The following quality assurance process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) quality assurance plans and schedules;

b) quality evaluation reports;

c) quality assurance records and reports;

d) incident records and reports.

NOTE The quality assurance process is often expected to generate outputs which are updated iteratively and provided periodically to stakeholders, when the system or software is required to be rapidly developed and maintained, and to improve the quality of the system, including functional correctness, usability, and performance efficiency for epidemic control and prevention.

6.4 Technical processes

6.4.1 Business or mission analysis process

6.4.1.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.1.1 or ISO/IEC/IEEE 12207:2017, 6.4.1.1 shall apply.

6.4.1.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.1.2 or ISO/IEC/IEEE 12207:2017, 6.4.1.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.1.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.1.3 or ISO/IEC/IEEE 12207:2017, 6.4.1.3 shall apply.

6.4.1.4 Business or mission analysis process outputs

The following business or mission analysis process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) identification of quantifiable need statements;

b) definition of technology maturation and other risk mitigation steps for potential future action to develop the promising system concepts;

c) sustainment strategies for the selected alternative solutions.

6.4.2 Stakeholder needs and requirements definition process

6.4.2.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.2.1 or ISO/IEC/IEEE 12207:2017, 6.4.2.1 shall apply as stated.

6.4.2.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.2.2 or ISO/IEC/IEEE 12207:2017, 6.4.2.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.2.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.2.3 or ISO/IEC/IEEE 12207:2017, 6.4.2.3 shall apply with the following addition:

NOTE 1 System instances are expected to be identified, coordinated, and resolved by various stakeholders. Systems and software life cycle processes can be applied in an incremental and iterative manner to address and resolve those issues.

NOTE 2 Changes in the epidemic situation can lead to relatively large and rapid changes in stakeholder needs and requirements.

— Add the following subtasks to activity a) "prepare for stakeholder needs and requirements definition", task 1):

i. Identify the interests and incentives of stakeholders.

NOTE 3 Stakeholders can include developers, maintainers, operators, medical experts, patients, and general public users. Annex A provides typical examples of issues and concerns of stakeholders and the application of life cycle processes in epidemic prevention and control systems.

ii. Coordinate among relevant stakeholders when systems and subsystem elements change.

NOTE 4 The interests and incentives of individual stakeholders among many subsystems for epidemic prevention and control can conflict, resulting in misalignment of incentives.

6.4.2.4 Stakeholder needs and requirements definition process outputs

The following stakeholder needs and requirements definition process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) defined set of user and other stakeholder requirements, appropriate to system maturity;

b) changes in the operational scenarios and OpsCon to fill the capability gaps.

Requirements and operational scenarios or OpsCon should include capabilities for the following:

— share information and warnings of epidemic status in a timely way for joint missions and rapid development;

— feedback stakeholder issues with epidemic prevention and control.

6.4.3 System requirements definition process

6.4.3.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.3.1 or ISO/IEC/IEEE 12207:2017, 6.4.3.1 shall apply.

6.4.3.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.3.2 or ISO/IEC/IEEE 12207:2017, 6.4.3.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.3.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.3.3 or ISO/IEC/IEEE 12207:2017, 6.4.3.3 shall apply with the following additions:

— Add the following to activity b) "define system requirements", task 3) (ISO/IEC/IEEE 15288:2023, 6.4.3.3) or activity b) "define system/software requirements", task 4) (ISO/IEC/IEEE 12207:2017, 6.4.3.3):

NOTE 1 The system requirements definition process is an iterative activity whereby system requirements are defined, refined, analysed, traded, and managed to remove deficiencies and minimize impacts of potential cost drivers to establish an agreed-to set of requirements coordinated with the appropriate stakeholders.

The epidemic prevention and control system may involve the definition of the interface for relevant data to interact within the organization and external organizations (the number of external organizations can be very large). Especially when interacting with external organizations, the interface definition, sufficient reserved interface resources, and the correct integrated implementation should be specified.

NOTE 2 In consideration of the suddenness of the epidemic and its impact on normal production the system requirements can include disaster tolerance and recovery capacity (resilience) of the system.

— Add the following to activity b) "define system requirements", task 4) (ISO/IEC/IEEE 15288:2023, 6.4.3.3) or activity b) "define system/software requirements", task 5) (ISO/IEC/IEEE 12207:2017, 6.4.3.3):

To prepare for contingencies when the system fails to respond or collapses, emergency plans should be prepared, including manual intervention for epidemic prevention and control data collection and rapid restart of the system.

NOTE 3 The system requirements specify performance and efficiency, such as response time, concurrent user capacity for key functions, and resilience under stress.

— Add the following note to activity d) "manage system requirements":

NOTE 4 This activity supports the configuration identification activities in the configuration management process (6.3.5) including definition of the functional baseline and continuing throughout the development process to also support the definition of the allocated baseline.

— Add the following note to activity d) "manage system requirements", task 3) (ISO/IEC/IEEE 15288:2023, 6.4.3.3) or activity d) "manage system/software requirements", task 2) (ISO/IEC/IEEE 12207:2017, 6.4.3.3):

NOTE 5 Adopting a requirements management system supported by tools can assist in accomplishing the activities and tasks and facilitate the sharing of requirements data.

6.4.3.4 System requirements definition process outputs

The following system requirements definition process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) a set of system requirements;

b) requirement traceability mapping.

NOTE Outputs of the system requirements definition process can support the following:

— system requirements that specify the system behaviour when resources are limited, to protect data integrity;

— system requirements that include data correctness, data analysis, and visualization functions for epidemic prevention and control;

— traceable mapping that addresses the priority of each system and implements the high-priority functions for epidemic prevention and control during early development iterations.

6.4.4 Architecture definition process

6.4.4.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.4.1 or ISO/IEC/IEEE 12207:2017, 6.4.4.1 shall apply with the following modification:

Iteration of the architecture definition process with the business or mission analysis process, the system requirements definition process, and the stakeholder needs and requirements definition is often employed to converge on a balanced solution. A balanced solution is determined by considering cost, schedule, performance, and risk within affordability constraints.

NOTE The architecture definition process often requires analyses and trades to converge on a balanced solution. The system analysis and decision management processes facilitate these analyses and trades.

6.4.4.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.4.2 or ISO/IEC/IEEE 12207:2017, 6.4.4.2 shall apply in accordance with the acquirer-supplier agreement with the following addition:

a) Functional (logical) architecture is defined.

b) Physical architecture is defined.

6.4.4.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.4.3 or ISO/IEC/IEEE 12207:2017, 6.4.4.3 shall apply.

6.4.4.4 Architecture definition process outputs

The following architecture definition process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) functional (logical) architecture view/model;

b) physical hierarchy or architecture view/model;

c) architecture traceability mapping.

NOTE Outputs of the architecture definition process can support the following.

— The functional (logical) architecture model describes interactions among the system stakeholders and external entities, such as use cases, biomedical data flows among stakeholders, and other connecting systems with multiple permission levels for access and use.

— The physical architecture model describes biomedical data distribution by location, equipment, or device, such as multiple data repository sites and servers, local medical facilities, hospitals or healthcare stations, medical staff or personnel, patients or relatives, and individual user's mobile phones or internet.

6.4.5 Design definition process

6.4.5.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.5.1 or ISO/IEC/IEEE 12207:2017, 6.4.5.1 shall apply with the following addition:

NOTE The essence of this activity is to achieve a balanced and feasible design with acceptable risk and within the program design constraints, including cost, schedule, and performance.

6.4.5.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.5.2 or ISO/IEC/IEEE 12207:2017, 6.4.5.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.5.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.5.3 or ISO/IEC/IEEE 12207:2017, 6.4.5.3 shall apply with the following addition:

Add the following notes to activity b) "create the system design", task 6) (ISO/IEC/IEEE 15288:2023, 6.4.5.3) or activity b) "establish designs related to each software system element", task 4) (ISO/IEC/IEEE 12207:2017, 6.4.5.3):

NOTE 1 Design solutions at the system level reflect limited infrastructure resources and situations where information content cannot be effectively and adequately supported in a short period of time.

NOTE 2 Specific requirements design and solutions at the system level reflect the constraints of a weak network environment (such as remote and underdeveloped areas), The design includes not only mainstream communication modes, but also special network solutions.

NOTE 3 Professional statistical analysis functions and visual data presentation are of great significance for risk assessment and response decision making in epidemic prevention and control.

6.4.5.4 Design definition process outputs

The following design definition process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) system design description;

b) interface definition with the following attributes:

   1) includes physical interactions;

   2) identifies system boundaries;

   3) includes functional interactions;

   4) identifies interactions with systems or environments outside the system boundaries;

c) allocated baseline;

d) product baseline, with consideration for the use of open source software.

NOTE The design definition process is often employed to generate outputs that can provide design definition to enable:

— system design descriptions, interface definitions, interactions, and shareable baselined design,

— minimized direct contact and physical interactions between humans and the system to reduce epidemic risks from the system operation itself;

— functional interactions between humans and the system to be available through remote access, in order to reduce epidemic risks from system operation itself;

— system boundaries to be extendable to treat additional stakeholders and usages during system operation.

6.4.6 System analysis process

6.4.6.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.6.1 or ISO/IEC/IEEE 12207:2017, 6.4.6.1 shall apply with the following addition:

NOTE System analysis includes the broad range of assessments, trades, and analyses performed over the entire life cycle of a system. System analyses are conducted as necessary to determine balanced technical solutions pertaining to system concepts, technologies, requirements, and designs of a system and its components.

6.4.6.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.6.2 or ISO/IEC/IEEE 12207:2017, 6.4.6.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.6.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.6.3 or ISO/IEC/IEEE 12207:2017, 6.4.6.3 shall apply.

6.4.6.4 System analysis process outputs

The following system analysis process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) ESOH analysis and impact assessment;

b) FMECA;

c) effectiveness analysis;

d) requirement analysis;

e) PSA.

NOTE The system analysis process is often expected to produce results of the effectiveness of epidemic prevention and control, updated with monitoring and feedback data from the system users.

6.4.7 Implementation process

6.4.7.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.7.1 or ISO/IEC/IEEE 12207:2017, 6.4.7.1 shall apply.

6.4.7.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.7.2 or ISO/IEC/IEEE 12207:2017, 6.4.7.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.7.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.7.3 or ISO/IEC/IEEE 12207:2017, 6.4.7.3 shall apply with the following addition:

— Add the following note to activity b) "perform implementation":

NOTE 1 Implementation includes work to build, reuse, code, or acquire the products that make up the system to include the implementation (fabrication and code) and sustainment assets as specified in the statement of work.

— Add the following note to activity b) "perform implementation", task 1):

NOTE 2 Considering the trade-off between the system and software development speed and quality, agile methodologies can be used to accelerate system and software development velocity. The aim is to achieve rapid and responsive results in an epidemic emergency.

6.4.7.4 Implementation process outputs

The following implementation process outputs shall be provided in accordance with the acquirer-supplier agreement: realization of the physical system elements as identified in the product baseline, including fabrication and production methods.

NOTE 1 The Implementation process is often expected to generate outputs that can enable:

— software necessary for the system or its elements to be applicable wherever users intend to use the system, e.g. with a reduced information communication network or internet facilities.

— system elements to be fabricated, supplied, repaired, and reproduced, where users are in problematic work environments, e.g. less energy supplies, less production facilities.

NOTE 2 Implementation outputs do not include tools (e.g. test tools) that the supplier uses prior to release of the asset (hardware or software) to configuration management.

6.4.8 Integration process

6.4.8.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.8.1 or ISO/IEC/IEEE 12207:2017, 6.4.8.1 shall apply.

6.4.8.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.8.2 or ISO/IEC/IEEE 12207:2017, 6.4.8.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.8.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.8.3 or ISO/IEC/IEEE 12207:2017, 6.4.8.3 shall apply with the following addition:

— Add to activity a) "prepare for integration":

Preparation for integration may include descriptions of processes or system required in epidemic emergencies, such as laboratories or other facilities, personnel, test stands, testing harnesses, testing software, and integration schedules.

Since the interface definition can be standardized and the number of external interfacing organizations can be very large, adequate interface resources should be reserved and allocated for the implementation.

— Add to activity b) "perform integration":

Identify methods of preparing anonymized data which can be shared.

— Add the following note to activity b) "perform integration", task 3) (ISO/IEC/IEEE 15288:2023, 6.4.8.3) or activity b) "perform integration", task 2) (ISO/IEC/IEEE 12207:2017, 6.4.8.3):

NOTE Integration activities are performed with approved assembly/integration and verification procedures at each level of the build-up.

6.4.8.4 Integration process outputs

The following integration process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) the SIP;

b) assembly/integration procedures that are aligned with verification procedures;

c) discrepancy reports, causal analyses, and corrective action procedures.

The integration process can generate the following outputs:

— software for the system to be integrated, wherever users intend to use the system, e.g. in locations with weaker information communication networks or internet facilities, or fewer experts;

— system to be integrated, even when users are in emergent situations, or in recovery actions from disaster, e.g. having limited energy supplies, limited spaces, outdoor fields, and less trained personnel.

6.4.9 Verification process

6.4.9.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.9.1 or ISO/IEC/IEEE 12207:2017, 6.4.9.1 shall apply with the following addition:

NOTE 1 The individual system elements provided by the implementation process are verified through DT&E, acceptance testing, or qualification testing.

NOTE 2 It is difficult to achieve 100 % coverage of verification. Therefore, in the case of sudden infectious public health events, verification can be based on the correctness and accuracy of data.

6.4.9.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.9.2 or ISO/IEC/IEEE 12207:2017, 6.4.9.2 shall apply in accordance with the acquirer-supplier agreement.

NOTE The verification process can generate outcomes that enable the following:

— trustworthy information, data, or medical cares and cures provided by the system, software and services for epidemic control and prevention;

— information and data from the system to be correctly exchanged with users and other systems to communicate and obtain feedback from stakeholders for improving epidemic control and prevention.

6.4.9.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.9.3 or ISO/IEC/IEEE 12207:2017, 6.4.9.3 shall apply with the following additions:

— Add the following note to activity a) "prepare for verification":

NOTE 1 The reuse of data and economical use of test resources in an integrated testing activity can help expedite verification.

— Add to activity a) "prepare for verification", task 1):

Define and specify relevant verification policies that include performance efficiency indicators, such as response time capability and concurrent user capacity for key functions of the system.

— Add the following note to activity a) "prepare for verification", task 4) (ISO/IEC/IEEE 15288:2023, 6.4.9.3) or activity a) "prepare for verification", task 1) (ISO/IEC/IEEE 12207:2017, 6.4.9.3):

NOTE 2 The verification strategy accounts for the diversity of related data within the organization, interaction with external organizations involved in epidemic prevention and control, and needs of various stakeholders in different environments at different stages of the system life cycle.

— Add the following note to activity b) "perform verification":

NOTE 3 Verification applies to the utility and integrity of the integration environment (e.g. its functional capabilities, safety, security, and calibration).

6.4.9.4 Verification process outputs

The following verification process outputs shall be provided in accordance with the acquirer-supplier agreement:

a) verification results;

b) design qualification data;

c) fault analysis conducted in support of system end-to-end testing;

d) end-to-end test plans; test procedures; test exceptions, discrepancies and associated fault risk assessments; and test results.

6.4.10 Transition process

6.4.10.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.10.1 or ISO/IEC/IEEE 12207:2017, 6.4.10.1 shall apply.

6.4.10.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.10.2 or ISO/IEC/IEEE 12207:2017, 6.4.10.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.10.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.10.3 or ISO/IEC/IEEE 12207:2017, 6.4.10.3 shall apply with the following addition:

Add to activity a) "prepare for the transition", task 1) (ISO/IEC/IEEE 15288:2023, 6.4.10.3) or activity a) "prepare for the software system transition", task 1) (ISO/IEC/IEEE 12207:2017, 6.4.10.3):

NOTE 1 Transition includes the conduct of deployment analyses and assessments to support the development of people, product, and process solutions necessary to deploy system end-items by the supplier to the extent required in the acquirer-supplier agreement.

NOTE 2 Personal medical record data or biometric data are carefully identified, secured, and classified for privacy protection. Patient data are anonymized, or fictitious data are used to prepare user documentation and to train the operators, users, and other stakeholders necessary for system utilization and support, as in ISO/IEC/IEEE 15288:2023, 6.4.10.3 b)5) or ISO/IEC/IEEE 12207:2017, 6.4.10.3 b)4).

6.4.10.4 Transition process outputs

The following transition process output shall be provided in accordance with the acquirer-supplier agreement: deployment analyses and assessments.

NOTE The transition process is often employed to generate outputs that can enable users to understand what constraints are imposed on distribution and installation to the user environments, e.g. individual user's mobile smart phone, medical equipment, outdoors, and higher or lower temperature places.

6.4.11 Validation process

6.4.11.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.11.1 or ISO/IEC/IEEE 12207:2017, 6.4.11.1 shall apply.

6.4.11.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.11.2 or ISO/IEC/IEEE 12207:2017, 6.4.11.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.11.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.11.3 or ISO/IEC/IEEE 12207:2017, 6.4.11.3 shall apply.

6.4.11.4 Validation process outputs

The following validation process outputs shall be provided in accordance with the acquirer-supplier agreement: system validation data.

6.4.12 Operation process

6.4.12.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.12.1 or ISO/IEC/IEEE 12207:2017, 6.4.12.1 shall apply as stated with the following addition:

In the context of an epidemic emergency, the rapid change of the epidemic situation and the consequent demand can involve frequent iteration of the epidemic prevention and control system/software. Adequate human resources and continuous service capacity should be provided to achieve the specified quality of the rapid iterative upgrades.

6.4.12.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.12.2 or ISO/IEC/IEEE 12207:2017, 6.4.12.2 shall apply in accordance with the acquirer-supplier agreement with the following additions.

a) The system is interoperable with external systems or as part of an SoS for epidemic control and prevention. For example, numbers of available beds for medical care are shared and timely updated on a hospital network.

b) Users choose adequate actions for epidemic control and prevention based on information, data, or medical cares and cures provided by the system, software, and services.

c) Operational analysis is related to trade-offs and linked to iterations of the systems and software engineering processes and related decisions.

6.4.12.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.12.3 or ISO/IEC/IEEE 12207:2017, 6.4.12.3 shall apply with the following addition:

Add to activity a) "prepare for operation":

NOTE 1 Operation includes performing operational analyses and assessments to support the delivery of services, people, product, and processes by the supplier to the extent required in the acquirer-supplier agreement.

NOTE 2 Information including personal medical record data or biometric data is carefully identified, securely treated, and classified for privacy protection when identifying or defining training and qualification requirements for personnel performing system operation [ISO/IEC/IEEE 15288:2023, 6.4.12.3 a)5) or ISO/IEC/IEEE 12207:2017, 6.4.12.3 a)5)].

6.4.12.4 Operation process outputs

The following operation process outputs shall be provided in accordance with the acquirer-supplier agreement: reports describing operational and hazard constraints that influence system requirements, architecture, or design.

NOTE Information and experience collected as output from the operations process can be used to determine priorities for improving epidemic control and prevention.

6.4.13 Maintenance process

6.4.13.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.3.13.1 or ISO/IEC/IEEE 12207:2017, 6.3.13.1 shall apply.

6.4.13.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.13.2 or ISO/IEC/IEEE 12207:2017, 6.4.13.2 shall apply in accordance with the acquirer-supplier agreement.

6.4.13.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.13.3 or ISO/IEC/IEEE 12207:2017, 6.4.13.3 shall apply with the following addition:

Add to activity c) "perform logistics support", task 2):

NOTE 1 During an epidemic emergency there is a risk that personnel are unavailable to implement maintenance or support the entire process of remote maintenance. An automated maintenance strategy can help prepare for times when the system/software version undergoes rapid iteration according to the epidemic situation.

NOTE 2 Information including personal medical record data or biometric data is carefully identified and minimally used for privacy protection when performing the task to plan for the necessary enabling systems or services to support maintenance, as in ISO/IEC/IEEE 15288:2023, 6.4.13.1 a)5) or ISO/IEC/IEEE 12207:2017 6.4.13.3 a)5).

6.4.13.4 Maintenance process outputs

Outputs of the maintenance process can enable the system to be adapted to different environments and to be improved iteratively for more effective epidemic control and prevention.

The following maintenance process output shall be provided in accordance with the acquirer-supplier agreement: sustainment strategy with trade-offs and other analyses to accommodate iterations of the systems engineering processes and associated decisions.

EXAMPLE Correcting fluctuations in individual patient test results or in the accuracy of analysis of clinical samples.

6.4.14 Disposal process

6.4.14.1 Purpose

ISO/IEC/IEEE 15288:2023, 6.4.14.1 or ISO/IEC/IEEE 12207:2017, 6.4.14.1 shall apply.

6.4.14.2 Outcomes

ISO/IEC/IEEE 15288:2023, 6.4.14.2 or ISO/IEC/IEEE 12207:2017, 6.4.14.2 shall apply with the following addition: disposal strategy.

6.4.14.3 Activities and tasks

ISO/IEC/IEEE 15288:2023, 6.4.14.3 or ISO/IEC/IEEE 12207:2017, 6.4.14.3 shall apply with the following addition:

NOTE Information including personal medical record data or biometric data is carefully identified, securely treated, and surely classified for privacy protection during preparing and performing disposition of the system. ISO/IEC/IEEE 15288:2023, 6.4.14.3 or ISO/IEC/IEEE 12207:2017, 6.4.14.3.

6.4.14.4 Disposal process outputs

The following disposal process output shall be provided in accordance with the acquirer-supplier agreement: disposal-related trade-offs and other analyses to support iterations of the systems engineering processes and related decisions.

NOTE The disposal process is often expected to generate outputs that can enable:

— continuing storage of information and data for improving epidemic control and prevention after the system is deactivated;

— clinical samples to be retained under strict control after the system is deactivated, for potential analysis in similar future epidemic events.

Annex A
(informative)

Issues and concerns of stakeholders in the application of lifecycle processes to epidemic prevention and control systems

A.1 General

This annex presents four examples of how the life cycle processes can be applied to typical systems developed for epidemic prevention and control.

— sharing capacities for accommodating infected patients among multiple hospitals/clinics;

— monitoring for symptoms of infected patients who are instructed to stay home for isolation;

— surveillance and epidemiological monitoring of facilities where people gather;

— warning individuals of suspected infection and raising epidemic awareness.

For each type of system, Tables A.1 to A.4 present typical examples of stakeholders and their urgent needs during epidemic prevention and control.

A.2 Life cycle processes, stakeholder concerns, and issues for a medical clinical facility capacity information system

Life cycle processes can be applied iteratively to a facility capacity information system as in the following example.

a) Apply the stakeholder needs and requirements definition (see Table A.1), system/software requirements definition, and architecture definition processes iteratively and rapidly. Initially focus on sharing simply the number of admitted or on-site serious symptom patients (or the number of available beds or spaces) among medical staffs in neighbouring hospitals/clinics, and successively involve other hospitals/clinics.

b) Apply system and software life cycle processes iteratively and rapidly, in conjunction with system operation. Incrementally enrich the symptom information. Involve more stakeholders, such as hospitals/clinics and their medical staffs, home care patients, and public healthcare centres in wider locations.

c) Apply life cycle processes iteratively to evolve operational systems and enable multiple hospitals/clinics to share timely data and information. Enhance capabilities to accommodate data on infected patients, such as their individual symptoms and severity levels, along with the capability of hospitals/clinics to provide adequate treatments for that severity level.

Table A.1 — Stakeholder concerns and issues: medical/clinical facility capacity information system

Stakeholder	Typical issues or concerns
Medical staff (e.g. doctor, nurse, care worker)	— When large number of patients with mild symptoms are admitted to the hospital/clinic for treatment, the medical staff are not able to treat patients with severe symptoms. — Medical personnel and team resources become less to treat adequately severe symptomatic patients for saving their lives, when recovering patients stay longer.