IFE/HR/E – 2006/006

Dependable Requirements Engineering and Change Management of Security-Critical ICT-Driven Systems

	KJELLER	**HALDEN**
Address	**NO-2027 Kjeller**	**NO-1751 Halden**
Telephone	**+47 63 80 60 00**	**+47 69 21 22 00**
Telefax	**+47 63 81 63 56**	**+47 69 21 23 22**

Report number **IFE/HR/E-2006/006**	**Date** 2006
Report title and subtitle Dependable Requirements Engineering and Change Management of Security-Critical ICT-Driven Systems	**Number of pages** 9
Project/Contract no. and name O-8088, HMS-Petroleum competence development project on Change, Organisation and Technology	**ISSN** 0807-5514
Client/Sponsor Organisation and reference Research Council of Norway	**ISBN** 82-7017-567-6

Abstract

This paper brings into focus the influence of dependable requirements engineering and change management in the dependability of specially security-critical ICT-driven systems, and suggests efforts towards a unified framework for taking into account the correlations and conflicts between security and other system dependability factors (safety, reliability, accessibility, flexibility, user-friendliness, etc.) when engineering the ICT-driven systems and when introducing changes in the original requirements defined at different levels of the systems' development process.

Keywords: ICT-Driven Systems, Dependable Requirements Engineering, Change Management

	Name	Date	Signature
Author(s)	Atoosa P-J Thunem	2006-01-23	
Reviewed by	Harald P-J Thunem	2006-01-27	
Approved by	Øivind Berg	2006-04-03	

DEPENDABLE REQUIREMENTS ENGINEERING AND CHANGE MANAGEMENT OF SECURITY-CRITICAL ICT-DRIVEN SYSTEMS

Atoosa P-J Thunem
Institute for Energy Technology, NO-1751 Halden, Norway
atoosa.p-j.thunem@hrp.no

SUMMARY/ABSTRACT

Especially within Information and Communication Technologies (ICT) and their applications in different branches, several approaches have been proposed towards a better system development process.

Nevertheless, despite the availability of detailed guidelines behind each approach (also called *life cycle model*), none links the concept of *requirement* to other development stages than the very first stages of the development process, i.e., where the business case and the overall requirements are defined. Furthermore, the models do not offer guidelines on how to achieve traceability among these requirements. Also, if system properties are addressed at all, the implied concern is almost entirely on functional and operational aspects, and not other dependability factors such as safety, security, reliability, flexibility and maintainability. To exemplify, there exist no instructions on how the security issues associated with the specific system architecture or application domain can influence the length of a certain development stage, or the amount of certain sub-activities during the iteration. The lack of addressing dependability factors in available life cycle models explains also why the concept of risk and risk analysis has not been an issue to take into account for these models.

In order to remain informative, communicative and applicable for several groups of users, systems driven by ICT (Information and Communication Technology) usually offer a relatively high degree of application possibilities. The systems are typically open-ended or have interfaces with open-ended systems, and must therefore be secured against possible threats or malevolent actions. The introduction and management of even minor changes in such systems can lower the system applicability or make the system potentially dangerous to use. In the first case, the reason could be a new security countermeasure that lacks accounting for all impacts on the system. In the latter case, the reason could be that a change has made a security guard practically useless.

Change management is closely related to the dependability of the approach used for carrying out the system development *process* (system life cycle) and the system itself, the *product*. All life cycle models, however, lack indications on *how* to carry out the development process. This paper suggests that the remedy for the problem lies in how to perceive the discipline of *requirements engineering*. The paper suggests that assuming the discipline to deal with not only the higher stages (levels or phases) of the system life cycle but also all other stages indeed offer the answer to how a system development process is in practice followed. Applying the concept of requirement to all levels of the system life cycle while requirements engineering will force the engineer to specify how each level of a V, Spiral, Water Fall or RUP model is carried out and what are the links amongst the levels.

Clear and sound change management mechanisms are necessary to ensure the dependability of the task of requirements engineering, given the task is understood as suggested in this work. Typically, the requirements at each stage of the system development process undergo many changes before the development is completed. These changes may be due to changes in the prospected operation environment, but may also happen simply as a result of improved insight during the development or a desire to incorporate technological advances into the development stages (use of new methods, procedures, tools, etc.). Thus, it appears that change management mechanisms themselves depend highly on whether they utilise requirements traceability mechanisms.

This paper brings into focus the influence of dependable requirements engineering and change management in the dependability of specially security-critical ICT-driven systems, and suggests efforts towards a unified framework for taking into account the correlations and conflicts between security and other system dependability factors (safety, reliability, accessibility, flexibility, user-friendliness, etc.) when engineering the ICT-driven systems and when introducing changes in the original requirements defined at different levels of the systems’ development process.

1 INTRODUCTION

The development of computers and computerised information and communication systems has been very rapid over the last decades. New generations of computerised equipment with improved performance have been introduced in the market at a high rate. This development is observed for all branches, where new and improved computerised systems have been installed for performing increasingly important and complex functions. Consequently, the development has also given rise to growing number of vulnerability sources, which may endanger physical as well as logical protection of the environments the systems are functioning within, and thus may eventually jeopardise human and public safety.

Within the nuclear domain and traditionally, physical protection of nuclear facilities has been aiming at establishing detection and response conditions that will minimise physically present possibilities for unauthorised removal[1] of nuclear material, and accidental or deliberate release (sabotage[2]) of nuclear material. Therefore, the term security has traditionally been used to address means for the prevention of unauthorised *physical* access to physical assets such as space and equipment. Meanwhile, the growing application of advanced computers and computerised information and communication systems at nuclear facilities have made a new kind of threats and attacks conceivable through interconnected systems within the facility and between facilities in different locations nationally and globally. This tendency is also seen within other domains, such as aviation, commerce, healthcare, and society infrastructure.

The common architecture of computerised systems driven by information and communication technologies (or in short ICT) makes it inherently impossible to suggest any fixed physical or logical boundaries for the systems, as continuous improvement of the systems with regard to accessing and processing information and then communicating the information with potential information users (could be other ICT-driven systems) constitutes the very core nature of the ICT-driven systems. The growing applicability and thus complexity of these systems within different domains and their related industrial branches has of course made the areas more vulnerable than ever. The new sources of vulnerabilities need to be responded to in a stringent and balanced manner. The ICT-driven systems are for example used in safety and safety-related systems, where their unavailability or malfunction may have impact on public safety. They are also used to control access to sensitive areas, where their unavailability or malfunction may introduce hazards either through unauthorised access or denial of access for authorised individuals. The systems are in addition used to store important and sensitive data, and possible deficiencies or susceptibilities in these cases may lead to loss of important data or release of sensitive information. At the same time, the complexity of the ICT-driven systems makes it difficult to identify possible trends, patterns or sequences that can introduce threats of various kinds to the systems and their surroundings. Even if the threats are assumed identified, the possible countermeasures often involve decisions hard to make and tasks complicated to implement.

Nevertheless, experience from the use of ICT-based systems in areas such as military, national security, critical infrastructure and banking shows that systems without a proper protection against threats and attacks may quickly become unavailable or unreliable. Experience shows also that the security of ICT-driven systems requires alertness throughout their whole *life cycle*, including functional and operational extensions or reconfigurations, improvement of design or implementation, and maintenance. Finally, experience shows that any security-related consideration must not only have operational facilities in focus, but also facilities under construction, and particularly within the nuclear domain, facilities that have been decommissioned. Such focus is needed, as undue or lack of access to important systems has the potential to introduce threats regardless of the operational state of the facilities.

For security-critical ICT-driven systems, change management is closely related to the dependability of the approach used for carrying out the system development *process* (system life cycle) and the dependability of the system itself, the *product*. All life cycle models, however, lack indications on *how* to carry out such development process. This paper suggests that the remedy for the problem lies in how to perceive the discipline of *requirements engineering*. The paper suggests that assuming the discipline to deal with not only the higher stages (levels or phases) of the system life cycle but also all other stages indeed contributes to the answer for how a system development process for the systems in focus is in practice followed. Applying the concept of requirement to all levels of the system life cycle while requirements engineering will force the engineer to specify how each level of a V, Spiral, Water Fall or RUP model is carried out and what are the links amongst the levels.

[1] It is presumed that authorised removal of nuclear material is usually not characterised as accidental removal.

[2] Unauthorised removal of nuclear material could of course have sabotage as its ultimate aim.

Clear and sound change management mechanisms are necessary to ensure the dependability of the task of requirements engineering, given the task is understood as suggested in this work. Typically, the requirements at each stage of the system development process undergo many changes before the development is completed. These changes may be due to changes in the prospected operation environment, but may also happen simply as a result of improved insight during the development or a desire to incorporate technological advances into the development stages (use of new methods, procedures, tools, etc.). Thus, it appears that change management mechanisms themselves depend highly on whether they utilise requirements traceability mechanisms.

This paper brings into focus the influence of dependable requirements engineering and change management in the dependability of specially security-critical ICT-driven systems, and suggests efforts towards a unified framework for taking into account the correlations and conflicts between security and other system dependability factors (safety, reliability, accessibility, flexibility, user-friendliness, etc.) when engineering the ICT-driven systems and when introducing changes in the original requirements defined at different levels of the systems' development process.

The paper addresses the relationship between security and safety from a rather different perspective than usually observed and applied. This perspective is at the same time a part of the paper's prime message, which is that security for ICT-driven systems ought to be described based on a much broader perception of system dependability than currently established. The paper especially highlights the influence on the security of ICT-driven systems by all other dependability factors and on that basis suggests a framework for ICT security profiling, where several security profiles are assumed to be valid and used in parallel for each ICT-driven system, sub-system or unit. The paper emphasises that awareness about the existence of these profiles plays a very crucial role in a dependable requirements engineering of security-critical ICT-driven systems, as the dependability factors will in this manner become integrated into the specified requirements at different levels of the development process. This will in turn contribute to a more trustworthy change management, as the dependability-informed requirements will provide indications of the risk factors related to the changes.

2 THE CONCEPT OF SECURITY AS A DEPENDABILITY FACTOR

During the recent years, technological research within security has evolved from computer and IT security, through cyber and information security and now to the rapidly growing scope of ICT security. During the era of IT and within the domain, the topic of security has for many years been perceived of as a "goodness" factor particularly relevant to IT in general and Telecommunications in particular. In the light of this, the topic of security from a pure technological point of view has been believed to be a function of mainly three variables, the notorious CIA (*Confidentiality*, *Integrity* and *Availability*). In accordance with the increasing complexity of information and communication technologies and their applications and especially within computer security, *Accountability*[3] is also believed to be the fourth deciding variable [1]. All four variables are mutually related. Nevertheless, the integration of ICT systems into all groups of society infrastructure has seriously challenged the validity of the CIAA belief. Within the ICT community, a common consensus today is that the deciding CIA variables are closely related to factors, which traditionally have not been regarded as of technological nature. The most compelling evidence is the issue of *safety*: While *security in the context of safety* has so far been an issue only within certain industrial domains such as the nuclear field, it has become more relevant today for other areas, e.g., healthcare and telemedicine. Examples of other factors increasing in their importance are trust, (data) protection of personal privacy, user-friendliness [2][3], robustness, maintainability, flexibility, and mobility.

For many years, sociological, financial, political, defence-political, jurisprudential and environmental observations and analyses have been contributing to a non-technological understanding of security. Then again, the observations and analyses made by these areas today cannot deny the major role of insight into technological trends such as the advance of ICT-driven systems on how to understand and deal with security. One example is from the banking domain where non-technological perceptions of security are among the oldest and where such perceptions today are replaced by modern views in accordance with incorporating ICT into the domain.

The above two paragraphs together indicate the inevitable: Ongoing and future security research efforts within various disciplines and application areas cannot be mutually exclusive, if wished to achieve

[3] A system's accountability is usually used to address a quality of a system that makes it possible to trace a security breach (related to one or several from CIA) caused by an artefact uniquely to that artefact.

an acceptable level of success. In other words, security research is by nature a multi-disciplinary and multi-sectoral research area.

Based on the above, it is not far from the (relative) truth to claim that competence in technological pillars of the ICT domain and dependability analysis, gained knowledge and experience within other domains that are relying on and applying ICT-driven systems, and focus on continuously learning from, exploiting and engaging other disciplines and application areas in the efforts within security research all contribute to better understanding of the relationships between the security on one side and other dependability factors on the other side, and hence to more dependable requirements engineering of about-to-be-constructed systems as well as effective and long-lasting change management mechanisms and also countermeasures against possible threats to the existing systems eventually resulting in serious security breaches [4].

To begin with understanding such relationships, the following provides detailed definition of safety and security and their associated risk. The definitions are not only in agreement with the corresponding definitions offered by applied international standards (e.g., IEC 61508), but also are more advanced, as far as the level of detail and clarity of involved terms are concerned.

2.1 Security, safety and their associated risk

The term **safety** is associated with a system's[4] physical condition not being harmed or damaged by its outside environment (including humans). At the same time, a system contributes to the safety of its outside environment, when the system is able to function and to be used as intended or expected without harming or damaging this environment. Thus, safety is used to express the prevention of unacceptable *risk* of *harm*. Harm and risk are defined as follows [5]:

- Harm is the physical injury, or the physical damage to condition or property of a system or its outside environment, caused by an intended or unintended action or an event.
- Risk is a collective effect (qualitative or quantitative) of the occurrence likelihood of a hazard causing harm and the degree of severity of the harm, given the degree of vulnerability of the system or its environment subject to that harm.

The perception of failure of a safety-related system can vary considerably depending on the application in focus. It is this variation that leads to concepts such as the "level of safety", the "Safety Integrity Level" (SIL), and the “As Low As Reasonably Possible” (ALARP) for a system.

In general, the term safety is more often applied for living beings than, e.g., pure technological systems. Bearing the physical condition and protection of a system in mind, however, the term is equally applicable for all systems.

The term **security** is associated with the protection of a system's *assets* such as the information[5] and information processing resources, from being *threatened* to unintended or intended damage by the system's outside environment. Thus, a system's level of security may decline without affecting the system's level of safety. As an example, the confidentiality of a nuclear scientist's knowledge carried by its brain may be intentionally disclosed, hence causing the scientist's information security level to decline, without affecting the scientist's level of safety in any manner.

Of course, a security breach for a system might affect the safety of its outside environment, both in a positive and negative manner. In the context of security, threat and risk are defined as follows [6]:

- Threat is defined as an intended or unintended action or an event that might jeopardise the security of a system.
- Risk is defined as the collective effect of the occurrence likelihood of a particular threat and the degree of severity of the threat (i.e., the potential consequences of the threat, if it did occur), given the degree of vulnerability of the system subject to that threat.

In general, the term security is more often applied for technological systems than living beings. Bearing the assets of a system in mind (i.e., its information and information processing resources),

[4] A *system* is a compound of interrelated and interconnected entities that function together in order to attain a set of overall goals for the system. Scientifically, a system can be of natural character (e.g., a human being) or human-made (e.g., an oven, a television set, or the nation-wide electricity power network).

[5] Thus, the asset can also include *knowledge*, which is a piece of information already declared to have a certain value of use.

however, the term is equally applicable for all systems that possess information. Nevertheless, the tradition of relating safety to the living beings and security to technological systems (or "machines") is still helpful, when addressing the relationship between safety and security (such as "security in the context of safety"). The best illustration existing today is perhaps *the three laws of Robotics*[6]:

- A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- A robot must obey orders given it by human beings except where such orders would conflict with the First Law.
- A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

2.2 Security-related issues important to dependable requirements engineering and change management

In order to gain interdisciplinary competence within dependable requirements engineering and change management of security-critical ICT-driven systems used in different domains, some issues call for further exploitation. Four of these are explained bellow.

There is a need for identification of technological and non-technological factors defining, deciding or relating to the level of security in security-critical systems, society and state infrastructures and processes. A society infrastructure can be the nationwide electricity network, where the relationships among factors such as availability, integrity, maintainability and safety are crucial to identify in order to ensure an acceptable level of security. A state process can be a continuously updated collection of guidelines and means to implement actions to protect the society against the threat caused by international terrorism. Here, it is of paramount importance to clarify factors such as trust, (data) protection of personal privacy, user-friendliness (e.g., of instructions) and robustness (e.g., against vulnerability sources), in order to establish a certain level of belief in security countermeasures.

Both overlaps and discrepancies across involving sectors need to be identified, so that it becomes easier to develop common methodologies and models to deal with security in present and future complex systems, infrastructures and processes, without causing the tailor-made methodologies and models in each sector to become invalid or ineffective.

There is a need for integration of risk factors into the established security affecting and security related factors addressed above, so that the entire risk management process, including risk analysis, assessment and treatment can be mapped into the development process (lifecycle) of security-critical systems, infrastructures and processes, hence resulting in risk-informed development processes with security as their core focus. In practice, this means that there should be a risk model involved as an integrated part of a certain security related factor for, e.g., a modernised ICT system, an updated guideline, or a modified state decision. This factor could be the "accepted" level of data protection of personal privacy, so that the consequence of its change to other levels in the future can be viewed and studied.

The focus should be intensified on research within communication and traceability of security affecting and security related requirements for all systems and processes used in technological/industrial, sociological, financial, political, defence-political, jurisprudential and environmental applications and sectors, in addition to society and state infrastructures. Joint efforts from different disciplines within this particular area are central in dealing with continuous changes in the requirements for such complex systems, processes and infrastructures, as a response to modernisation and improvement needs, as well as social, economical, environmental, technological and political influences from the world.

3 ICT SECURITY PROFILING

3.1 The relationships between security and other dependability factors

When it comes to development or application of ICT, analysing relevant dependability factors plays a crucial role in the credibility of the results from any R&D project dealing with technologies,

[6] The three laws of Robotics were established by the father of Robotics, Isaac Asimov whose ideas and theories on possible patterns of relationships between humans and machines have for many years inspired the masters of information and communication engineering as well as human factors engineering.

methodologies and tools for engineering, using and maintaining any product or service that, towards attaining its purpose, is either based on or making use of ICT. At the same time, ICT-oriented commercial applications usually have a very high focus on certain dependability factors such as availability, accessibility, efficiency and flexibility, at the expense of others such as security, maintainability, accountability and safety[7]. For many purposes, such a focus is sufficient. However, problems arise when attempting to use the same applications for purposes that are critical with regard to the down-prioritised or neglected factors [7]. In order to qualify and thus further develop those applications, the challenge is not just to achieve a "mediocre" balance but the most optimal one. Clearly, such a balance is highly purpose and context dependent, even within a specific field.

As stated previously, the topic of security from a pure technological point of view has been believed to be a function of mainly confidentiality, integrity, availability and accountability. As explained earlier, however, this perception of security is no longer sufficient to analyse and treat security aspects. In fact, this paper advocates that security and in particular ICT security depends on all other dependability factors currently defined or specified. This is illustrated in Figure 1.

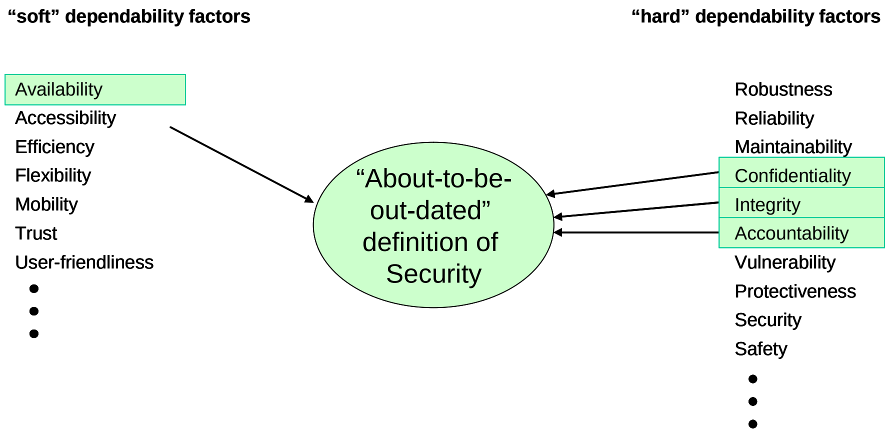

Figure 1. Soft and hard dependability factors.

To better describe the security factor for a certain system fulfilling certain applications or performing certain tasks, dependability factors might be grouped in various fashions. Based on the level of independency, for example, some factors might be defined to be a collection of others, e.g., safety. Based on the generality issue, on the other hand, some factors might be understood as generic for all applications (robustness) and others to be highly application-oriented (confidentiality). Nevertheless, all factors separately and together decide different models for security, hence leading to different security profiles for the same system, depending on the application or task in focus.

3.2 A framework for ICT security profiling

Considering three typical tasks of planning, inspection and emergency for a certain application involving the use of security-critical ICT-driven systems, one can think of different dependability profiles that are produced based on a certain type and level of application of the system, as illustrated in Figure 2.

Now, recalling the discussion at the previous section, a framework for ICT security profiling will involve identifying the most critical dependability factors related to various vulnerability and threat scenarios for security-critical ICT-related applications. This identification is conducted by analysing and assessing a wide range of relevant dependability factors, where the analysis and assessment will be based on information from the scenarios, the application or task in focus, and available historical dependability data. Next, the accepted level of these factors, eventually altering the functionality and operational modes of the application-triggered features of the ICT-driven system is decided by a model-based vulnerability and risk analysis and assessment (hence including models of the features, and qualitative as well as quantitative analysis) together with available historical data [8][9][10]. Once the levels for the most

[7] In this paper, the factors belonging to the former category are called "soft", whereas those belonging to the later category are called "hard".

critical factors are decided, other related dependability factors are analysed and their level adjusted under the condition of preserving the level for the critical factors. The results are ICT security profiles displaying the influence from related dependability factors and tailor-made for various applications and tasks, such as planning, inspection and emergency, which are security-critical in diverse degrees. Figure 3 illustrates. As implied, the framework includes a generic dependability analysis and assessment unit, and a generic model-based vulnerability and risk analysis and assessment unit, together with the internal and external communication paths.

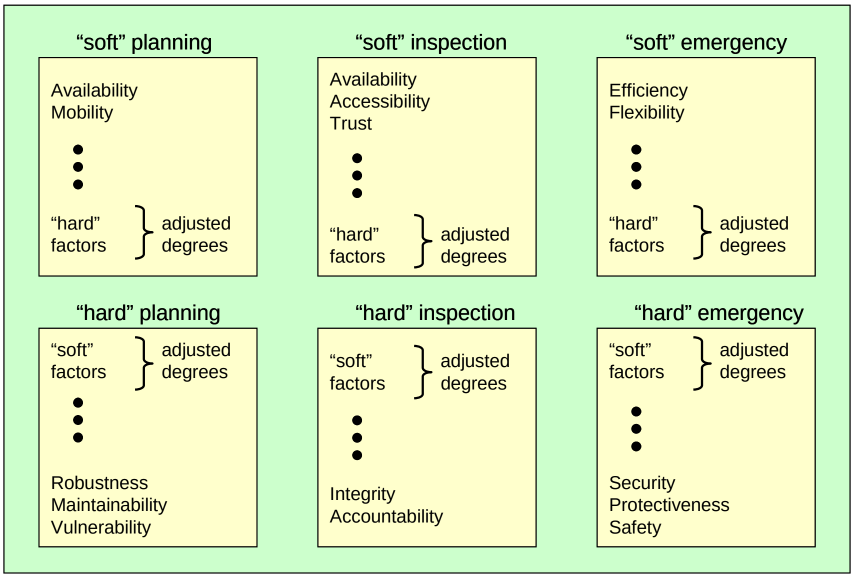

Figure 2. Different dependability profiles that are produced based on a certain type and level of application of the system.

4 TOWARDS AN APPROACH FOR DEPENDABLE REQUIREMENTS ENGINEERING AND CHANGE MANAGEMENT

The following describes ideas towards a practical approach for dependable requirements engineering and change management of computerised systems. The ideas are the result of joint research within requirements engineering, systems modelling (mainly based on object-oriented, semi-formal and agent-oriented modelling methodologies), and model-based risk analysis and assessment.

4.1 The background

Especially within ICT and its application in different branches, several approaches have been proposed towards a better system development process. Among the most applied is the Rational Unified Process (RUP) that provides a matrix-oriented lifecycle model highly supporting the time aspect of the lifecycle. Here, the road map is formed by two main activity categories: disciplines followed to develop the system and phases related to its life-path. The workload in each phase is decided by the actual discipline in focus: More elaboration phase is required during the design discipline, whereas more construction is needed during the implementation. Figure 4 illustrates another extended version of the RUP model, called the Enterprise Unified Process (EUP).

Nevertheless, despite the availability of detailed guidelines for sub-activities in each discipline and for the number of iterations in each phase, neither RUP nor any other lifecycle models provide guidelines on how to achieve traceability among phases and disciplines. Also, if system properties are addressed at all, the implied concern is almost entirely on functional and operational factors, and not other dependability factors such as safety, security, reliability, flexibility and maintainability. To exemplify, there exist no instructions on how the security issues associated with the specific system architecture or application domain can influence the length of a certain phase, or the amount of certain sub-activities during the iterations. The lack of addressing dependability factors in available life cycle models explains also why the concept of risk and risk analysis has not been an issue to take into account for these models.

As already mentioned change management is closely related to the maintainability of the system development process and the result (product) of this process, the operational and applied system itself. In reality, clear and sound change management mechanisms are necessary to ensure the dependability of the task of requirements engineering. Typically, the requirements at each stage of the development process of a system undergo many changes before the development is completed. These changes may be due to changes in the prospected operation environment, but may also happen simply as a result of improved insight during the development or a desire to incorporate technological advances into the development stages (use of new methods, procedures, tools, etc.). Thus, it appears that change management mechanisms themselves depend highly on whether they utilise requirements traceability mechanisms.

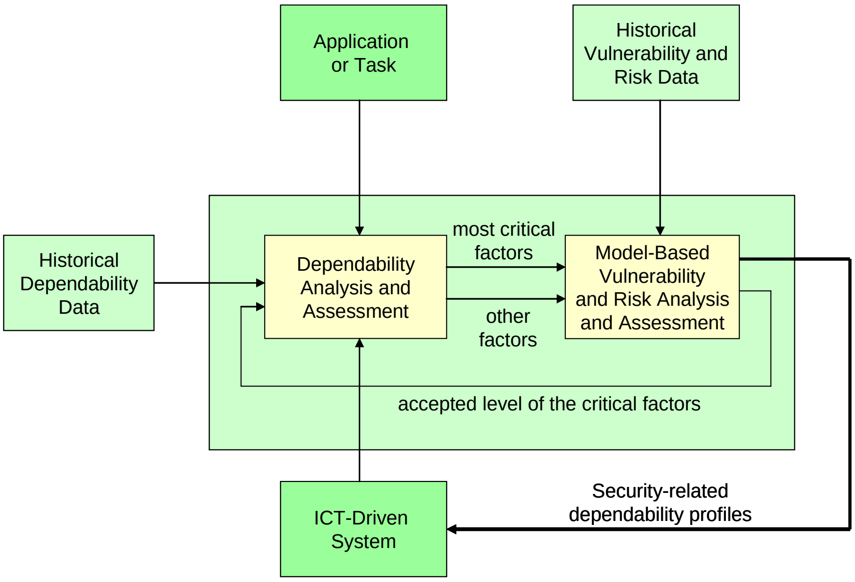
Application or Task
Historical Vulnerability and Risk Data
Historical Dependability Data
Dependability Analysis and Assessment
most critical factors
other factors
Model-Based Vulnerability and Risk Analysis and Assessment
accepted level of the critical factors
ICT-Driven System
Security-related dependability profiles

Figure 3. A framework for ICT-security profiling based on generic dependability analysis and associated vulnerability and risk analysis.

4.2 The elements of the prospective approach

The approach advocates a perception of a requirement to be applicable for *all stages* of the system development process and not only the high-level stages. Based on this perception, the requirements should be identified, specified, validated and verified, and finally implemented for all stages of the system development process. Referring to the disciplines in the RUP/EUP model shown in Figure 4, this means that requirements should be defined and specified in an inter-disciplinary fashion.

Furthermore, the approach aims at making a computerised system and its lifecycle analysable with regard to several *dependability factors* such as safety, security, reliability, flexibility and maintainability [4]. This means that dependability factors are integrated into the lifecycle, thus also integrated into the very definition of dependability-critical requirements. Additionally, the approach recognises the relationship between how a requirement can be met and how it can be opposed to, due to unexpected or unwanted events. Thus, the requirements expressed in this approach are also *risk-informed*. Finally, the approach acknowledges the importance of well-defined *traceability mechanisms* to provide links between the requirements belonging to a particular stage or different stages of the lifecycle.

In order to validate and verify the requirements and their changes for security-critical ICT-driven systems in a dependable manner, different analyses are needed as an integrated part of carrying out each stage of the development process. The most important analysis is that of thorough risk analysis with focus on one or several security profiles that need to be analysed and assessed, before introducing any progress or any change. There is a need for *traceability* of the requirements for a specific risk analysis method, in accordance with the requirements of system development process and its product the risk analyst is supposed to analyse.

5 CONCLUSIONS

This paper has addressed issues related to requirements engineering and change management of security-critical ICT-driven systems. The paper has emphasised that security for ICT-driven systems ought to be described based on a much broader perception of system dependability than currently established. The paper especially has highlighted the influence on the security of ICT-driven systems by all other dependability factors and on that basis has suggested a framework for ICT security profiling, where several security profiles are assumed to be valid and used in parallel for each ICT-driven system, sub-system or unit. It has been stated that awareness about the existence of these profiles plays a very crucial role in a dependable requirements engineering of security-critical ICT-driven systems, as the dependability factors will in this manner become integrated into the specified requirements at different levels of the development process. This will in turn contribute to a more trustworthy change management, as the dependability-informed requirements will provide indications of the risk factors related to the changes.

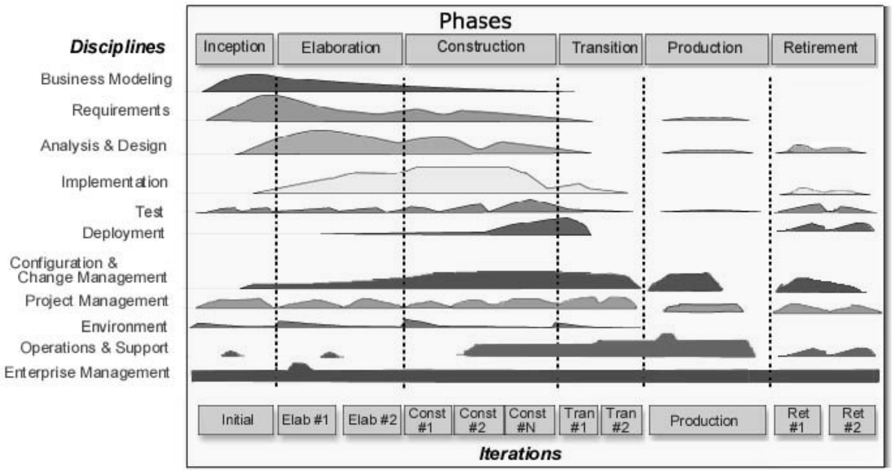

Figure 4. The Enterprise Unified Process (EUP).

REFERENCES

1. NIST: Computer Security, Underlying Technical Models for Information Technology Security, http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf.
2. EVANS, S., Heinbuch D., Kyle, E., Wallner, J.: “Agency Risk-Based Systems Security Engineering: Stopping Attacks with Intention”, IEEE Security & Privacy Transactions, November/December 2004, pp 59-62.
3. Yan, J., Blackwell, A., Anderson, R., Grant, A.: “Password Memorability and Security: Empirical Results”, IEEE Security & Privacy Transactions, September/October 2004, pp 25-31.
4. Thunem, A. P-J.: “Modelling of Knowledge Intensive Computerised Systems Based on Capability-Oriented Agent Theory (COAT)”, the International IEEE Conference on Integration of Knowledge Intensive Multi-Agent Systems, IEEE-KIMAS’03, pp 58-63, Cambridge (MA), USA, 2003.
5. International Atomic Energy Agency: “Planning and Preparing for Emergency Response to Transport Accidents Involving Radioactive Material”, Safety Guide, Safety Standard Series, No. TS-G-1.2 (ST-3).
6. International Standardisation Organisation: “Banking and related financial services (standards)”, ISO TC68.
7. Thunem, A. P-J: “Security Research from a Multi-Disciplinary and Multi-Sectoral Perspective”, SafeComp 2005 international conference, pp 381-389, Fredrikstad, Norway, 2005.

8. Nicol, D. M., Sanders, W. H., Trivedi, K. S.: “Model-Based Evaluation: From Dependability to Security”, IEEE transactions on Dependable and Secure Computing, Vol. 1, No. 1, pp. 48-65, January-March 2004.
9. Grance, T., Hash, J., Stevens, M.: “Security Considerations in the Information System Development Life Cycle”, 800-series, No. 800-64, Recommendations of the National Institute of Standards and Technology (NIST), 2003, USA.
10. Thunem, A. P-J: “A Cognitive and Formal Terminology for Descriptive Parameters in Concurrent Real-Time Distributed Software Systems”, published as Chapter 2, Part 3, pages 229-248, in the book “Soft Computing for Risk Evaluation and Management”, ISBN 3790814067, Physica Verlag Publisher, 2001.