Software Process Capability/Maturity Model for the Development of Asynchronous Store-and-Forward Telemedicine Systems in the Context of Digital Convergence - A Draft Model -

Christiane Gresse von Wangenheim

Working Paper	WP_GQS_01-2011_v10
Status	Final
Publicação	Public

Software Quality Group - GQS
National Institute for Research and Technology on Digital Convergence - INCOD
Department of Informatics and Statistics - INE
Federal University of Santa Catarina - UFSC
88049-200 Florianópolis - SC
Brazil

1. Introduction

Telemedicine broadly refers to the use of information and telecommunication technologies to distribute information or expertise necessary for providing or delivering healthcare services among geographically separated participants, including physicians and patients (Institute of Medicine, 1996). It allows the creation of virtual service networks, which have the potential to solve diverse problems in modern health care by increasing quality, accessibility and utilization effectiveness/efficiency as well as reducing costs (Bashshur, 1997) (U.S. Congress, 1995). This has motivated a fast growing interest and applications of telemedicine around the world (Ronie, 2001).

Despite such potential, many telemedicine innovations are either not accepted or not successfully implemented (Bangert, 2003) (Institute of Medicine, 1996). While various telemedicine pilot projects have been run worldwide, uptake and routine usage of such services is still subject to noticeable variations (EHTEL, 2008) (Office of Rural Health Policy, 1997). Reasons for the problems regarding the broad diffusion of telemedicine, typically, include poor technology performance, organizational issues, financial and legal barriers (Bashshur, 2000.) (EHTEL, 2008) (Telehealth Research Project, 2008) (Paul, 1999). It is also widely recognized that users of telemedicine services, physicians and other medical staff in most cases, are notorious for their non-responsiveness and resistance to the usage of information technologies (Anderson, 2005). Often, there also do not exist well-defined and long-term telehealth policies and coordination of telemedicine programs, which may result in premature funding termination.

Among those barriers, technological aspects of telemedicine products/services remain a challenge to the success of telemedicine projects (Paul, 1999). Telemedicine system and services include a broad spectrum of capabilities including acquisition, storage, presentation, and management of patient information (represented in different digital forms such as video, audio, or data), and communication of this information between care facilities with the use of communications links. (ISO, 2004).

And, telemedicine systems have a high criticality regarding their desired outcomes to the improvement of human health (LeRouge, 2004). This brings a great concern about safety, reliability, privacy, security, efficiency and effectiveness of telemedicine technology. For instance, does a radiologist at a central medical center, get radiological images with the proper resolution to effectively make a correct examination result? Are the patient's data and information protected against access of non-authorized persons? Will there be no erroneous mix ups of examination results to patients?

Many of the telemedicine systems in use today are adaptations of existing teleconferencing or desk top computer systems which were originally designed for purposes other than health care delivery. Although the system's individual components, such as software, may be regulated for safety, the entire telemedicine system is not necessarily evaluated objectively for its ability to safely provide diagnostic information. To further complicate the problem, telemedicine needs and practices are widely diverse and rapidly changing.

Given these concerns, there exists a legitimate interest in protecting the public from unsafe and untested telemedicine technologies. However, so far, there is no official telemedicine standard (ISO, 2004). So, commonly the telemedicine industry uses high-level health care guidelines and technical standards developed for various technology sectors including multimedia conferencing, information technology, data communications, and security. In this context, basically, three types of guidelines can be identified: clinical, operational and technical (Loane, 2002). Clinical guidelines addressing specific medical specialities, e.g., for teleradiology, telepsychiatry, surgical telemedicine or teledermatology. Operational guidelines focus on providing guidance on email communication, Internet access and videoconferencing, whereas technical guidelines cover specific aspects, such as interoperability, security, privacy, etc. Well-known examples, include DICOM (Digital Imaging and Communications in Medicine), a standard for the transfer of radiologic images and other medical information and HL7, a standard for the electronic interchange of clinical, financial and administrative information among independent health care oriented computer systems. However, the scarcity of guidelines and standards is still not comprehensive for the development of routine telemedicine products or services (Loane, 2002).

Yet, concerning the assessment and improvement of the software process for the development and maintenance of telemedicine systems and services is, basically, not covered by any standard so far. Such a standard or reference model is important when visioning the improvement of the product/ service quality as a result of a mature process executed for its development and maintenance. In this respect, there exist various well-accepted generic standards reference models focusing on software process assessment and improvement, including the CMMI framework (CMMI Product Team, 2006), ISO/IEC 12207 (ISO/IEC, 2008)/ ISO/IEC 15504 (ISO/IEC, 2003), or ITIL (ITIL, 2008). However, as being generic models, they do not provide specific support for telemedicine products or services. A step in this direction is the MEDI SPICE initiative, which is initiating work on a customisation of ISO/IEC 15504 for the development of medical devices (McCaffery, 2007).

In this context, the research objective of this work is to develop a customized reference process model for the development and maintenance of telemedicine software and services based on existing standards and models, such as ISO/IEC 12207, ISO/IEC 15504, CMMI framework, ITIL, etc. Such a tailored reference model is expected to facilitate software process assessment & improvement in this specific domain as well as to contribute positively to the quality of the systems and services being developed.

2 Telemedicine

Telemedicine is broadly defined as the use of information technology to deliver health care services and information from one location to another, geographically separated location (U.S. General Accounting Office, 1997) (Institute of Medicine, 1996). More particularly, these services can speed up diagnosis and therapeutic care delivery for emergencies, support virtual hospitals in patients' homes and allow primary healthcare providers in geographically dispersed locations to receive continuous assistance from specialised coordination centres.

Telemedicine covers a wide range of services and applications, and, while there is much disagreement about definitions (Tulu, 2005), telemedicine generally involves two general application purposes: clinical and non-clinical applications. Clinical applications of telemedicine can be classified as (Tulu, 2005): Triage, Diagnostic, Non-Surgical Treatment, Surgical Treatment, Consultation, Monitoring, Provision of specialty care, Supervision of primary care. Non-clinical purposes include medical education, research, administrative meetings.

Telemedicine can be applied for diverse medical specialties, including, for example,: Home Care, Microbiology and Immunology, Cardiology, Ophthalmology, Mental Health, Pathology, Dermatology, Radiology, Emergency Room, Pediatrics, etc. (Tulu, 2005).

Another aspect is the physical environment that the physician or patient will be using during the telemedicine event. This can range from a patient at a primary care hospital to a mobile patient, or a professional at a fully equipped hospital to a professional being reached at home (Tulu, 2005).

Delivery options refers to the applications provided to conduct a telemedicine event. In general, these events are classified in (Maheu, 2001.) (Coiera, 1997): (1) synchronous (real time) and (2) asynchronous (store-and-forward) events. Information transactions that occur among two or more number of participants simultaneously are called synchronous communications, e.g., telemedicine through telephone calls or robotic surgery. It requires the presence of both parties

at the same time and a communications link between them that allows a real-time interaction to take place. Video-conferencing equipment is one of the most common forms in synchronous telemedicine. There are also peripheral devices which can be attached to computers or the video-conferencing equipment which can aid in an interactive examination, such as, e.g., a tele-stethoscope. In asynchronous communications these transactions occur at different points in time (Glueckauf, 2002). Store-and-forward telemedicine involves acquiring medical data (like medical images, biosignals, etc) and then transmitting this data to a doctor or medical specialist at a convenient time for assessment offline. It does not require the presence of both parties at the same time.

The actual communication infrastructure can range from wired networks, radio waves, fiber optic lines, and many other forms of telecommunication technologies (Paul, 1999).

2.1 Focus on asynchronous store-and-forward telemedicine systems

In this broad field of telemedicine applications, we focus our research on asynchronous store-and-forward telemedicine systems for diagnostic purposes implemented as web-based systems. Such systems serve for the consultation of one (or more) distant health care professional(s) by a locally present health care professional about a patient‘s case, diagnosis and treatment a web-based telemedicine system to bridge the spatial distance between the two (or more) participants. Such systems offer opportunities of improving cooperation, especially among healthcare professionals, and simultaneously enhances the quality of patient care. Teleconsultations are increasingly used in those specialist fields of medicine, in which corresponding diagnostic findings data (mainly images) can be transmitted digitally, such as teleradiology, telecardiology, or teledermatology. For example, in the state of Santa Catarina/Brazil, a public asynchronous web-based telemedicine network is being build up that performs store-and-forward and examination and findings reports delivery in the fields of: clinical laboratory analysis, radiology (MR, OS, CT, SPECT, densitometry) endoscopy and colonoscopy, and EKG, besides asynchronous emergency assessment, mainly on trauma cases (Maia, 2006). Today, the network interconnects already more than 80 hospitals and primary health care facilities in 73 cities.

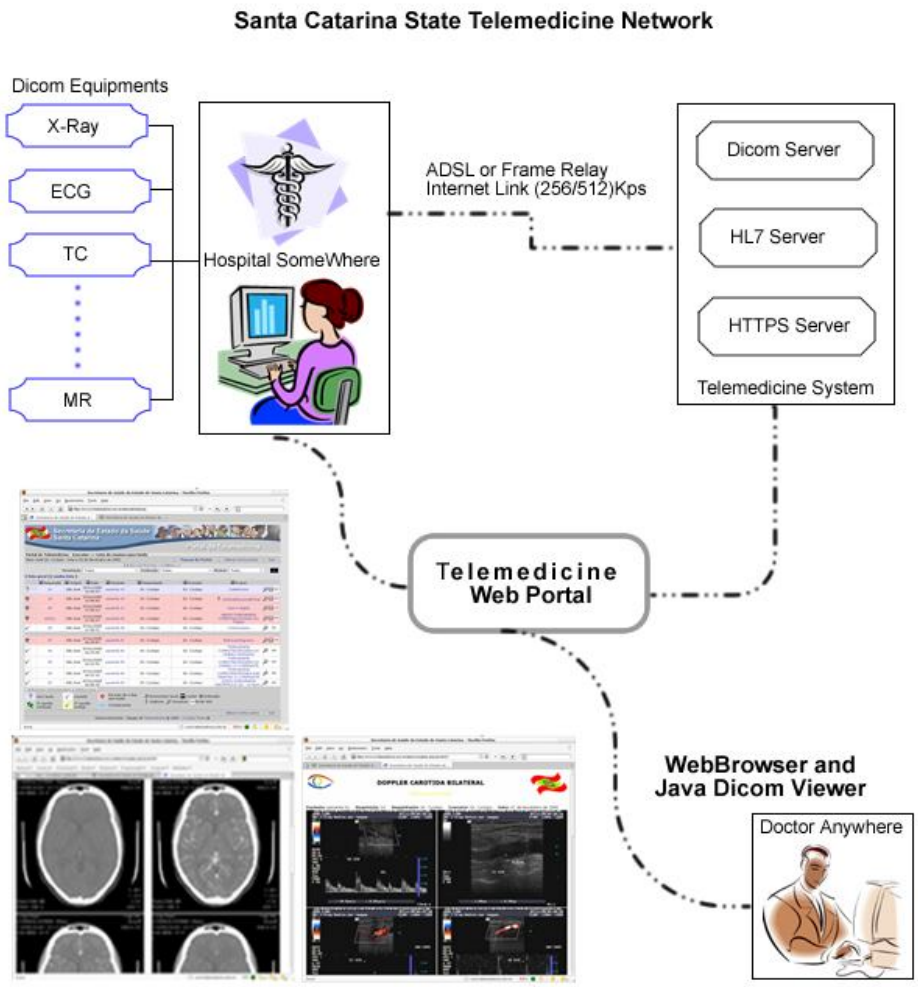

Figure 1. Conception of the Santa Catarina Telemedicine Network (Maia, 2006)

Asynchronous telemedicine systems are gaining increased acceptance and are becoming a preferred method, e.g., for obtaining second opinions of highly specialised physicians (EHTEL, 2008), as they do not require the simultaneous presence of doctors, required, for example, in teleconsultations via videoconference, which generally is extremely difficult as the likelihood of all physicians being available at the same time is a rarity. In addition, access to emerging telemedicine applications, such as tele-diagnosis and tele-care, is an issue of great concern to remotely situated primary health care facilities. However, economic considerations and infrequent consultation sessions may make the installation of high-speed lines required to provide remote facilities with these much-needed services impossible. On the other side, asynchronous web-based systems generally require less infrastructure including lower bandwidth for the purpose of batch mode diagnosis, operating over low-data rate communication lines.

A typical workflow of such asynchronous web-based diagnostic telemedicine systems is:

1. A patient is examined at a remote health care facility (hospital, primary health care facility, clinic, etc.) by a doctor, non-medical technical personnel or nurse. The examination is captured as an electronic file.

2. The examination and accompanying medical notes on the patient's medical record are sent electronically to a central telemedicine server and become available for medical staff responsible for tele-diagnosis.

3. The responsible medical doctor/specialist analyses the examination and notes in order to indicate findings and stores the findings together with the examination information on the central telemedicine server.

4. The examination information and findings become available for the requesting physician and the regulating commission.

5. The requesting physician analyses the examination and findings and provides a diagnosis and continues the patient's treatment.

From a technology standpoint, telemedicine is the application of telecommunications and computer technologies that are already in use in other industries (U.S. General Accounting Office, 1997) (Institute of Medicine, 1996) (Perednia, 1995). The technology includes the hardware, software, and communications link of the telemedicine project. The technology infrastructure is a telecommunications network with input and output devices at each connected location. An example of typical architecture of web-based asynchronous diagnostic telemedicine systems is shown in figure 2.

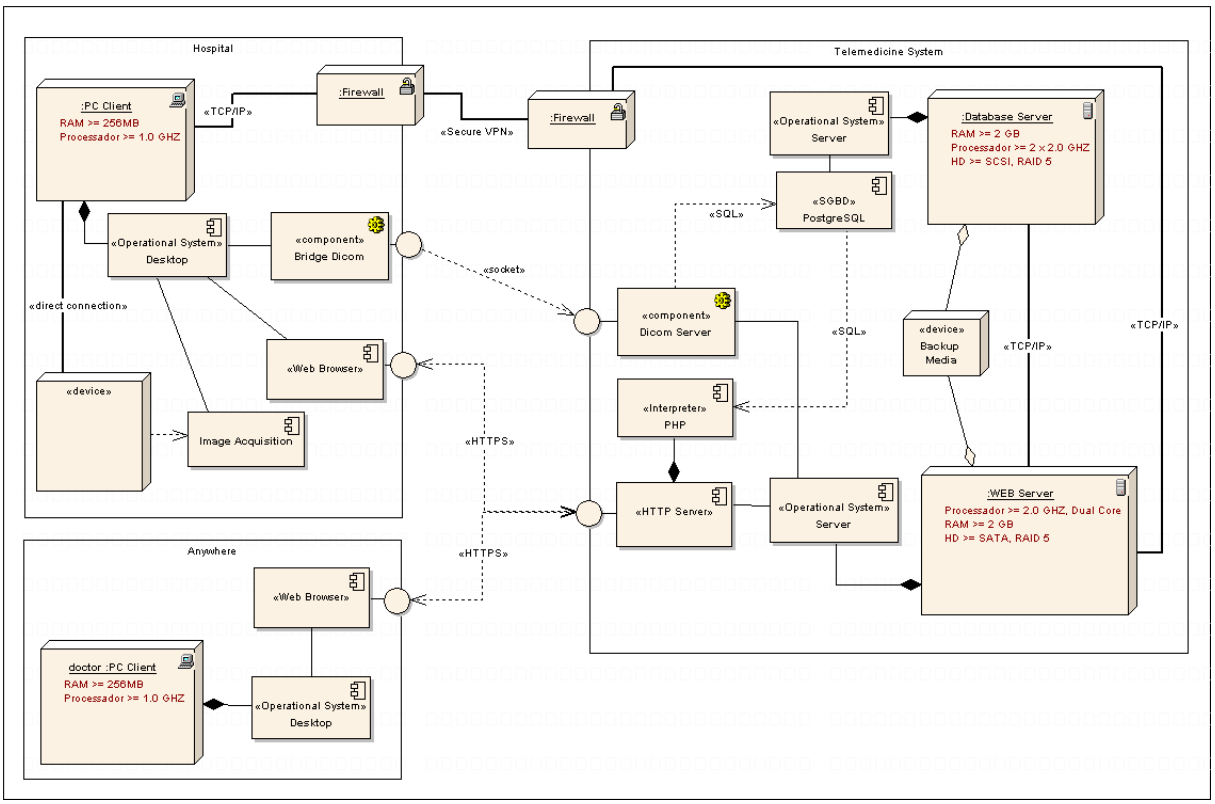

Figure 2. Architecture of web-based asynchronous diagnostic telemedicine systems

3 Software Process Capability/Maturity Model

The objective of this research work is to develop a tailored software process capability/maturity model for the assessment and improvement of the software development and maintenance of asynchronous store-and-forward telemedicine diagnosis systems (SPCMM-ASFTSs).

The basis for the SPCMM-ASFTSs is given by ISO/IEC 15504 (ISO/IEC, 2003), which provides a framework for the assessment of processes. This framework can be used by organizations involved in planning, managing, monitoring, controlling, and improving the acquisition, supply, development, operation, evolution and support of product.

Following the standard ISO/IEC 15504, the context of an assessment process is summarized in Figure 3.

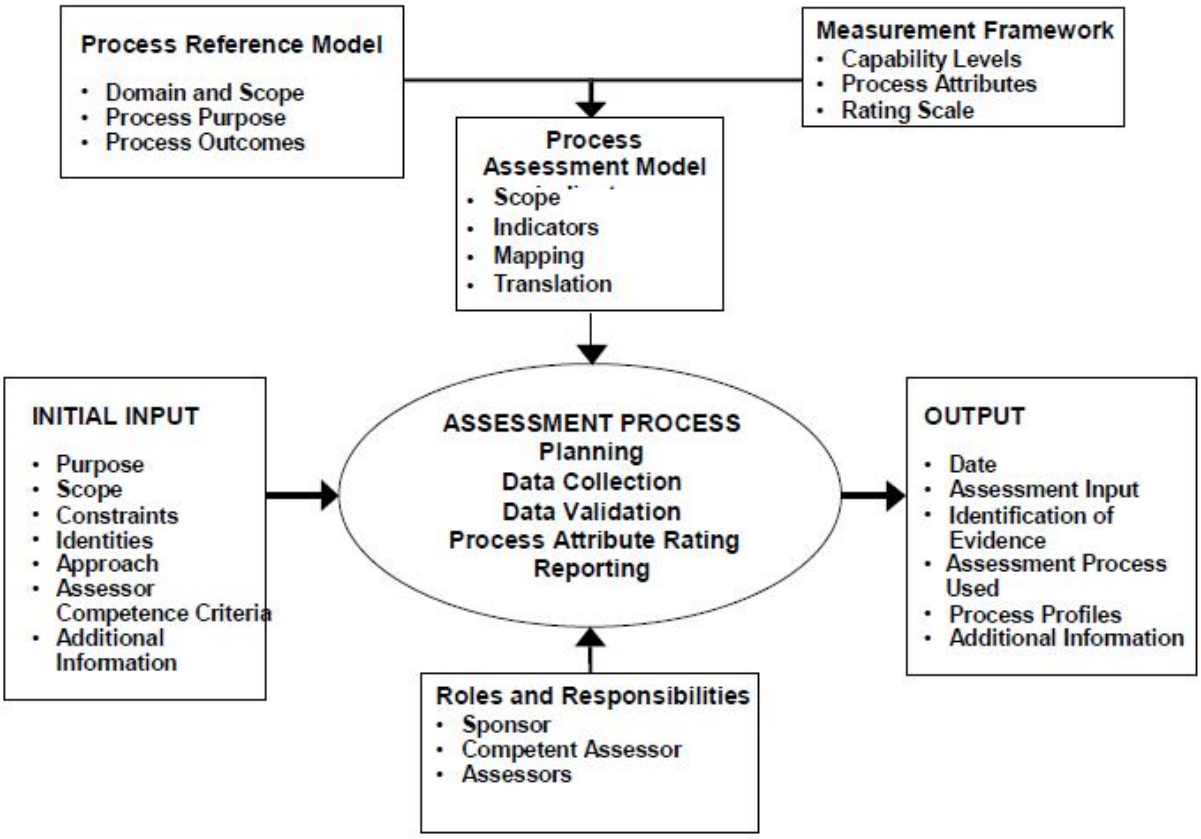

Figure 3. Major elements of the assessment process (ISO/IEC, 2003)

An assessment is carried out by assessing selected processes against the assessment model(s) chosen for the assessment. This assessment model(s) have to be compatible with the requirements defined in ISO/IEC 15504-2 and is selected according to the application domain of interest. Here, in the field of software engineering, we select the process model defined in ISO/IEC 12207. Figure 5 shows the relationship between a processs reference model, corresponding assessment model and the measurement framework. The two-dimensional model, as depicted in figure 5, consists of a set of processes defined in terms of their purpose and outcomes and a measurement framework which contains a set of process attributes. The process attributes apply across all processes. They are grouped into capability levels that may be used to determine the capability of the process. The assessment output includes a set of process profiles and optionally a capability level rating for each process assessed.

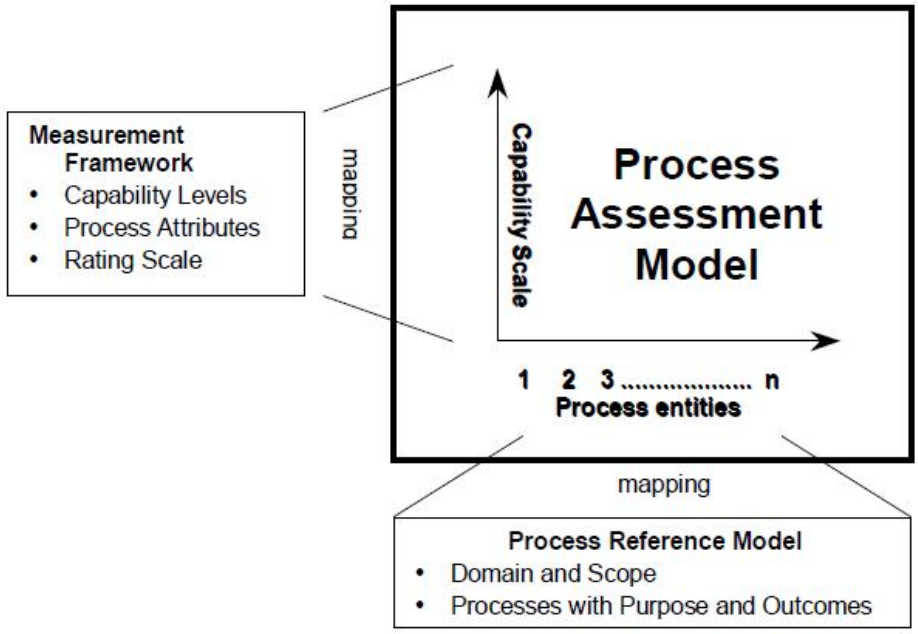

Figure 4. Process assessment model relationships

ISO/IEC 15504-2 defines a measurement framework that provides a basis for rating the capability of processes, based on their achievement of defined process attributes. ISO/IEC 15505-7 establishes a framework for determining overall Organizational Maturity, based upon assessed profiles of process capability.

3.1 Measurement framework

The measurement framework of SPCMM-ASFTSs is based on a continuous representation on ISO/IEC 15504-2 defining capability levels and on a staged representation based on ISO/IEC 15504-7 defining maturity levels.

3.1.1 Definition of process capability

Based on ISO/IEC 15504-2, process capability is defined on a six point ordinal scale that enables capability to be assessed from the bottom of the scale, **Incomplete**, through to the top end of the scale, **Optimizing**. The scale represents increasing capability of the implemented process, from not achieving the process purpose through to meeting current and projected business goals.

Within this Measurement Framework, the measure of capability is based upon a set of Process Attributes (PA). Each attribute defines a particular aspect of process capability. The extent of

process attribute achievement is characterised on a defined rating scale. The combination of process attribute achievement and a defined grouping of process attributes together determine the process capability level (Table 1).

Table 1. Capability Levels

Level 0: Incomplete process	The process is not implemented, or fails to achieve its process purpose. At this level there is little or no evidence of any systematic achievement of the process purpose.		
Level 1: Performed process	The implemented process achieves its process purpose.	**PA 1.1 Process performance attribute**	The process performance attribute is a measure of the extent to which the process purpose is achieved. As a result of full achievement of this attribute: a) the process achieves its defined outcomes.
Level 2: Managed process	The previously described *Performed process* is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.	**PA 2.1 Performance management attribute**	The performance management attribute is a measure of the extent to which the performance of the process is managed. As a result of full achievement of this attribute: a) objectives for the performance of the process are identified; b) performance of the process is planned and monitored; c) performance of the process is adjusted to meet plans; d) responsibilities and authorities for performing the process are defined, assigned and communicated; e) resources and information necessary for performing the process are identified, made available, allocated and used; f) interfaces between the involved parties are managed to ensure both effective communication and also clear assignment of responsibility
		PA 2.2 Work product management attribute	The work product management attribute is a measure of the extent to which the work products produced by the process are appropriately managed. As a result of full achievement of this attribute: a) requirements for the work products of the process are defined; b) requirements for documentation and control of the work products are defined; c) work products are appropriately identified, documented, and controlled; d) work products are reviewed in accordance with planned arrangements and adjusted as necessary to meet requirements.

Level 3: Established process	The previously described *Managed process* is now implemented using a defined process is capable of achieving its process outcomes.	**PA 3.1 Process definition attribute**	The process definition attribute is a measure of the extent to which a standard process is maintained to support the deployment of the defined process. As a result of full achievement of this attribute: a) a standard process, including appropriate tailoring guidelines, is defined that describes the fundamental elements that must be incorporated into a defined process; b) the sequence and interaction of the standard process with other processes is determined; c) required competencies and roles, for performing a process are identified as part of the standard process; d) required infrastructure and work environment for performing a process are identified as part of the standard process; e) Suitable methods for monitoring the effectiveness and suitability of the process are determined.
		PA 3.2 Process deployment attribute	The process deployment attribute is a measure of the extent to which the standard process is effectively deployed as a defined process to achieve its process outcomes. As a result of full achievement of this attribute: a) a defined process is deployed based upon an appropriately selected and/or tailored standard process; b) required roles, responsibilities and authorities for performing the defined process are assigned and communicated; c) personnel performing the defined process are competent on the basis of appropriate education, training, and experience; d) required resources and information necessary for performing the defined process are made available, allocated and used; e) required infrastructure and work environment for performing the defined process are made available, managed and maintained; f) appropriate data are, collected and analysed as a basis for understanding the behaviour of, and to demonstrate the suitability and effectiveness of the process, and to evaluate where continuous improvement of the process can be made.

Level 4: Predictable process	The previously described *Established process* now operates within defined limits to achieve its process outcomes.	**PA 4.1 Process measurement attribute**	The process measurement attribute is a measure of the extent to which measurement results are used to ensure that performance of the process supports the achievement of relevant process performance objectives in support of defined business goals. As a result of full achievement of this attribute: a) process information needs in support of relevant defined business goals are established; b) process measurement objectives are derived from process information needs; c) quantitative objectives for process performance in support of relevant business goals are established; d) measures and frequency of measurement are identified and defined in line with process measurement objectives and quantitative objectives for process performance e) results of measurement are collected, analysed and reported in order to monitor the extent to which the quantitative objectives for process performance are met; f) measurement results are used to characterise process performance.
		PA 4.2 Process control attribute	The process control attribute is a measure of the extent to which the process is quantitatively managed to produce a process that is stable, capable, and predictable within defined limits. As a result of full achievement of this attribute: a) analysis and control techniques are determined and applied where applicable; b) control limits of variation are established for normal process performance; c) measurement data are analysed for special causes of variation; d) corrective actions are taken to address special causes of variation; e) control limits are re-established (as necessary) following corrective action.

Level 5: Optimizing process	The previously described *Predictable process* is continuously improved to meet relevant current and projected business goals.	**PA 5.1 Process innovation attribute**	The process innovation attribute is a measure of the extent to which changes to the process are identified from analysis of common causes of variation in performance, and from investigations of innovative approaches to the definition and deployment of the process. As a result of full achievement of this attribute: a) process improvement objectives for the process are defined that support the relevant business goals; b) appropriate data are analysed to identify common causes of variations in process performance; c) appropriate data are analysed to identify opportunities for best practice and innovation; d) improvement opportunities derived from new technologies and process concepts are identified; e) an implementation strategy is established to achieve the process improvement objectives.
		PA 5.2 Process optimization attribute	The process optimization attribute is a measure of the extent to which changes to the definition, management and performance of the process result in effective impact that achieves the relevant process improvement objectives. As a result of full achievement of this attribute: a) impact of all proposed changes is assessed against the objectives of the defined process and standard process; b) implementation of all agreed changes is managed to ensure that any disruption to the process performance is understood and acted upon; c) effectiveness of process change on the basis of actual performance is evaluated against the defined product requirements and process objectives to determine whether results are due to common or special causes.

Rating process attributes

The **process attribute rating scale** is the extent of achievement of a process attribute is measured using an ordinal scale of measurement as defined below.

Process attribute rating values are defined through an ordinal rating scale that shall be used to express the levels of achievement of the process attributes.

Table 2. Process attribute ratings

N	Not achieved	There is little or no evidence of achievement of the defined attribute in the assessed process.	0 to 15% achievement
P	Partially achieved	There is some evidence of an approach to, and some achievement of, the defined attribute in the assessed process. Some aspects of achievement of the attribute may be unpredictable.	> 15% to 50% achievement
L	Largely achieved	There is evidence of a systematic approach to, and significant achievement of, the defined attribute in the assessed process. Some weakness related to this attribute may exist in the assessed process.	> 50% to 85% achievement
F	Fully achieved	There is evidence of a complete and systematic approach to, and full achievement of, the defined attribute in the assessed process. No significant weaknesses related to this attribute exist in the assessed process.	> 85% to 100% achievement

Process attribute ratings. Each process attribute shall be rated using the ordinal rating scale defined above. A process shall be assessed up to and including the highest capability level defined in the assessment scope.

Process capability level model

The capability level achieved by a process shall be derived from the process attribute ratings for that process according to the process capability level model defined in table 3.

Table 3. Capability level ratings

Scale	Process Attributes	Rating
Capability Level 1	Process Performance	Largely or fully
Capability Level 2	Process Performance	Fully
	Performance Management	Largely or fully
	Work Product Management	Largely or fully
Capability Level 3	Process Performance	Fully
	Performance Management	Fully
	Work Product Management	Fully
	Process Definition	Largely or fully
	Process Deployment	Largely or fully
Capability Level 4	Process Performance	Fully
	Performance Management	Fully
	Work Product Management	Fully
	Process Definition	Fully
	Process Deployment	Fully
	Process Measurement	Largely or fully
	Process Control	Largely or fully
Capability Level 5	Process Performance	Fully
	Performance Management	Fully
	Work Product Management	Fully
	Process Definition	Fully
	Process Deployment	Fully
	Process Measurement	Fully
	Process Control	Fully
	Process Innovation	Largely or fully
	Process Optimization	Largely or fully

3.1.2 Definition of Organizational Maturity

As defined ISO/IEC 15504-7, **Organizational Maturity** is an expression of the extent to which an organization consistently implements processes within a defined scope that contributes to the achievement of its business goals (current or projected).

Organizational maturity is defined on a six point ordinal scale that enables maturity to be assessed from the bottom of the scale, Level 0 Organization - **the Immature Organization**, through to the top end of the scale, Level 5 Organization - **the Innovating Organization**. The scale represents the extent to which the organization has explicitly and consistently performed, managed and established it processes with predicable performance and demonstrated the ability to change and adapt the performance of the processes fundamental to achieving the organization's business goals.

Table 4. Organizational Maturity Levels

Level 0 Organization - Immature	The organization does not demonstrate effective implementation of its processes that are fundamental to support the organization's business.		At least one process in the basic process set is assessed at Capability Level 0.
Level 1 Organization - Basic	The organization demonstrates achievement of the purpose of the processes that are fundamental to support the organization's business.	As a result of achieving this level of maturity, the organization: a) implements the processes required to support the organization's business; b) performs sets of activities and tasks that achieve the purposes of these processes.	All processes in the basic process set are assessed at Capability Level 1 or higher.
Level 2 Organization – Managed	The organization demonstrates management of the processes that are fundamental to support the organization's business.	As a result of achieving this level of maturity, the organization: a) establishes plans for the performance of the processes that are fundamental to support the organization's business; b) acts to ensure effective communication regarding the performance of the processes, through clear assignment of responsibilities and authorities to involved parties; c) allocates adequate resources and information to ensure implementation of the plans; d) monitors performance of the processes against plans in the individual instances; e) takes action to address deviation from planned performance of the process; f) identifies requirements for the management of work products developed by the processes; g) takes action through appropriate reviews and control mechanisms to ensure that the requirements for work product management are satisfied.	All processes in the basic process set are assessed at Capability Level 2 or higher. The extended process set incorporates additional processes that ensure management of process performance and work product integrity. The processes in the extended process set are assessed at Capability Level 2 or higher.
Level 3	The organization	As a result of achieving this level of maturity, the	All processes in the basic

Organization – Established	demonstrates effective definition and deployment of the processes that are fundamental to support the organization's business.	organization: a) establishes standard process descriptions covering all of the basic and extended sets of processes employed on a routine basis in the organization; b) ensures that individual implementations of the processes are performed as defined processes with appropriately tailored standard processes; c) collects and analyses data and information from the performance of the defined processes and stores this data for use across the organization; d) uses the collected data and information to improve both the standard and defined processes.	process set are assessed at Capability Level 3 or higher. The extended process set incorporates additional processes that ensure that processes are established and deployed using a defined process that is capable of achieving its process outcomes. The processes in the extended process set are assessed at Capability Level 3 or higher.
Level 4 Organization – Predictable	The organization demonstrates a quantitative understanding of relevant processes that are fundamental to support the organization's business goals, in order to establish consistent and predictable performance.	As a result of achieving this level of maturity, the organization: a) establishes quantitative objectives for process performance, based upon business goals; b) selects processes for process performance analyses, covering at a minimum the basic process set, on the basis of their relevance and significance to the achievement of business goals; c) employs effective measurement to collect, store and analyse data on the performance of the selected processes; d) identifies special causes of variation in the performance of the selected processes and takes appropriate corrective and preventive action to address them; e) establishes stable, capable and predictable performance of the selected processes within defined control limits.	One or more of the processes in the basic process set, selected on the basis of their relevance and significance to support the organization's business goals, are assessed at Capability Level 4 or higher. The extended process set incorporates additional processes that support the achievement of a quantitative understanding of the performance of relevant processes in the overall process profile of the organization. The processes in the extended process set are assessed at Capability Level 3 or higher; one or more of the processes in the extended process set may be assessed at Capability Level 4 or higher.
Level 5 Organization – Innovating	The organization demonstrates the ability to change and adapt the performance of the processes that are fundamental to support the organization's business goals in a systematically planned and predictable manner.	As a result of achieving this level of maturity, the organization: a) identifies common causes of variation in process performance, based on results of process performance analysis, and identifies candidate improvements to address these, in the light of the business goals; a) identifies innovations with the potential to improve process performance and business success; b) identifies opportunities for piloting potential innovative and incremental improvements with control of associated risk; c) collects and analyses data from the pilot implementations, and uses the results of analysis to select improvements for organizational deployment based on their impact on process performance and business success; d) deploys the improvements, monitors	One or more of the processes in the basic process set, selected on the basis of their relevance and significance to support the organization's business goals, ,are assessed at Capability Level 5. The extended process set incorporates additional processes that support the continuous and predictable improvement of process performance. The processes in the extended process set are assessed at Capability Level 3 or higher; one or more of the processes in the extended process set may be assessed at Capability Level 5.

		performance of the improved processes and compares the results of improvement to expected values.	

Each level of Organizational Maturity is characterised by the demonstration of achievement of specified levels of Process Capability in process sets based on the specified Process Reference Model(s). Processes can be categorized into 5 sets based on their contributions to the business goals of the organization. The set of fundamental processes that support the business is called the basic process set. Each organizational Maturity Level beyond level 1 maturity is characterized by the implementation, at an appropriate level of Process Capability, of a further set of processes that drive the achievement of the capabilities relevant to each Maturity Level. These are called extended process sets.

An Organizational Maturity Model shall include a set of elements from the Process Assessment Model(s) constituting the **basic process set** for the model. The basic process set shall include:
– A minimum set of elements that define Level 1 Maturity for all assessments based on the model;
– Additional elements that are required for assessments in particular domains or scope of application; and
– Additional elements that are optional depending on the particular circumstances of the organization.
The model shall include specifications of the particular circumstances for inclusion of the additional processes in the basic process set, and an indication of how the use of additional processes is to be reflected in the published assessment record. The model shall define, through reference to the established mapping of the Process Assessment Model(s), the processes from relevant Process Reference Model(s) that constitute the basic process set.

An Organizational Maturity Model shall include sets of elements constituting the **extended process sets** for each Maturity Level addressed by the model. The extended process sets shall include:
– A minimum set of elements that define the specified level of Maturity for all assessments based on the
model;
– Additional elements that are required for assessments with particular scope of application; and

– Additional elements that are optional depending on the particular circumstances of the organization.

The model shall include specifications of the particular circumstances for inclusion of the additional processes in the extended process set, and an indication of how the use of additional processes is to be reflected in the published assessment record. The model shall define, through reference to the established mapping of the Process Assessment Model(s), the processes from relevant Process Reference Model(s) that constitute each extended process set.

Table 5. Processes associated to Maturity Levels

	ML	List of Processes	Minimum Set	Additional processes	
				ID	Conditions
Basic process set	**1**	1.4.1 Stakeholder Requirements Definition 1.4.1 System Requirements Analysis 1.4.3 System Architectural Design 2.1.1 Software Requirements Analysis 2.1.3 Software Architectural Design 2.1.4 Software Detailed Design 2.1.5 Software Construction 2.1.6 Software Integration 2.1.7 Software Qualification Testing 1.4.5 System Integration 1.4.6 System Qualification Testing 1.4.7 Software Installation 1.4.10 Software Maintenance 2.4.2 Safety Engineering 2.5.1 Administer Security Controls 2.5.2 Assess Impact 2.5.3 Assess Security Risk 2.5.4 Assess Threat 2.5.5 Assess Vulnerability 2.5.6 Build Assurance Argument 2.5.7 Coordinate Security 2.5.8 Monitor Security Posture 2.5.9 Provide Security Input 2.5.10 Specify Security Needs 2.5.11 Verify and Validate Security 2.6.2 Context of Use Specification 2.6.3 HCD Solution Production 2.6.4 HCD Evaluation	1.4.1 Stakeholder Requirements Definition 2.1.1 Software Requirements analysis 2.1.3 Software Architectural Design 2.1.4 Software Detailed Design 2.1.5 Software Construction 2.1.6 Software Integration 2.1.7 Software Qualification Testing 2.4.2 Safety Engineering 2.5.1 Administer Security Controls 2.5.2 Assess Impact 2.5.3 Assess Security Risk 2.5.4 Assess Threat 2.5.5 Assess Vulnerability 2.5.6 Build Assurance Argument 2.5.7 Coordinate Security 2.5.8 Monitor Security Posture 2.5.9 Provide Security Input 2.5.10 Specify Security Needs 2.5.11 Verify and Validate Security	1.4.1 System Requirements Analysis 1.4.3 System Architectural Design 1.4.5 System Integration 1.4.6 System Qualification Testing	Required where development covers system issues and not exclusively software issues.

			2.6.2 Context of use specification process 2.6.3 HCD solution production process 2.6.4 HCD evaluation process		
				1.4.7 Software Installation	Required where the OU is responsible for installing the software product in the customer environment.
				1.4.10 Software Maintenance	Required where the OU is responsible for ongoing maintenance and evolution of the software and/or system.
Extended Process sets	**2**	2.2.3 Software Quality Assurance 2.2.4 Software Verification 2.2.5 Software Validation 2.2.6 Software Review 2.2.1 Software Documentation Management 2.2.2 Software Configuration Management 2.2.8 Software Problem Resolution Management 2.2.9 Change Request Management 1.3.1 Project Planning 1.3.2 Project Assessment and Control 1.3.2 Risk Management 1.3.6 Information Management 1.1.1 Acquisition 1.1.2 Supply 2.4.1 Safety Management 2.5.12 Manage Product Line Evolution Process	1.1.2 Supply 2.2.4 Software Verification 2.2.1 Software Documentation Management 2.2.2 Software Configuration Management 2.2.8 Software Problem Resolution Management 2.2.9 Change Request Management 1.3.1 Project Planning 1.3.2 Project Assessment and Control 1.3.4 Risk Management 2.4.1 Safety Management 2.5.12 Manage Product Line Evolution Process	1.1.1 Acquisition	Required where external or internal suppliers of product components, services or infrastructure are involved in the development projects.
				2.2.5 Software Validation	Optional.
				1.1.2 Supply	Optional where the work in the OU involves product acceptance support.
	3	1.2.3 Project Portfolio Management 1.2.4 Human Resource	1.2.4 Human Resource	2.3.2 Reuse Asset	Optional if the OU has a structured reuse

		Management 1.2.2 Infrastructure Management 1.2.1 Life Cycle Model Management 1.2.6 Organization Management 1.2.5 Quality Management 1.3.7 Measurement 2.2.7 Software Audit 2.3.2 Reuse Asset Management 2.3.3 Reuse Program Management 2.3.1 Domain Engineering 2.4.3 Safety Qualification 2.6.1 HCD strategy 2.7.1 Scoping 2.7.2 Funding 2.7.3 Market Analysis 2.7.4 Organizational Planning 2.7.5 Organizational Risk Management 2.7.6 Structuring the Organization 2.7.7 Technology Forecasting	Management 1.2.2 Infrastructure Management Life Cycle Model Management 1.2.6 Organization Management 1.2.5 Quality Management 1.3.7 Measurement 2.2.7 Software Audit 2.4.3 Safety Qualification 2.6.1 HCD strategy 2.7.1 Scoping 2.7.2 Funding 2.7.3 Market Analysis 2.7.4 Organizational Planning 2.7.5 Organizational Risk Management 2.7.6 Structuring the Organization 2.7.7 Technology Forecasting	Management 2.3.3 Reuse Program Management 2.3.1 Domain Engineering	program in force - the three processes are mutually reinforcing.
	4	N/A	N/A	N/A	N/A
	5	N/A	N/A	N/A	N/A

3.2 Definition of Process Reference Model

Process Reference Models provide the mechanism whereby defined Process Assessment Models are related to the Measurement Framework defined by ISO/IEC 15504. A Process Reference Model is defined external to ISO/IEC 15504 and provides the basis for one or more Process Assessment Models. Process Assessment Model(s) are based on the process descriptions provided in Process Reference Models. In order to assure that assessment results are translatable into an ISO/IEC 15504 process profile in a repeatable and reliable manner, Process Reference Models shall adhere to certain requirements.

Following ISO/IEC 15504-2, a Process Reference Model shall contain:

a) a declaration of the domain of the Process Reference Model;

b) a description of the processes, meeting the requirements of clause 6.2.4 of this International Standard, of the processes within the scope of the Process Reference Model;

c) a description of the relationship between the Process Reference Model and its intended context of use;
d) a description of the relationship between the processes defined within the Process Reference Model;
e) the Process Reference Model shall document the community of interest of the model and the actions taken to achieve consensus within that community of interest:
   1) the relevant community of interest will be characterized or specified;
   2) the extent of achievement of consensus shall be documented;
   3) if no actions are taken to achieve consensus, a statement to this effect shall be documented;
f) The processes defined within a Process Reference Model shall have unique process descriptions and identification.

The fundamental elements of a Process Reference Model are the **process descriptions** of the processes within the scope of the model. The process descriptions in the Process Reference Model incorporate a statement of the purpose of the process which describes at a high level the overall objectives of performing the process, together with the set of outcomes which demonstrate successful achievement of the process purpose. These process descriptions shall meet the following requirements:

g) a process shall be described in terms of its purpose and outcomes;
h) in any process description the set of process outcomes shall be necessary and sufficient to achieve the purpose of the process;
i) process descriptions shall be such that no aspects of the Measurement Framework as described in clause 5 of this International Standard beyond level 1 are contained or implied.

An outcome statement describes one of the following:

— Production of an artefact;
— A significant change of state;
— Meeting of specified constraints, e.g. requirements, goals etc.

Considering the context of this work, the international standard ISO/IEC 12207 provides an adequate base for defining a process reference model. **ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes** is an international standard that provides a comprehensive set of life cycle processes, activities and tasks for software that is part of a larger system, and for stand-alone software products and services. Annex B of ISO/IEC

12207:2008 defines a Process Reference Model (PRM) at a level of abstraction higher than that of the detailed requirements contained in the main text of this International Standard that is applicable to an organization that is assessing its processes in order to determine the capability of these processes. The PRM is intended to be used to develop assessment model(s) for assessing processes using ISO/IEC 15504-2.

ISO/IEC 12207:2008 groups the activities that may be performed during the life cycle of a software system into seven process groups (Figure 5). Each of the life cycle processes within those groups is described in terms of its purpose and desired outcomes and lists activities and tasks which need to be performed to achieve those outcomes.

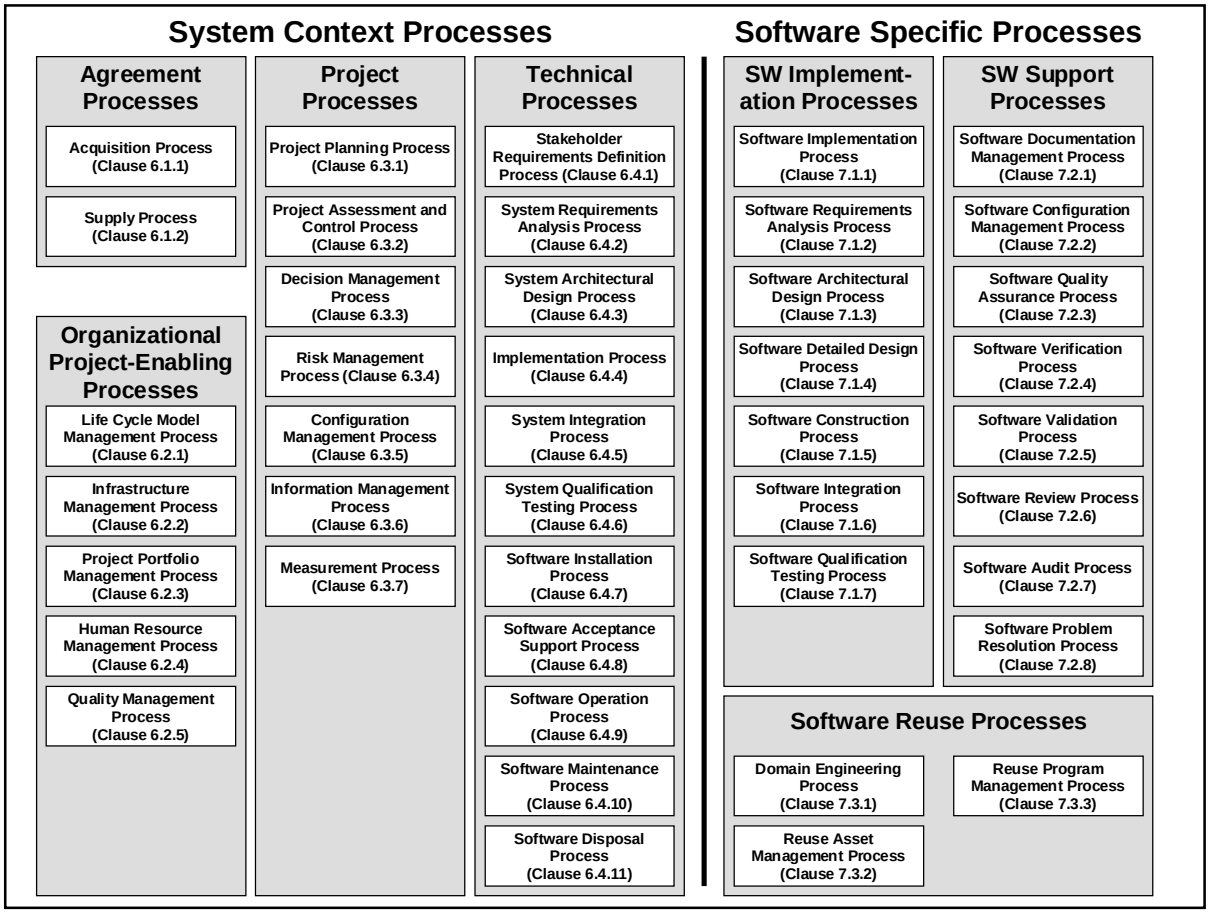

Figure 5. Life Cycle Process Groups

Tailoring of process reference model to the context of ASFTSs

In order to attend specific needs and characteristics of a specific domain, standard process reference models, such as ISO/IEC 12207, have to be tailored. This means that processes can be selected or modified in accordance with the tailoring process prescribed in ISO/IEC 12207 - Annex A.

Based on the contextualization of ASFTSs and the software quality model for ASFTSs as defined in (Wangenheim & Wangenheim, 2011), we tailor the standard ISO/IEC 15504 by adding additionally relevant processes. An overview of the resulting process reference model, its groups and processes including the references to the source of each of the processes is given in Table 6.

Table 6. Process reference model for ASFTSs

Process number	Process Name	Source	Source process number	Source process name
1	**System Life Cycle Processes**	ISO/IEC 12207:2008	6	System Life Cycle Processes
1.1	Agreement Processes	ISO/IEC 12207:2008	6.1	Agreement Processes
1.1.1	Acquisition	ISO/IEC 12207:2008	6.1.1	Acquisition Process
1.1.2	Supply	ISO/IEC 12207:2008	6.1.2	Supply Process
1.2	Organizational Project-Enabling Processes	ISO/IEC 12207:2008	6.2	Organizational Project-Enabling Processes
1.2.1	Life Cycle Model Management	ISO/IEC 12207:2008	6.2.1	Life Cycle Model Management Process
1.2.2	Infrastructure Management	ISO/IEC 12207:2008	6.2.2	Infrastructure Management Process
1.2.3	Project Portfolio Management	ISO/IEC 12207:2008	6.2.3	Project Portfolio Management Process
1.2.4	Human Resource Management	ISO/IEC 12207:2008	6.2.4	Human Resource Management Process
1.2.5	Quality Management	ISO/IEC 12207:2008	6.2.5	Quality Management Process
1.2.6	Organization Management	ISO/IEC 15504-5:2006	MAN.1	Organization management
1.3	Project Processes	ISO/IEC 12207:2008	6.3	Project Processes
1.3.1	Project Planning	ISO/IEC 12207:2008	6.3.1	Project Planning Process
1.3.2	Project Assessment and Control	ISO/IEC 12207:2008	6.3.2	Project Assessment and Control Process
1.3.3	Decision Management	ISO/IEC 12207:2008	6.3.3	Decision Management Process
1.3.4	Risk Management	ISO/IEC 12207:2008	6.3.4	Risk Management Process
1.3.5	Configuration Management	ISO/IEC 12207:2008	6.3.5	Configuration Management Process
1.3.6	Information Management	ISO/IEC 12207:2008	6.3.6	Information Management Process

Process number	Process Name	Source	Source process number	Source process name
1.3.7	Measurement	ISO/IEC 12207:2008	6.3.7	Measurement Process
1.4	Technical Processes	ISO/IEC 12207:2008	6.4	Technical Processes
1.4.1	Stakeholder Requirements Definition	ISO/IEC 12207:2008	6.4.1	Stakeholder Requirements Definition Process
1.4.2	System Requirements Analysis	ISO/IEC 12207:2008	6.4.2	System Requirements Analysis
1.4.3	System Architectural Design	ISO/IEC 12207:2008	6.4.3	System Architectural Design
1.4.4	Implementation	ISO/IEC 12207:2008	6.4.4	Implementation Process
1.4.5	System Integration	ISO/IEC 12207:2008	6.4.5	System Integration Process
1.4.6	System Qualification Testing	ISO/IEC 12207:2008	6.4.6	System Qualification Testing Process
1.4.7	Software Installation	ISO/IEC 12207:2008	6.4.7	Software Installation
1.4.8	Software Acceptance Support	ISO/IEC 12207:2008	6.4.8	Software Acceptance Support
1.4.9	Software Operation	ISO/IEC 12207:2008	6.4.9	Software Operation Process
1.4.10	Software Maintenance	ISO/IEC 12207:2008	6.4.10	Software Maintenance Process
1.4.11	Software Disposal	ISO/IEC 12207:2008	6.4.11	Software Disposal Process
2	**Software Life Cycle Processes**	**ISO/IEC 12207:2008**	**7**	**Software Life Cycle Processes**
2.1	Software Implementation Processes	ISO/IEC 12207:2008	7.1	Software Implementation Processes
2.1.1	Software Implementation	ISO/IEC 12207:2008	7.1.1	Software Implementation Process
2.1.2	Software Requirements Analysis	ISO/IEC 12207:2008	7.1.2	Software Requirements Analysis Process
2.1.3	Software Architectural Design	ISO/IEC 12207:2008	7.1.3	Software Architectural Design Process
2.1.4	Software Detailed Design	ISO/IEC 12207:2008	7.1.4	Software Detailed Design Process
2.1.5	Software Construction	ISO/IEC 12207:2008	7.1.5	Software Construction Process
2.1.6	Software Integration	ISO/IEC 12207:2008	7.1.6	Software Integration Process
2.1.7	Software Qualification Testing	ISO/IEC 12207:2008	7.1.7	Software Qualification Testing Process
2.2	Software Support Processes	ISO/IEC 12207:2008	7.2	Software Support Processes
2.2.1	Software Documentation Management	ISO/IEC 12207:2008	7.2.1	Software Documentation Management Process
2.2.2	Software Configuration Management	ISO/IEC 12207:2008	7.2.2	Software Configuration Management Process
2.2.3	Software Quality Assurance	ISO/IEC 12207:2008	7.2.3	Software Quality Assurance Process

Process number	Process Name	Source	Source process number	Source process name
2.2.4	Software Verification	ISO/IEC 12207:2008	7.2.4	Software Verification Process
2.2.5	Software Validation	ISO/IEC 12207:2008	7.2.5	Software Validation Process
2.2.6	Software Review	ISO/IEC 12207:2008	7.2.6	Software Review Process
2.2.7	Software Audit	ISO/IEC 12207:2008	7.2.7	Software Audit Process
2.2.8	Software Problem Resolution	ISO/IEC 12207:2008	7.2.8	Software Problem Resolution Process
2.2.9	Change Request Management	ISO/IEC 15504-5:2006	SUP.10	Change request management
2.3	Software Reuse Processes	ISO/IEC 12207:2008	7.3	Software Reuse Processes
2.3.1	Domain Engineering	ISO/IEC 12207:2008	7.3.1	Domain Engineering Process
2.3.2	Reuse Asset Management	ISO/IEC 12207:2008	7.3.2	Reuse Asset Management Process
2.3.3	Reuse Program Management	ISO/IEC 12207:2008	7.3.3	Reuse Program Management Process
2.4	Safety Engineering Processes	ISO/IEC PRF TS 15504-10 Information technology -- Process assessment -- Part 10: Safety extension		
2.4.1	Safety Management	ISO/IEC PRF TS 15504-10	SAF.1	Safety Management
2.4.2	Safety Engineering	ISO/IEC PRF TS 15504-10	SAF.2	Safety Engineering
2.4.3	Safety Qualification	ISO/IEC PRF TS 15504-10	SAF.3	Safety Qualification
2.5	Security Engineering Processes	ISO/IEC 21827:2008 Systems Security Engineering Capability Maturity Model (SSE-CMM)		
2.5.1	Administer Security Controls	ISO/IEC 21827:2008	PA01	Administer Security Controls Process
2.5.2	Assess Impact	ISO/IEC 21827:2008	PA02	Assess Impact Process
2.5.3	Assess Security Risk	ISO/IEC 21827:2008	PA03	Assess Security Risk Process
2.5.4	Assess Threat	ISO/IEC 21827:2008	PA04	Assess Threat Process
2.5.5	Assess Vulnerability	ISO/IEC 21827:2008	PA05	Assess Vulnerability Process
2.5.6	Build Assurance Argument	ISO/IEC 21827:2008	PA06	Build Assurance Argument Process
2.5.7	Coordinate Security	ISO/IEC 21827:2008	PA07	Coordinate Security Process
2.5.8	Monitor Security Posture	ISO/IEC 21827:2008	PA08	Monitor Security Posture Process
2.5.9	Provide Security Input	ISO/IEC 21827:2008	PA09	Provide Security Input Process
2.5.10	Specify Security Needs	ISO/IEC 21827:2008	PA10	Specify Security Needs Process
2.5.11	Verify and Validate Security	ISO/IEC 21827:2008	PA11	Verify and Validate Security Process
2.5.12	Manage Product Line Evolution	ISO/IEC 21827:2008	PA20	Manage Product Line Evolution Process

Process number	Process Name	Source	Source process number	Source process name
2.6	Usability Engineering	ISO/TR 18529:2000 Ergonomics -- Ergonomics of human-system interaction -- Human-centred lifecycle process descriptions		
2.6.1	HCD Strategy	ISO/TR 18529:2000	HCD.1	Ensure HCD content in system strategy
2.6.2	Context of Use Specification	ISO/TR 18529:2000	HCD.4	Understand and specify the context of use
2.6.3	HCD Solution Production	ISO/TR 18529:2000	HCD.5	Produce design solutions
2.6.4	HCD Evaluation	ISO/TR 18529:2000	HCD.6	Evaluate designs against requirements
2.7	Software Product Line Engineering Processes	A Framework for Software Product Line Practice (v5.0)		
2.7.1	Scoping	A Framework for Software Product Line Practice		Scoping
2.7.2	Funding	A Framework for Software Product Line Practice		Funding
2.7.3	Market Analysis	A Framework for Software Product Line Practice		Market Analysis
2.7.4	Organizational Planning	A Framework for Software Product Line Practice		Organizational Planning
2.7.5	Organizational Risk Management	A Framework for Software Product Line Practice		Organizational Risk Management
2.7.6	Structuring the Organization	A Framework for Software Product Line Practice		Structuring the Organization
2.7.7	Technology Forecasting	A Framework for Software Product Line Practice		Technology Forecasting

3.2.1 ISO/IEC 15504-5 Extensions

Process ID	1.2.6		
Process Name	Organization Management		
Process Purpose	The purpose of the Organization management process is to establish and perform software management practices, during the performance of the processes, needed for providing software products and services that are consistent with the business goals of the organization. NOTE: Although organizational operations in general have a much broader scope than that of software process, software processes are implemented in a business context and to be effective, require an appropriate organizational environment.		
Process Outcomes	As a result of the successful implementation of Organization management process: 1) the organization will invest in the appropriate management infrastructure; 2) the best practices are identified to support the implementation of effective organization and project management; and 3) provide a basis for evaluating the achievement of organization business goals based on these management practices.		
Base Practices	**BP1: Identify management infrastructure**. Identify management infrastructure appropriate to perform software management practices that are consistent with the business goals of the organization. [Outcome: 1] NOTE 1: Management infrastructure may include organizational roles and responsibilities, decision-making system, communication mechanisms and planning / monitoring of business operations. **BP2: Provide management infrastructure**: Provide the identified management infrastructure appropriate in organization's broader scope. [Outcome: 1] **BP3: Identify and implement software management practices.** Identify and implement effective software management practices to implement and improve competitive software processes and to construct effective organizations and effective enterprise project management. [Outcome: 2] **BP4: Perform identified management practices.** Perform management practices using management infrastructure. [Outcome: 2] **BP5: Evaluate effectiveness.** Evaluate the effectiveness of implemented software management practices to achieve the related organization business goals. [Outcome: 3] **BP6: Provide support to adopt best practices**. Use incentive approaches and software management infrastructure to support implementation of effective software management practices. [Outcome: 2, purpose] NOTE 2: Best practice may be related to the achieved or next capability level. See Knowledge management process (RIN.3) to manage and disseminate best practices as part of organizational knowledge assets.		

Process ID	2.2.9		
Process Name	Change Request Management		
Process Purpose	The purpose of the Change request management process is to ensure that change requests are managed, tracked and controlled.		
Process Outcomes	As a result of successful implementation of the Change request management process: 1) a change management strategy is developed; 2) requests for changes are recorded and identified; 3) dependencies and relationships to other change requests are identified; 4) criteria for confirming implementation of change requests are defined; 5) requests for change are prioritized, and resource requirements estimated; 6) changes are approved on the basis of priority and availability of resources; 7) approved changes are implemented and tracked to closure; and 8) the status of all change requests is known.		
Base Practices	**BP1: Develop a change management strategy**. A change management strategy is established and implemented to ensure changes can be described, recorded, analyzed, and actioned. [Outcome: 1] **BP2: Record the request for change.** Each change request is uniquely identified, and recorded. [Outcome: 2]		

	BP3: Record the status of change requests. Change requests and changes are allocated a status indication to facilitate tracking. [Outcome: 8] NOTE 1: Provide traceability to the reason for the change. Change requests submitted as a resolution to a problem or error report should retain a link to the originating problem or error report. [Outcome: 3] **BP4: Establish the dependencies and relationships to other change requests**. Identify the relationship of a change request to other change requests to establish dependencies (e.g. towards another change to the same software element or for a set of changes related to a planned release). [Outcome: 3] **BP5: Assess the impact of the change.** Assess the impact, resources, risks, and potential benefits of the change request and establish criteria for confirming implementation. [Outcome: 4, 5] NOTE 2: A Change Request Board (CRB) is a common mechanism used to assess change requests. When conducting impact and resource assessment, the effect on the infrastructure and users must be considered together with the resources required for implementing the change, including likely costs, the number and availability of people and the elapsed time to implement. **BP6: Identify the verification and validation activities to be performed for implemented changes**. Before implementing a change the scope of verification and validation activities to be undertaken are identified. [Outcome: 7] **BP7: Approve changes**. All changes are approved before implementation. [Outcome: 6] **BP8: Implement the change**. Approved changes are implemented. [Outcome: 5, 7] NOTE 3: Scheduled changes may be incorporated into target releases. A packaged release may incorporate corrective and adaptive changes. **BP9: Review the implemented change.** All changes are reviewed after implementation and before closure to ensure that they had the desired effect and met their objectives. [Outcome:7, 8]

3.2.2 Safety Engineering

In order to enhance the process reference model with respect to safety, we use as a basis ISO/IEC PRF TS 15504-10:2011 Information technology -- Process assessment -- Part 10: Safety extension. The processes defined in this document are consistent with the following domain specific safety standards:

- IEC 61508
- +SAFE, A Safety Extension to CMMI-DEV, V.1.2.
- IEC 60880
- UK MoD Def Stan 00-56
- ISO 26262

ISO/IEC PRF TS 15504-10:2011 defines three processes:

- SAF.1 Safety Management
- SAF.2 Safety Engineering
- SAF.3 Safety Qualification

Comparing the processes with ISO/IEC 12207 and the measurement framework defined in ISO/IEC 15504-2/15504-7, we identify the need to add new processes for each of the processes defined in ISO/IEC PRF TS 15504-10:2011 (Table 7).

Table 7. Mapping of ISO/IEC PRF TS 15504-10:2011 processes

ISO/IEC PRF TS 15504-10:2011 Process	Corresponding ISO/IEC 12207 Process(es)	Corresponding ISO/IEC 15504 Process Attributes	New Process
SAF.1 Safety Management			Safety management process
SAF.2 Safety Engineering			Safety engineering process
SAF.3 Safety Qualification			Safety qualification process

The following processes are added based on ISO/IEC PRF TS 15504-10:2011.

Process ID	2.4.1		
Process Name	Safety Management		
Process Purpose	The purpose of the Safety Management Process is to ensure that products, services and life cycle processes meet safety objectives.		
Process Outcomes	1) Safety principles and safety criteria are established. 2) The scope of the safety activities for the project is defined 3) Safety activities are planned and implemented covering safety engineering, supporting safety verification and validation, and independent assessment activities. 4) Tasks and resources necessary to complete the safety activities are sized and estimated.		

	5) Safety organization structure (responsibilities, roles, reporting channels, interfaces with other projects or OUs, …) is established 6) Safety activities are monitored, safety-related incidents are reported, analysed, and resolved. 7) Agreement on safety policy and requirements for supplied products or services is achieved. 8) Supplier's safety activities are monitored.
Base Practices	**BP.1: Define safety objectives and criteria**: the limits of acceptable risk associated with a hazard are defined externally as imposed safety targets or developed from analysis or development policy. Safety targets and/or acceptable levels of risk are determined. (outcome1) **BP.2: Define Safety Life Cycle**: The Safety Lifecycle is defined, which is appropriate to the context, complexity, safety criteria and targets for the project. (outcome 2) NOTE:Assure Functional safety throughout the product lifecycle. For this reason, the safety management includes and reflects all phases of the product lifecycle. **BP.3: Perform safety planning**: safety engineering and management activities to be implemented in the project in order to meet and verify safety requirements are identified, their dependencies are determined and their performance planned, the resource needs are identified. (outcome 3) **BP.4: Define safety activities integration**: safety activities integration with product development, project lifecycle and support process is determined. (outcome 3, 5) NOTE 3: Examples of integration between development lifecycle and safety activities can be found in IEC 61508 and ISO 26262 NOTE 4:Traceability of safety requirements during the development lifecycle supports safety activities integration. **BP.5: Define skills requirements definition and allocate responsibility**: skills needs for carrying out planned safety activities are identified and responsibilities, authorities, and independence of involved roles are defined and allocated accordingly. (outcome 3, 4, 5) **BP.6: Implement planned safety activities**: the activities defined in the safety planning are implemented. (outcome 3) **BP.7: Monitor the deployment of the safety activities**: Monitor the deployment of the safety activities and act to correct deviations: safety activities of the project are monitored, and safety-related incidents identified in work products, and safety activities are reported, analyzed, managed to closure and further prevented (outcome 6) **BP.8: Define and agree safety policy and safety requirements with suppliers.** Methods and techniques to monitor supplier's safety activities are agreed with the customer. Define an agreement on how the supplier assures safety of the supplied product. (outcome 7) **BP.9: Monitor the safety activities of the supplier**. Supplier's safety activities to meet the safety requirements are monitored and reported. (outcome 8) **BP.10: Implement an escalation mechanism.** Develop and maintain the escalation mechanism that ensures that safety issues may be escalated to appropriate levels of management to resolve them. (outcome 6)

Process ID	2.4.2		
Process Name	Safety Engineering		
Process Purpose	The purpose of the Safety Engineering process is to ensure that safety is adequately addressed throughout all stages of the engineering processes.		
Process Outcomes	1) Hazards related to product are identified and analysed ; 2) Hazard log is established and maintained ; 3) Safety case for the product lifecycle is established and maintained; 4) Safety requirements are defined; 5) Safety integrity requirements are defined and allocated; 6) Safety principles are applied to development processes; 7) Impacts on safety of change requests are analysed; 8) product is validated against safety requirements; 9) Independent evaluations are performed.		
Base Practices	**BP.1: Identify hazard sources and hazards.** Hazard sources and hazards of relevant operational conditions and for foreseeable misuse are identified. (outcome 1) **BP.2: Analyze hazards and risks.** For each hazard, analyze likelihood and severity of impact, and evaluate the risk of the hazard. (outcome 1) **BP.3: Establish and maintain hazard log.** Status of hazards is maintained throughout the whole product lifecycle. (outcome 2)		

	BP.4: Establish and maintain safety case. Safety case is created and maintained during the lifecycle of the product. Process and product documentation is collected for safety case evidence. (outcome 3) **BP.5: Establish and maintain safety requirements**. Establish and maintain throughout the lifecycle safety requirements based on the results of hazard and risk analysis and any other applicable sources. (outcome 4) NOTE 2: Applicable sources can be: legislative requirements, standards, regulations, company policies, customer requirements, customer and end user feedback, verification results, quality assurance findings, validation results, safety validation results, production experiences, commissioning and decommissioning experiences, maintenance and repair experiences, and product field studies. **BP.6: Determine safety integrity requirements.** Safety integrity requirements for each safety requirement based on the risk evaluation of their hazards are determined. (outcome 5) NOTE 3: The appropriateness of a technique for determining safety integrity requirements depends on legal and safety regulatory requirements, accepted good practices, specific hazards, consequences and risks and the availability of data upon which the hazard and risk analysis is to be based. NOTE 4: Safety integrity requirement may be described i.e. as safety integrity level. **BP.7: Allocate safety requirements and safety integrity requirements**. Safety requirements and safety integrity requirements are allocated to architecture, subsystems and components. (outcome 5) **BP.8: Apply safety principles to achieve safety integrity requirements.** Principles and methods relevant for achieving the required safety integrity requirements are applied during the product lifecycle. (outcome 6) NOTE 5: Principles and methods may include for example avoidance of common cause failures by designing diversity, or use of formal methods, defensive programming or perspective based inspections. **BP.9: Perform safety impact analysis on changes.** Analyse the impact of the change requests on hazards and risks. Traceability between a change request and the affected safety work products is established. (outcome 7) **BP.10: Perform safety validations on product.** Safety validations should be based on the outcomes of hazard and risk analyses and performed against safety targets. (outcome 8) **BP.11: Perform independent assessments.** Independent assessments of product and processes are performed in preset points during the product life cycle. (outcome 9) NOTE 6: The evaluations may include verification or validation of any work product. NOTE 7: The required level of independence may vary from an independent person to independent organisation.

Process ID	2.4.2		
Process Name	Safety Qualification		
Process Purpose	The purpose of the Safety Qualification process is to assess the suitability of external resources when developing a safety-related software or system.		
Process Outcomes	As a result of the successful implementation of the Safety Qualification process: 1) safety qualification strategy for external resources is developed 2) safety qualification plan is developed and executed 3) safety qualification documentation is written 4) safety qualification report is produced NOTE1:A safety case is a way to collect and present the information about the safety qualification activities. For more information about safety case and assurance case in general see ISO/IEC 15026.		
Base Practices	**BP.1**: **Develop a safety qualification strategy**: Develop a qualification strategy. The qualification strategy shall consider the quality requirements of the external resources (reflecting the safety requirements determined for the safety-related software or system). The qualification strategy includes criteria for selecting qualification methods. (Outcome 1) **BP.2**: **Plan the safety qualification of external resources** : Plan the qualification acitivities for the external resources . Select the appropriate qualification method for each external resources . (Outcome 2) NOTE 2: The process of external resources selection is not in the scope of the qualification process. NOTE 3: For the safety qualification it may be helpful to define a classification scheme for external resources . Every class may have a set of qualification methods assigned to it. An exemplar classification of tools based on the impact on software: - Core engineering tools are software tools, which have direct impact on the generated source code or binary code and therefore can inject defects into the target software. - Engineering support tools are software tools, which do not have direct impact on the generated source code or binary code, but either they do support the generation of source code or binary code or their mal-function may prevent the detection of defects in the target software. - Management support tools are software tools, which do not have any impact on the generated		

	source code or binary code. Examples for core engineering tools are automatic code generators, compilers and linkers; for engineering support tools are test, build and configuration management tools; and for management support tools are documentation and project management tools. NOTE 4: Qualification methods include • Increased confidence from use • Evaluation of the development process; Demonstration that the development was based on a safety standard • Validation of the tool • Development in compliance with safety standard • Certification **BP.3: Qualify the external resources :** Execute qualification according to the qualification methods chosen. (Outcome 2) **BP.4: Record the safety qualification results.** Record the results of the safety qualification and disseminate the results from the qualification to all interested parties. (Outcome 3) NOTE 5: The qualification documentation incudes: • Unique identification and version number of the external resources • Configuration of external resources • Qualification method used • Result of qualification **BP.5: Maintain and update the safety qualification results.** Maintain and update the safety qualification results and documentation throughout the usage of the external resources . (Outcome 4)

3.2.2 Security Engineering

The process reference model is enhanced with respect to security engineering based on ISO/IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM). This International Standard specifies the Systems Security Engineering – Capability Maturity Model (SSE-CMM). The SSE-CMM is a process reference model focused upon the requirements for implementing security in a system or series of related systems that are the information technology security (ITS) domain. Within the ITS domain, the SSE-CMM is focused on the processes used to achieve ITS, most specifically on the maturity of those processes.

The SSE-CMM divides security engineering into three basic areas: risk, engineering, and assurance, see Figure 6. At the simplest level, the risk process identifies and prioritizes dangers inherent to the developed product or system. The security engineering process works with the other engineering disciplines to determine and implement solutions to the problems presented by the dangers. Finally, the assurance process establishes confidence in the security solutions and conveys this confidence to the customers.

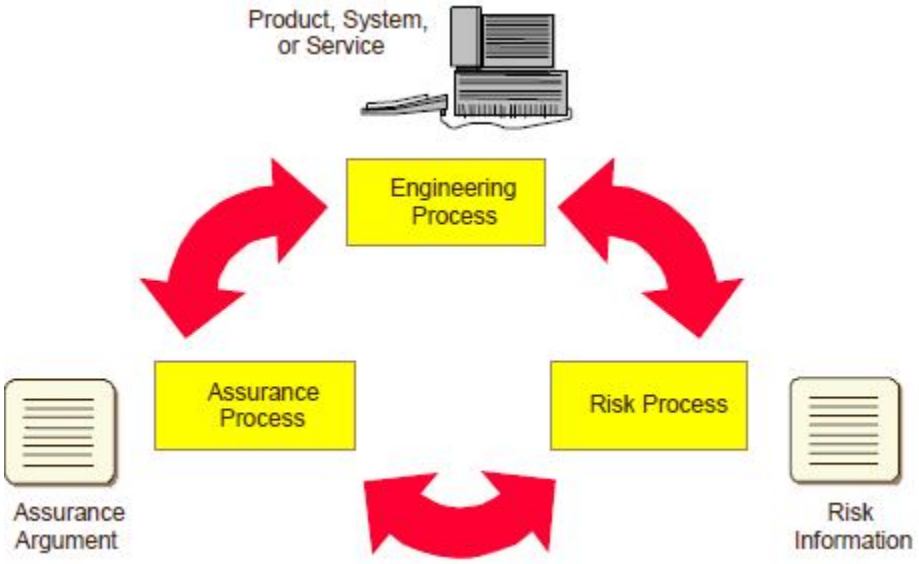

Figure 6. Main areas of the security engineering process

ISO/IEC 21827:2008 defines relevant process areas in two categories as shown in Table 8.

Table 8. Overview on ISO/IEC 21827:2008

Systems security engineering process areas	Project and organizational practices process areas
PA01 Administer Security Controls PA02 Assess Impact	PA12 Ensure Quality PA13 Manage Configuration

PA03 Assess Security Risk	PA14 Manage Project Risk
PA04 Assess Threat	PA15 Monitor and Control Technical Effort
PA05 Assess Vulnerability	PA16 Plan Technical Effort
PA06 Build Assurance Argument	PA17 Define Organization's Systems Engineering Process
PA07 Coordinate Security	PA18 Improve Organization's Systems Engineering Process
PA08 Monitor Security Posture	PA19 Manage Product Line Evolution
PA09 Provide Security Input	PA20 Manage Systems Engineering Support Environment
PA10 Specify Security Needs	PA21 Provide Ongoing Skills and Knowledge
PA11 Verify and Validate Security	PA22 Coordinate with Suppliers

Analysing the correspondence of the security engineering processes with ISO/IEC 12207 as process reference model and the measurement framework as defined in ISO/IEC 15504-2, we defined the mapping of the standard ISO/IEC 21827:2008 as presented in Table 9.

Table 9. Mapping of ISO/IEC 21827:2008 processes

ISO/IEC 21827:2008 Process	**Corresponding ISO/IEC 12207 Process(es)**	**Corresponding ISO/IEC 15504 Process Attributes**	**New Process**
Systems security engineering process areas			
PA01 Administer Security Controls			Administer Security Controls Process
PA02 Assess Impact			Assess Impact Process
PA03 Assess Security Risk			Assess Security Risk Process
PA04 Assess Threat			Assess Threat Process
PA05 Assess Vulnerability			Assess Vulnerability Process
PA06 Build Assurance Argument			Build Assurance Argument Process
PA07 Coordinate Security			Coordinate Security Process
PA08 Monitor Security Posture			Monitor Security Posture Process
PA09 Provide Security Input			Provide Security Input Process
PA10 Specify Security Needs			Specify Security Needs Process
PA11 Verify and Validate Security			Verify and Validate Security Process
Project and organizational practices process areas			
PA12 Ensure Quality	7.2.3 Software Quality Assurance Process		
PA13 Manage Configuration	7.2.2 Software Configuration Management Process		
PA14 Manage Project Risk	6.3.4 Risk Management Process		
PA15 Monitor and Control Technical Effort	6.3.2 Project Assessment and Control Process		
PA16 Plan Technical Effort	6.3.1 Project Planning Process		
PA17 Define Organization's Systems Engineering Process		PA 3.1 Process definition attribute	
PA18 Improve Organization's Systems		PA 3.2 Process deployment attribute	

Engineering Process			
PA19 Manage Product Line Evolution			Manage Product Line Evolution Process
PA20 Manage Systems Engineering Support Environment	6.2.2 Infrastructure Management Process		
PA21 Provide Ongoing Skills and Knowledge	6.2.4 Human Resource Management Process		
PA22 Coordinate with Suppliers.	6.1.1 Acquisition Process		

The additional processes being defined are presented here.

Process ID	2.5.1		
Process Name	**Administer Security Controls**		
Process Purpose	The purpose of Administer Security Controls is to ensure that the intended security for the system that was integrated into the system design is in fact achieved by the resultant system in its operational state.		
Process Outcomes	Security controls are properly configured and used.		
Base Practices	BP. 01 Establish responsibilities and accountability for security controls and communicate them to everyone in the organization. BP. 02 Manage the configuration of system security controls. BP. 03 Manage security awareness, training, and education programs for all users and administrators. BP. 04 Manage periodic maintenance and administration of security services and control mechanisms.		

Process ID	2.5.2		
Process Name	**Assess Impact**		
Process Purpose	The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible, such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.		
Process Outcomes	The security impacts of risks to the system are identified and characterized.		
Base Practices	BP. 01 Identify, analyse, and prioritize operational, business, or mission capabilities leveraged by the system. BP.002 Identify and characterize the system assets that support the key operational capabilities or the security objectives of the system. BP.03 Select the impact metric to be used for this assessment, BP. 04 Identify the relationship between the selected measurements for this assessment and metric conversion factors if required, BP.05 Identify and characterize impacts. BP. 06 Monitor ongoing changes in the impacts.		

Process ID	2.5.3		
Process Name	**Assess Security Risk**		
Process Purpose	The purpose of Assess Security Risk is to identify, analyse and evaluate the security risks involved with relying on a system in a defined environment. This process area focuses on ascertaining these risks based on an established understanding of how capabilities and assets are vulnerable to threats. Specifically, this activity involves identifying and assessing the likelihood of the occurrence of exposures. This set of activities is performed any time during a system's life cycle to support decisions related to developing, maintaining, or operating the system within a known environment.		
Process Outcomes	(1) An understanding of the security risk associated with operating the system within a defined environment is achieved; and (2) risks are prioritized according to a defined methodology.		

Base Practices	BP.01 Select the methods, techniques, and criteria by which security risks for the system in a defined environment are identified, analysed, evaluated, and compared. BP.02 Identify threat/vulnerability/impact triples (exposures), BP.03 Assess the risk associated with the occurrence of an exposure. BP.04 Assess the total uncertainty associated with the risk for the exposure. BP.05 Order risks by priority. BP.06 Monitor ongoing changes in the risk spectrum and changes to their characteristics.

Process ID	2.5.4		
Process Name	**Assess Threat**		
Process Purpose	The purpose of the Assess Threat process area is to identify security threats and their properties and characteristics.		
Process Outcomes	(1) Threats to the security of the system are identified and characterized.		
Base Practices	BP. 01 Identify applicable threats arising from a natural source. BP. 02 Identify applicable threats arising from man-made sources, either accidental or deliberate. BP.03 Identify appropriate units of measure, and applicable ranges, in a specified environment. BP. 04 Assess capability and motivation of threat agent for threats arising from man-made sources. BP. 05 Assess the likelihood of an occurrence of a threat event. BP.06 Monitor ongoing changes in the threat spectrum and changes to their characteristics.		

Process ID	2.5.5		
Process Name	**Assess Vulnerability**		
Process Purpose	The purpose of Assess Vulnerability is to identify and characterize system security vulnerabilities. This process area includes analysing system assets, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability. The terms associated with security risk and vulnerability assessment are used differently in many contexts. For the purposes of this model, “vulnerability” refers to an aspect of a system that can be exploited for purposes other than those originally intended, weaknesses, security holes, or implementation flaws within a system that are likely to be attacked by a threat. These vulnerabilities are independent of any particular threat instance or attack. This set of activities is performed any time during a system's life-cycle to support the decision to develop, maintain, or operate the system within the known environment.		
Process Outcomes	(1) An understanding of system security vulnerabilities within a defined environment is achieved.		
Base Practices	BP.01 Select the methods, techniques, and criteria by which security system vulnerabilities in a defined environment are identified and characterized. BP. 02 Identify system security vulnerabilities. BP. 03 Gather data related to the properties of the vulnerabilities. BP. 04 Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities. BP. 05 Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.		

Process ID	2.5.6		
Process Name	**Build Assurance Argument**		
Process Purpose	The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by assurance evidence that may be derived from multiple sources and levels of abstraction. This process includes identifying and defining assurance related requirements; evidence production and analysis activities; and additional evidence activities needed to support assurance requirements. Additionally, the evidence generated by these activities is gathered, packaged, and prepared for presentation.		
Process Outcomes	(1) The work products and processes clearly provide the evidence that the customer's security needs have been met.		
Base Practices	BP. 01 Identify the security assurance objectives. BP. 02 Define a security assurance strategy to address all assurance objectives. BP. 03 Define measures to monitor security assurance objectives. BP. 04 Identify and control security assurance evidence.		

	BP. 05 Perform analysis of security assurance evidence. BP. 06 Provide a security assurance argument that demonstrates the customer's security needs are met.

Process ID	2.5.7		
Process Name	**Coordinate Security**		
Process Purpose	The purpose of Coordinate Security is to ensure that all parties are aware of and involved with security engineering activities. This activity is critical as security engineering cannot succeed in isolation. This coordination involves maintaining open communications between all project personnel and external groups. Various mechanisms may be used to coordinate and communicate the security engineering decisions and recommendations between these parties, including memoranda, documents, e-mail, meetings, and working groups.		
Process Outcomes	(1) All members of the project team are aware of and involved with security engineering activities to the extent necessary to perform their functions; and (2) Decisions and recommendations related to security are communicated and coordinated.		
Base Practices	BP. 01 Define security engineering coordination objectives and relationships. BP. 02 Identify coordination mechanisms for security engineering. BP. 03 Facilitate security engineering coordination. BP. 04 Use the identified mechanisms to coordinate decisions and recommendations related to security.		

Process ID	2.5.8		
Process Name	**Monitor Security Posture**		
Process Purpose	The purpose of Monitor Security Posture is to ensure that all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security are identified and reported. The external and internal environments are monitored for all factors that may have an impact on the security of the system.		
Process Outcomes	(1) Both internal and external security related events are detected and tracked; (2) Incidents are responded to in accordance with policy; and (3) Changes to the operational security posture are identified and handled in accordance with the security objectives.		
Base Practices	BP. 01 Analyse event records to determine the cause of an event, how it proceeded, and likely future events. BP. 02 Monitor changes in threats, vulnerabilities, impacts, risks, and the environment. BP. 03 Identify security relevant incidents. BP. 04 Monitor the performance and functional effectiveness of security safeguards. BP. 05 Review the security posture of the system to identify necessary changes. BP. 06 Manage the response to security relevant incidents. BP. 07 Ensure that the artifacts related to security monitoring are suitably protected.		

Process ID	2.5.9		
Process Name	**Provide Security Input**		
Process Purpose	The purpose of Provide Security Input is to provide system architects, designers, implementers, or users with the security information they need. This information includes security architecture, design, or implementation alternatives and security guidance. The input is developed, analysed, provided to and coordinated with the appropriate organization members based on the security needs identified in the Administer Security Controls Process.		
Process Outcomes	(1) All system issues are reviewed for security implications and are resolved in accordance with security goals; (2) All members of the project team have an understanding of security so they can perform their functions; (3) The solution reflects the security input provided.		
Base Practices	BP. 01 Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs. BP. 02 Determine the security constraints and considerations needed to make informed engineering choices. BP. 03 Identify alternative solutions to security related engineering problems. BP. 04 Analyse and prioritize engineering alternatives using security constraints and considerations. BP.05 Provide security related guidance to the other engineering groups. BP. 06 Provide security related guidance to operational system users and administrators.		

Process ID	2.5.10		
Process Name	**Specify Security Needs**		
Process Purpose	The purpose of Specify Security Needs is to explicitly identify the needs related to security for the system. Specify Security Needs involves defining the basis for security in the system in order to meet all legal, policy, and organizational requirements for security. These needs are tailored based upon the target operational security context of the system, the current security and systems environment of the organization, and a set of security objectives are identified. A set of security-related requirements is defined for the system that becomes the baseline for security within the system upon approval.		
Process Outcomes	(1) A common understanding of security needs is reached between all parties, including the customer.		
Base Practices	BP.01 Gain an understanding of the customer's security needs. BP. 02 Identify the laws, policies, standards, external influences and constraints that govern the system. BP.03 Identify the purpose of the system in order to determine the security context. BP. 04 Capture a high-level security oriented view of the system operation. BP. 05 Capture high-level goals that define the security of the system. BP. 06 Define a consistent set of statements which define the protection to be implemented in the system. BP. 07 Obtain agreement that the specified security requirements match the customer's needs.		

Process ID	2.5.11		
Process Name	**Verify and Validate Security**		
Process Purpose	The purpose of Verify and Validate Security is to ensure that solutions are verified and validated with respect to security. Solutions are verified against the security requirements, architecture, and design using observation, demonstration, analysis, and testing. Solutions are validated against the customer's operational security needs.		
Process Outcomes	(1) Solutions meet security requirements. (2) Solutions meet the customer's operational security needs.		
Base Practices	BP.01 Identify the solution to be verified and validated. BP.02 Define the approach and level of rigour for verifying and validating each solution. BP. 03 Verify that the solution implements the requirements associated with the higher level of abstraction. BP. 04 Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs. BP.11.05 Capture the verification and validation results for the other engineering groups.		

Process ID	2.5.12		
Process Name	**Manage Product Line Evolution**		
Process Purpose	The purpose of the Manage Product Line Evolution process is to introduce services, equipment, and new technology to achieve the optimal benefits in product evolution, cost, schedule, and performance over time as the product line evolves toward its ultimate objectives.		
Process Outcomes	(1) Product lines are evolved towards their ultimate objectives.		
Base Practices	BP.01 Define the types of products to be offered. BP.02 Identify new product technologies or enabling infrastructure that will help the organization acquire, develop, and apply technology for competitive advantage. BP.03 Make the necessary changes in the product development cycle to support the development of new products. BP.04 Ensure critical components are available to support planned product evolution. BP.05 Insert new technology into product development, marketing, and manufacturing.		

3.2.3 Usability Engineering

In order to attend the usability quality characteristics, specifically important in the context of software development in a digital convergence/divergence scenario, we add 4 processes from ISO/TR 18529:2000 Ergonomics -- Ergonomics of human-system interaction -- Human-centred lifecycle process descriptions, an technical report developed by an international ISO working group (Figure 7).

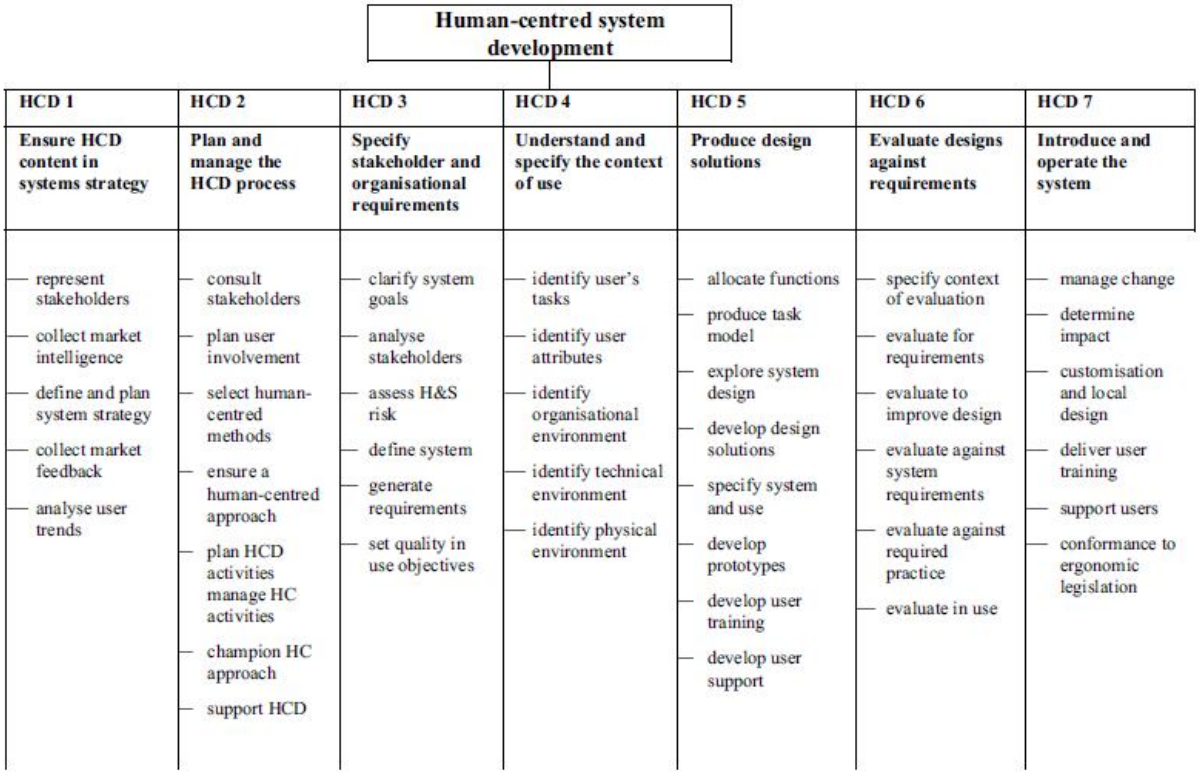

Figure 7. Overview on processes defined by ISO/TR 18529:2000

Table 10. Mapping of ISO/TR 18529:2000 processes

ISO/TR 18529:2000 Process	Corresponding ISO/IEC 12207 Process(es)	Corresponding ISO/IEC 15504 Process Attributes	New Process
HDC.1 Ensure HCD content in system strategy			HCD strategy process
HDC.2 Plan and manage the HDC process		PA 2.1 Performance management attribute	
HDC.3 Specify stakeholders and organizational requirements	6.4.1 Stakeholder Requirements Definition Process		
HDC.4 Understand and			Context of use specification

specify the context of use			process
HDC.5 Produce design solutions			HCD solution production process
HDC.6 evaluate designs against requirements			HCD evaluation process
HDC.7 Introduce and operate the system	6.4.9 Software Operation Process		

In order to attend the quality needs, we add the following processes.

Process ID	2.6.1		
Process Name	**HCD Strategy**		
Process Purpose	The purpose of the *HCD strategy process* is to establish and maintain a focus on stakeholder and user issues in each part of the organisation which deals with system markets, concept, development and support.		
Process Outcomes	As a result of successful implementation of the process, the following will be defined: - marketing will take account of usability, ergonomics and socio-technical issues - systems will be targeted to meet users' needs and expectations - planners will consider stakeholder and organisation requirements in setting out systems strategy - the system will be more responsive to changes in its users (their needs, tasks, context etc.) - the enterprise will be more responsive to changes in its users - the system is less likely to be rejected by the market.		
Base Practices	- Collect market intelligence - Define and plan a system strategy - Collect market feedback - Analyse trends in users		

Process ID	2.6.2		
Process Name	**Context of Use Specification**		
Process Purpose	The purpose of the Context of use specification process is to identify, clarify and record the characteristics of the stakeholders, their tasks and the organisational and physical environment in which the system will operate.		
Process Outcomes	As a result of successful implementation of this process the following will be defined: - the characteristics of the intended users - the tasks the users are to perform - the organisation and environment in which the system is used.		
Base Practices	- Identify and document user's tasks - Identify and document significant user attributes - Identify and document organisational environment - Identify and document technical environment - Identify and document physical environment		

Process ID	2.6.3		
Process Name	**HCD Solution Production**		
Process Purpose	The purpose of the HCD solution production process is to create potential design solutions by drawing on established state-of-the-art practice, the experience and knowledge of the participants and the results of the context of use analysis.		
Process Outcomes	As a result of successful implementation of this process the following will be defined: - the whole socio-technical system in which any technical components operate will be considered in the design - user characteristics and needs will be taken into account in the purchasing of system components - user characteristics and needs will be taken into account in the design of the system - existing knowledge of best practice from socio-technical systems engineering, ergonomics, psychology,		

	cognitive science and other relevant disciplines will be integrated into the system - communication between stakeholders in the system will be improved because the design decisions will be more explicit - the development team will be able to explore several design concepts before they settle on one - stakeholder and end-user feedback will be incorporated in the design early in the development process - it will be possible to evaluate several iterations of a design and alternative designs - the interface between the user and the software, hardware and organisational components of the system will be designed - user training and support will be developed.
Base Practices	**-** Allocate functions - Produce composite task model - Explore system design - Use existing knowledge to develop design solutions - Specify system - Develop prototypes - Develop user training - Develop user support

Process ID	2.6.4		
Process Name	**HCD Evaluation**		
Process Purpose	The purpose of the HCD evaluation process is to collect feedback on the developing design. This feedback will be collected from end users and other representative sources.		
Process Outcomes	- feedback will be provided to improve the design - there will be an assessment of whether stakeholder and organisational objectives have been achieved or not - long-term use of the system will be monitored. In the case of evaluation to identify improvements to the system (formative evaluation), successful implementation of the process will reflect: - potential problems and scope for improvements in: the technology, supporting material, organisational or physical environment and the training - which design option best fits the functional and user requirements - feedback and further requirements from the users. In the case of evaluation to assess whether objectives have been met (summative evaluation), successful implementation of the process will demonstrate: - how well the system meets its organisational goals - that a particular design meets the human-centred requirements - conformity to international, national and/or statutory requirements.		
Base Practices	**-** Specify and validate context of evaluation - Evaluate early prototypes in order to define the requirements for the system - Evaluate prototypes in order to improve the design - Evaluate the system in order to check that the system requirements have been met - Evaluate the system in order to check that the required practice has been followed - Evaluate the system in use in order to ensure that it continues to meet organisational and user needs.		

3.2.4 Software Product Line Management

A software product line is a set of software-intensive systems that share a common, managed set of features satisfying the specific needs of a particular market segment or mission and that are developed from a common set of core assets in a prescribed way (Northrop & Clements . , 2007).

Product flexibility is the anthem of the software marketplace, and product lines fulfill the promise of tailor-made systems built specifically for the needs of particular customers or customer groups. A product line succeeds because the commonalities shared by the software products can be exploited to achieve economies of production. The products are built from common assets in a prescribed way.

At its essence, fielding a product line involves core asset development and product development using the core assets, both under the aegis of technical and organizational management. Core asset development and product development from the core assets can occur in either order: new products are built from core assets, or core assets are extracted from existing products. Often, products and core assets are built in concert with each other (Figure 8).

Figure 8. Essential Activities for Software Product Lines

Core Asset Development. The goal of the core asset development activity is to establish a

production capability for products. Figure 9. illustrates the core asset development activity along with its outputs and influential contextual factors.

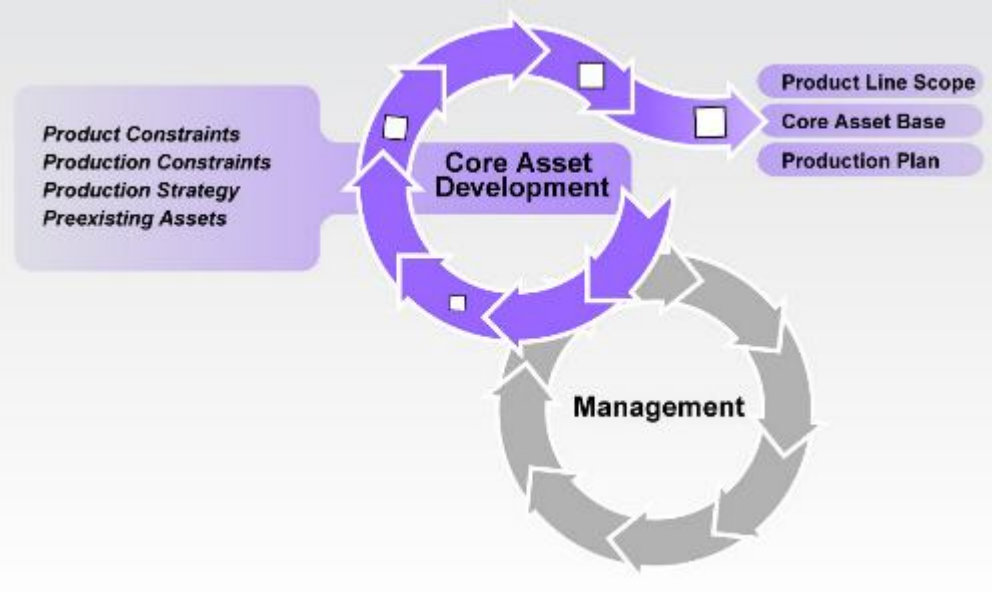

Figure 9. Core Asset Development

Product Development. The product development activity depends on the three outputs described above–the product line scope, the core assets, and the production plan–plus the product description for each individual product. Figure 10. illustrates these relationships.

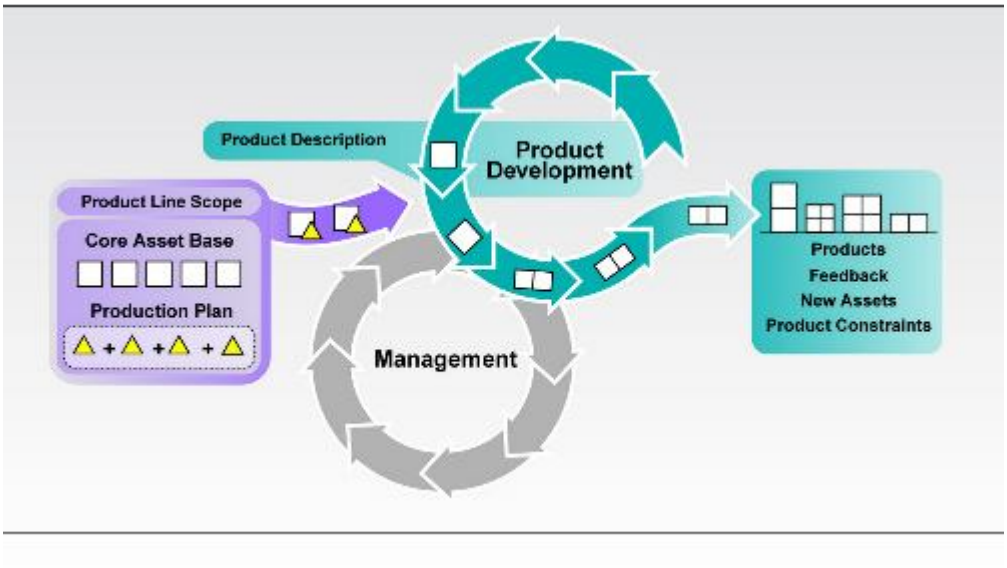

Figure 10. Product Development

Management. Management plays a critical role in the successful fielding of a product line.

Activities must be given resources and then be coordinated and supervised. Management at both the technical (or project) and organizational levels must be strongly committed to the software product line effort. That commitment manifests itself in a number of ways that feed the product line effort and keep it healthy and vital.

Product Line Practice Areas. To achieve a software product line, you must carry out the three essential activities described in Product Line Essential Activities: core asset development, product development, and management.

Since there are so many practice areas, we need a way of organizing them for easier access and reference. For this reason, we divide them loosely into three categories as illustrated in Table 11.

Table 11. Practice area categories

	Software Engineering Practice Areas	**Technical Management Practice Areas**	**Organizational Management Practice Areas**
Description	Software engineering practice areas are those necessary for applying the appropriate technology to create and evolve both core assets and products.	Technical management practices are those management practices that are necessary for the development and evolution of both core assets and products.	Organizational management practices are those practices that are necessary for the orchestration of the entire product line effort.
Practice areas	• Architecture Definition • Architecture Evaluation • Component Development • Mining Existing Assets • Requirements Engineering • Software System Integration • Testing • Understanding Relevant Domains • Using Externally Available Software	• Configuration Management • Make/Buy/Mine/Commission Analysis • Measurement and Tracking • Process Discipline • Scoping • Technical Planning • Technical Risk Management • Tool Support	• Building a Business Case • Customer Interface Management • Developing an Acquisition Strategy • Funding • Launching and Institutionalizing • Market Analysis • Operations • Organizational Planning • Organizational Risk Management • Structuring the Organization • Technology Forecasting • Training

Mapping ISO/IEC 12207 processes to the software product line practice process areas (based on (Jones & Soule, 2002) (Stallinger et al, 2011.) (Hoyer & Chroust, 2006).

Table 12. Mapping of SPL practice process areas

Software Product Line Practice Process Area	**Corresponding ISO/IEC 12207 Process(es)**	**Corresponding ISO/IEC 15504 Process Attributes**	**New Process**
Software Engineering Practice Areas			
Architecture Definition	7.1.3 Software Architectural Design Process		
Architecture Evaluation	7.1.3 Software Architectural Design Process		
Component Development	7.1.5 Software Construction		

	Process		
Mining Existing Assets	7.3.2 Reuse Asset Management Process		
Requirements Engineering	7.1.2 Software Requirements Analysis Process		
Software System Integration	7.1.6 Software Integration Process		
Testing	7.2 Software Qualification Testing Process		
Understanding Relevant Domain	7.3.1 Domain Engineering Process		
Using Externally Available Software	6.1.1 Acquisition Process 7.1.6 Software Integration Process		
Technical Management Practice Areas			
Configuration Management	7.2.2 Software Configuration Management Process		
Make/Buy/Mine/Commission Analysis	6.3.3 Decision Management Process		
Measurement and Tracking	6.3.7 Measurement Process 6.3.2 Project Assessment and Control Process		
Process Discipline		PA 3.1 Process definition attribute PA 3.2 Process deployment attribute	
Scoping			Scoping
Technical Planning	6.3.1 Project Planning Process		
Technical Risk Management	6.3.4 Risk Management Process		
Tool Support	6.2.2 Infrastructure Management Process		
Organizational Management Practice Areas			
Building a Business Case	6.2.3 Project Portfolio Management Process		
Customer Interface Management	6.4.1 Stakeholder Requirements Definition Process 6.1.2 Supply Process		
Developing an Acquisition Strategy	6.1.1 Acquisition Process		
Funding			Funding
Launching and Institutionalizing		PA 3.2 Process deployment attribute	
Market Analysis			Market Analysis
Operations	6.4.9 Software Operation Process		
Organizational Planning			Organizational Planning
Organizational Risk Management			Organizational Risk Management
Structuring the Organization			Structuring the Organization
Technology Forecasting			Technology Forecasting

Training	6.2.4 Human Resource Management Process		

The following processes are added in order to completely cover the SPL practice process areas.

Process ID	2.7.1		
Process Name	**Scoping**		
Process Purpose	The purpose of Scoping is to bound a system or set of systems by defining those behaviors or aspects that are "in" and those behaviors or aspects that are "out."		
Process Outcomes	Software Product Line Scope		
Base Practices	Applying the *What to Build* pattern Examining existing products Conducting a workshop to understand product line goals and products Context diagramming Developing an attribute/product matrix Developing product line scenarios		

Process ID	2.7.2		
Process Name	**Funding**		
Process Purpose	The purpose of Funding is to define how the software development effort have to be financed.		
Process Outcomes	Funding plan		
Base Practices	Identify funding strategies for each of the product line activities		

Process ID	2.7.3		
Process Name	**Market Analysis**		
Process Purpose	Market analysis is the systematic research and analysis of the external factors that determine the success of a product in the marketplace. It involves the gathering of business intelligence, competitive studies and assessments, market segmentation, customer plans and strategies, and the integration of this information into a cohesive business strategy and plan.		
Process Outcomes	Market analysis		
Base Practices	Identify information sources Gather information Identify customer segments Map products to segments Examine the competition		

Process ID	2.7.4		
Process Name	**Organizational Planning**		
Process Purpose	The purpose of Organizational planning is to realize strategic or organizational-level planning.		
Process Outcomes	Organizational management plans including product line adoption plans and core asset funding plans.		
Base Practices	Establish the organizational management plan and its contents Establish estimates of the resources required to carry out the organizational management plan Review organizational management plan for feasibility Establish commitments to the organizational management plan		

Process ID	2.7.5		
Process Name	**Organizational Risk Management**		
Process Purpose	The purpose of Organizational Risk Management is to manage risk at the strategic level by managing risks that transcend, or are shared across, projects.		
Process Outcomes	Organizational risks		
Base Practices	Identify organizational risks Analyze organizational risk Plan responses to organizational risks Monitor & control organizational risks		

Process ID	2.7.6		
Process Name	**Structuring the Organization**		
Process Purpose	The purpose of Structuring the Organization is to define and place placing thoe roles specific to SPLs into the appropriate organizational units to most effectively support the product line approach.		
Process Outcomes	Organizational Structure		
Base Practices	Identify organizational chart and boundaries Identify functional groupings Establish interorganizational relationships		

Process ID	2.7.7		
Process Name	**Technology Forecasting**		
Process Purpose	The purpose of technology forecasting is to identify and assess technologies continuously. They are assessed both for their immediate benefit and their potential future applicability		
Process Outcomes	A technology forecasting that covers both technologies that enable specific product features and technologies that support the engineering tasks in the development of those features.		
Base Practices	Keep current with technology trends. Validate the forecast.		

Acknowledgements

This work has been supported by the CNPq (*Conselho Nacional de Desenvolvimento Científico e Tecnológico* – www.cnpq.br), an entity of the Brazilian government focused on scientific and technological development.

References

Akao, Y. Quality Function Deployment. Productivity Press, 2004.

Anderson, J. G. "Clearing the way for physicians' use of clinical information systems," Communications of the ACM, vol. 40, pp. 83 - 90, 1997; L. Lapointe and S. Rivard, "A Multilevel Model of Resistance to Information Technology Implementation," MIS Quarterly, vol. 29, pp. 461- 491, 2005.

Bashshur, R.L. Telemedicine and the Health Care System in Telemedicine - Theory and Practice, R.L. Bashshur, J.H. Sanders, and G.W. Shannon (eds.), Charles C. Thomas, Springfield, IL, 1997.

Bashshur, R., L. Telemedicine Nomenclature: What Does it Mean? Telemedicine Journal, vol. 6, pp. 1-3, 2000.

Bangert, D. Doktor, R. "The role of organizational culture in the management of clinical e-health systems," presented at 36th Annual Hawaii International Conference System Sciences, Island of Hawaii, U.S.A., 2003; Institute of Medicine, Telemedicine: A Guide to Assessing Telecommunications in Health Care. Washington D.C.: National Academy Press, 1996.

CYCLOPS, The Cyclops Group. http:// www.cyclops.ufsc.br

CMMI Product Team. CMMI for Development (CMMI-DEV), Version 1.2. Technical Report CMU/SEI-2006-TR-008, Carnegie Mellon University/ Software Engineering Institute, Pittsburgh, August 2006.

Coiera, E. Guide to Medical Informatics, The Internet and Telemedicine, First ed. London,UK: Chapman & Hall, 1997.

EHTEL - European Health Telematics Association. Sustainable Telemedicine: Paradigms for future-proof healthcare - A Briefing Paper. Version 1.0, 20 February 2008.

Glueckauf, R. L., Whitton, J. D. and Nickelson, D. W. Telehealth: The New Frontier in Rehabilitation and Health Care, in Assistive Technology: Matching Device and Consumer for Successful Rehabilitation, M. J. Scherer, Ed., 1st ed. Washington D.C.: Amarican Psychological Association, 2002.

C.Hoyer, G. Chroust. Evolving Standard Process Reference Models for Product Line Development. Proc. of Conference on Software Engineering and Advanced Applications, Dubrovnik, Croatia, 2006

Institute of Medicine, Telemedicine: A Guide to Assessing Telecommunications in Health Care, National Academy Press, Washington, DC, 1996.

ISO/IEC 12207: 2008, Information technology - Software life cycle processes. Int'l Organization for Standardization, 2008.

ISOIEC 15504: 2005, Information technology - Software process assessment. Int'l Organization for Standardization, 2003-2005.

ISO/IEC 9126-1:2001, Software Engineering—Product Quality—Part 1: Quality Model, Int'l Organization for Standardization, 2001

ISO/IEC 25030:2007, Software Engineering—Software Product Quality Requirements and Evaluation (SQuaRE)—Quality Requirements, Int'l Organization for Standardization, 2007.

ISO/TR 16056-1:2004 Health informatics – Interoperability of telehealth systems and networks, 2004.

ITIL v3, 2007. http:// www.itil-officialsite.com. Access on febuary, 2008.

L.G. Jones & A. L. Soule . Software Process Improvement and Product Line Practice: CMMI and the Framework for Software Product Line Practice, Technical Note CMU/SEI-2002-TN-012, July 2002

LeRouge, Cynthia, et al. Telemedicine Encounter Quality: Comparing Patient and Provider Perspectives of a Socio-Technical System. Proceedings of the 37th Hawaii International Conference on System Sciences, 2004

Loane, M., Wootton, R. A review of guidelines and standards for telemedicine. Journal of Telemedicine and Telecare, vol. 8, no. 2, 2002.

Maia, R. S., Wangenheim, A. von, Nobre, L. F. A Statewide Telemedicine Network for Public Health in Brazil. In Proc. of 19th IEEE Symposium on Computer Based Medical Systems - CBMS2006, Salt Lake City, 2006.

Maheu, M. M., Whitten, P. and A. Allen, E-Health, Telehealth, and Telemedicine: A Guide to Start-Up and Success, First ed. San Francisco: Jossey-Bass Inc., 2001.

McCaffery, F., Richardson, I.. MedeSPI :A Software Process Improvement Model for the medical device industry based upon ISO/IEC 15504, International SPICE Days 2007, Germany, 2007.

L.M. Northrop, P. C. Clements . A Framework for Software Product Line Practice, Version 5.0. SEI, July 2007 http://www.sei.cmu.edu/productlines/frame_report

Office of Rural Health Policy - U.S. Department of Health and Human Services, Exploratory Evaluation of Rural Applications of Telemedicine. Rockville, MD: ORHP, 1997.

Paul, D. L. Assessing Technological Barriers to Telemedicine: Technology-Management Implications. IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, VOL. 46, NO. 3, AUGUST 1999.

Perednia D. A., Allen, A. Telemedicine technology and clinical applications. J. Amer. Med. Assoc., vol. 273, no. 6, pp. 483–488, 1995

Roine, R., Ohinmaa, A., Hailey, D. Assessing telemedicine: a systematic review of the literature, CMAJ, SEPT. 18, 2001; 165

F. Stallinger, R. Neumann, R.Schossleitner, R. Zeilinger. Linking Software Life Cycle Activities with Product Strategy and Economics: Extending ISO/IEC 12207 with Product Management Best Practices. Proc. of the International Conference SPICE , Limerick/Irleland, 2011

The National First Nations Telehealth Research Project Final Report, http://www.hcsc.gc.ca/fnihb/phcph/telehealth/publications/final_report.htm, access on February, 2008.

Tulu, B. Chatterjee, S. Laxminarayan, S. A Taxonomy of Telemedicine Efforts with respect to Applications, Infrastructure, Delivery Tools, Type of Setting and Purpose. Proceedings of the 38th Hawaii International Conference on System Sciences, Island of Hawaii, 2005.

U.S. Congress, Office of Technology Assessment, "Bringing Health Care Online: The Role of Information Technologies," Office of Technology Assessment. U.S. Congress, Ed.: U.S. Government Printing Office, 1995.

U.S. General Accounting Office, Telemedicine: Federal Strategy is Needed to Guide Investments. Washington, DC: U.S. Senate, 1997.

C. Gresse von Wangenheim and A. von Wangenheim. Defining a Software Quality Model for Asynchronous Store-and-Forward Telemedicine Systems. Technical Report INCoD/UFSC, in progress.

A. I. Wasserman. Software Engineering Issues for Mobile Application Development. Proc. of Workshop on Mobile Software Engineering/MobiCASE, Santa Clara/USA, 2010

ANNEX A. Software Quality Model for ASFTSs

In (Wangenheim & Wangenheim, 2011), we define a Software Quality Model for ASFTSs. Within this model the abstract product quality is decomposed in 3 categories: quality in use (Table 13), system quality (Table 14) and data quality (Table 15). The decomposition and definition of the quality (sub-)characteristics are based on ISO/IEC 25000 and the degree of importance is based on the median of the importance ratings given by an expert panel.

Table 13. Quality in use

Characteristic	Sub-characteristic	Description	*Degree of Importance*
Satisfaction: degree to which user needs are satisfied when a product or system is used in a specified context of use.	Usefulness	degree to which a user is satisfied with their perceived achievement of pragmatic goals, including the results of use and the consequences of use.	*important*
	Trust	degree to which a user or other stakeholder has confidence that a system will behave as intended.	*essential*
	Pleasure	degree to which a user obtains pleasure from fulfilling their personal needs.	*important*
	Comfort	degree to which the user is satisfied with physical comfort.	*important*
Context coverage: degree to which a product or system can be used with effectiveness, efficiency, freedom from risk and satisfaction in both specified contexts of use and in contexts beyond those initially explicitly identified.	Context completeness	degree to which a system can be used with effectiveness, efficiency, freedom from risk and satisfaction in all the specified contexts of use.	*important*
	Flexibility	degree to which a system can be used with effectiveness, efficiency, freedom from risk and satisfaction in contexts beyond those initially specified in the requirements.	*important*
Freedom from risk: degree to which a product or system mitigates the potential risk to economic status, human life, health, or the environment	Health and safety risk mitigation	degree to which a product or system mitigates the potential risk to people in the intended contexts of use.	*essential*

Compared to ISO/IEC 25000, we do not explicitly include the characteristics effectiveness and efficiency as they are also covered by system quality characteristics.

System quality is defined as presented in Table 14. In accordance to ISO/IEC 25000, system quality is decomposed in eight quality characteristics.

Table 14. System quality

Characteristic	Sub-characteristic	Description	Degree of importance
Functional suitability:	Functional	degree to which the set of functions of the system	*Important/essential*

degree to which a product or system provides functions that meet stated and implied needs when used under specified conditions.	completeness	covers all the specified tasks and user objectives: request examination, realizing examination, interpreting examination/report findings, distributing.	
	Functional correctness	degree to which a system provides the correct results with the needed degree of precision.	*Essential*
	Functional appropriateness	degree to which the functions facilitate the accomplishment of specified tasks and objectives: request examination, realizing examination, interpreting examination/report findings, distributing.	*Important*
Performance efficiency: performance relative to the amount of resources used under stated conditions.	Time behaviour	degree to which the response and processing times and throughput rates of a system, when performing its functions, meet requirements.	*Important*
	Resource utilization	degree to which the amounts and types of resources used by a system when performing its functions meet requirements.	*Important*
	Capacity	degree to which the maximum limits of a system parameter meet requirements.	*Important*
Compatibility: degree to which a product, system or component can exchange information with other products, systems or components, and/or perform its required functions, while sharing the same hardware or software environment (Adapted from ISO/IEC/IEEE 24765).	Co-existence	degree to which a system can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product.	*Important*
	Interoperability	degree to which two or more systems can exchange information and use the information that has been exchanged.	*Important*
Usability: degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use (Adapted from ISO 9241-210).	Appropriateness recognizability	degree to which users can recognize whether a system is appropriate for their needs.	*Important*
	Learnability	degree to which a system can be used by specified users to achieve specified goals of learning to use the product or system.	*Important*
	Operability	degree to which a system has attributes that make it easy to operate and control.	*Important*
	User error protection	degree to which a system protects users against making errors.	*Important/Essential*
	User interface aesthetics	degree to which a user interface enables pleasing and satisfying interaction for the user.	*Important*
Reliability: degree to which a system, product or component performs specified functions under specified conditions for a specified period of time (Adapted from ISO/IEC/IEEE 24765)	Maturity	degree to which a system meets needs for reliability under normal operation.	*Essential*
	Availability	degree to which a system is operational and accessible when required for use (ISO/IEC/IEEE 24765).	*Essential*
	Fault tolerance	degree to which a system operates as intended despite the presence of hardware or software faults (Adapted from ISO/IEC/IEEE 24765).	*Essential*
	Recoverability	degree to which, in the event of an interruption or a failure, a system can recover the data directly affected and re-establish the desired state of the system.	*Essential*

Security: degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization.	Confidentiality	degree to which a system ensures that data are accessible only to those authorized to have access.	*Essential*
	Integrity	degree to which a system prevents unauthorized access to, or modification of, computer programs or data (ISO/IEC/IEEE 24765).	*Essential*
	Non-repudiation	degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later (Adapted from ISO 7498-2:1989).	*Essential*
	Accountability	degree to which the actions of an entity can be traced uniquely to the entity (Adapted from ISO 7498-2:1989).	*Essential*
	Authenticity	degree to which the identity of a subject or resource can be proved to be the one claimed (Adapted from ISO/IEC 13335-1:2004).	*Essential*
Maintainability: degree of effectiveness and efficiency with which a product or system can be modified by the intended Maintainers.	Modularity	degree to which a system is composed of discrete components such that a change to one component has minimal impact on other components (ISO/IEC/IEEE 24765).	*Important*
	Reusability	degree to which an asset can be used in more than one system, or in building other assets (Adapted from IEEE 1517-2004).	*Desirable*
	Analysability	degree of effectiveness and efficiency with which it is possible to assess the impact on a system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.	*Important*
	Modifiability	degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality.	*Important*
	Testability	degree of effectiveness and efficiency with which test criteria can be established for a system and tests can be performed to determine whether those criteria have been met (Adapted from ISO/IEC/IEEE 24765).	*Important*
Portability: degree of effectiveness and efficiency with which a system, product or component can be transferred from one hardware, software or other operational or usage environment to another.	Adaptability	degree to which a system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments.	*Important*
	Installability	degree of effectiveness and efficiency with which a system can be successfully installed and/or uninstalled in a specified environment.	*Important*
	Replaceability	degree to which a system can be replaced by another specified software product for the same purpose in the same environment.	*Desirable*

Based on ISO/IEC 25000, data quality is defined trough a set of 9 quality characteristics, having been identified as relevant in the expert interviews (Table 15).

Table 15. Data quality

Characteristic	**Description**	***Degree of importance***
Completeness	extent to which data are sufficiently able to satisfy user's stated needs from quantitative point of view.	*Essential*
Precision	capability of the value assigned to an attribute to provide the degree of	*Essential*

	information needed in a stated context of use.	
Accuracy	degree to which a data value conforms to its actual or specified value.	*Essential*
Consistency	degree to which apparent contradictions within data are absent.	*Important*
Currency	extent to which data is up-to-date	*Important*
Understandability	extent to which the real meaning of data is easy for users to comprehend (data is in appropriate languages, symbols and units, and the degree to which its definitions are clear).	*Essential*
Managability	capability of data to be stored appropriately from a functional point of view.	*Important*
Credibility	extent to which data are regarded as true and credible by users.	*Essential*
Regulatory compliance	capability of data to adhere to standards, conventions or regulations in force and similar rules relating to data quality.	*Important*

ANNEX B. Software Quality Model in the context of Digital Convergence/Divergence

Based on a literature review, we identified in alignment with (Wasserman, 2010), important quality characteristics for the development of software in the context of digital convergence/divergence, where typically applications have to run on diverse devices.

Differences of software development for different kind of devices

In many respects, developing applications for different kind of devices (cell phones, tablets, Interactive Digital TV, etc.) is similar to software engineering for computer applications. Common issues include integration with device hardware, as well as traditional issues of security, performance, reliability, and storage limitations. However, in the context of developing applications in a digital convergence/divergence scenario, we can identify some differences and emphases, including:

1) Potential interaction with other applications, e.g., mobile devices may have numerous applications from varied sources, with the possibility of interactions among them;

2) Sensor handling. Most modern mobile devices, e.g., “smartphones”, include an accelerometer that responds to device movement, a global positioning system, a microphone usable by applications other than voice calls, cameras, etc. that may be used by the applications.

3) Diverse types of applications, including native applications, web applications or widgets. In case of native applications they use only software installed directly on the device, whereas, mobile web applications invoke services over the telephone network or the Internet via a web browser and affect data and displays on the device;

4) Fragmentation of device market in terms of hardware and software platforms. Mobile devices may have to support applications that were written for all of the varied devices supporting the operating system, and also for different versions of the operating system.

5) Security. Mobile platforms are typically open, allowing the installation of new “malware” applications that can affect the overall operation of the device, including the surreptitious transmission of local data by such an application.

6) User interfaces. Due to the great variety of input and output visualization of the diverse devices, the question of usability and user interface design becomes much more important as often convergent applications must adapt to the different kinds of input and output forms and share common elements of the user interface with other applications.

7) Complexity of testing. Mobile applications or IDTV applications are particularly challenging to test, especially when trying to test them in a real application situation (e.g., “on the go”).

Important Software Quality Characteristics

Analyzing the difference and starting from ISO/IEC 25010 (System Quality), we identify relevant quality characteristics in the context of digital convergence/divergence (Table 16).

Table 16. System quality

Characteristic	Sub-characteristic	Description	Degree of importance
Functional suitability: degree to which a product or system provides functions that meet stated and implied needs when used under specified conditions.	Functional completeness	degree to which the set of functions of the system covers all the specified tasks and user objectives: request examination, realizing examination, interpreting examination/report findings, distributing.	*Important*
	Functional correctness	degree to which a system provides the correct results with the needed degree of precision.	*Important*
	Functional appropriateness	degree to which the functions facilitate the accomplishment of specified tasks and objectives: request examination, realizing examination, interpreting examination/report findings, distributing.	*Important*
Performance efficiency: performance relative to the amount of resources used under stated conditions.	Time behaviour	degree to which the response and processing times and throughput rates of a system, when performing its functions, meet requirements.	*Important*
	Resource utilization	degree to which the amounts and types of resources used by a system when performing its functions meet requirements.	*Important*
	Capacity	degree to which the maximum limits of a system parameter meet requirements.	*Important*
Compatibility: degree to which a product, system or component can exchange information with other products, systems or components, and/or perform its required functions, while sharing the same hardware or software environment (Adapted from ISO/IEC/IEEE 24765).	Co-existence	degree to which a system can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product.	*Important*
	Interoperability	degree to which two or more systems can exchange information and use the information that has been exchanged.	*Important*
Usability: degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use (Adapted from ISO 9241-210).	Appropriateness recognizability	degree to which users can recognize whether a system is appropriate for their needs.	*Important*
	Learnability	degree to which a system can be used by specified users to achieve specified goals of learning to use the product or system.	*Important*
	Operability	degree to which a system has attributes that make it easy to operate and control.	*Essential*
	User error protection	degree to which a system protects users against making errors.	*Important*

	User interface aesthetics	degree to which a user interface enables pleasing and satisfying interaction for the user.	*Essential*
Reliability: degree to which a system, product or component performs specified functions under specified conditions for a specified period of time (Adapted from ISO/IEC/IEEE 24765)	Maturity	degree to which a system meets needs for reliability under normal operation.	*Important*
	Availability	degree to which a system is operational and accessible when required for use (ISO/IEC/IEEE 24765).	*Important*
	Fault tolerance	degree to which a system operates as intended despite the presence of hardware or software faults (Adapted from ISO/IEC/IEEE 24765).	*Important*
	Recoverability	degree to which, in the event of an interruption or a failure, a system can recover the data directly affected and re-establish the desired state of the system.	*Important*
Security: degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization.	Confidentiality	degree to which a system ensures that data are accessible only to those authorized to have access.	*Important*
	Integrity	degree to which a system prevents unauthorized access to, or modification of, computer programs or data (ISO/IEC/IEEE 24765).	*Important*
	Non-repudiation	degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later (Adapted from ISO 7498-2:1989).	*Important*
	Accountability	degree to which the actions of an entity can be traced uniquely to the entity (Adapted from ISO 7498-2:1989).	*Important*
	Authenticity	degree to which the identity of a subject or resource can be proved to be the one claimed (Adapted from ISO/IEC 13335-1:2004).	*Important*
Maintainability: degree of effectiveness and efficiency with which a product or system can be modified by the intended Maintainers.	Modularity	degree to which a system is composed of discrete components such that a change to one component has minimal impact on other components (ISO/IEC/IEEE 24765).	*Important*
	Reusability	degree to which an asset can be used in more than one system, or in building other assets (Adapted from IEEE 1517-2004).	*Essential*
	Analysability	degree of effectiveness and efficiency with which it is possible to assess the impact on a system of an intended change to one or more of its parts, or to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.	*Important*
	Modifiability	degree to which a product or system can be effectively and efficiently modified without introducing defects or degrading existing product quality.	*Important*
	Testability	degree of effectiveness and efficiency with which test criteria can be established for a system and tests can be performed to determine whether those criteria have been met (Adapted from ISO/IEC/IEEE 24765).	*Essential*
Portability: degree of effectiveness and efficiency with which a	Adaptability	degree to which a system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage	*Essential*

system, product or component can be transferred from one hardware, software or other operational or usage environment to another.		environments.	
	Installability	degree of effectiveness and efficiency with which a system can be successfully installed and/or uninstalled in a specified environment.	*Important*
	Replaceability	degree to which a system can be replaced by another specified software product for the same purpose in the same environment.	*Desirable*