Towards Advanced Enterprise Information Systems Engineering - Solving Resilience, Security and Usability Issues within the Paradigms of Socio-Technical Systems

Wilson Goudalo, Christophe Kolski

Towards Advanced Enterprise Information Systems Engineering
Solving Resilience, Security and Usability Issues within the Paradigms of Socio-Technical Systems

Wilson Goudalo[1,2] and Christophe Kolski[1]
[1]*LAMIH-UMR CNRS 8201, University of Valenciennes, Valenciennes, France*
[2]*Research and Innovation Department, ABE - Advanced Business Engineering, Lagny, France*

Keywords: Enterprise Information System, System Resilience, Information Security, Privacy, Human-Computer Interaction, Usability, User eXperience, Socio-Technical Systems, Design Patterns.

Abstract: Resilience and Security are very important attributes for most enterprise Information Systems (IS). These systems have human users with various capabilities, experiences and behaviors. Therefore, they have to be resilient, secure and usable. Resilience requires the capacity to prepare and adapt, facing perpetuating evolutionary conditions, and to restore full capability after an incident or an attack. We track and solve Resilience, Security and Usability issues jointly in Enterprise IS. This challenge requires considering the ergonomics of interactions, effectiveness and efficiency of the task realization, user satisfaction, and trust as well as human feelings when using the secure services. In this paper, we propose an approach based on paradigms of socio-technical systems to model the interplay between resilience, security and usability. We detail a case study illustrating the proposed approach and detailing the elaboration of user-experience-based design patterns.

1 INTRODUCTION

Information systems, and more precisely the services they deliver, have completely invaded our lives and play an increasingly prominent role. This is verified for individuals, as well as for organizations and for enterprises (Larson, 2008).

Security concerns are crucial in many services (SBIC, 2008), (IBM, 2014), (KPMG, 2014) and (Umhoefer, 2014). As a quality attribute, the meanings of security have evolved, and the technologies in the industry and in the standards have adapted to this evolution. In the field of IT systems, the initiatives were mostly based on "securing the perimeter". In the case of Information system and the extended enterprise, initiatives have evolved into guaranteeing security strategy in depth. To improve the security strategy in depth, Goudalo and Seret (Goudalo, 2008) proposed a methodological approach that operates on building a membership canvas of all stakeholders of the company.

Therefore, there is an urgent need for new approaches focusing on human aspects including usability to ensure the security of systems. Indeed systems are used by humans, although they are increasingly automated. Ferrary showed that human resources are now at the heart of the business model of organizations and indicated "the human factor as a main source of operational risk in banking" (Ferrary, 2014). Cranor and Garfinkel's book indicates the research trends in security and usability (Cranor, 2005). Clarke and Furnell's book presents the state of the art on "the human aspect in success of the security" (Clarke, 2014). Most initiatives are carried on specific security solutions. We notice a lack of research on the overall engineering of security from the point of view of HCI (Human-Computer Interaction).

In this paper, we introduce first the concept of socio-technical systems as an engineering approach. We also explain how resilience, usability and security can be addressed by using a socio-technical systems approach. We introduce then our socio-technical systems resilience approach, through design patterns based on user experiences. A case study on medical analysis laboratory is used to illustrate the application of our suggested approach.

Goudalo, W. and Kolski, C.
Towards Advanced Enterprise Information Systems Engineering - Solving Resilience, Security and Usability Issues within the Paradigms of Socio-Technical Systems.
In *Proceedings of the 18th International Conference on Enterprise Information Systems (ICEIS 2016) - Volume 2*, pages 400-411
ISBN: 978-989-758-187-8

2 PARADIGMS OF SOCIO-TECHNICAL SYSTEMS

2.1 Socio-technical Systems versus Information Systems

The concept of *socio-technical system* was created in the context of labor studies by the Tavistock Institute in London by the end of the 50's (Trist, 1967) and (Emery, 1967). Sperber and Wilson treat the relevance of communication (and cognition) in social context (Sperber, 1995). Socio-technical systems aim to model all together human, social and technological capabilities in using and dealing with value added services. Singh defines socio-technical systems (STS) as multi-stakeholder cyber physical systems (Singh, 2013). They contend with complexity and change in both the cyber and the physical (social) worlds.

Socio-technical approaches can help the design of organizational structures and business processes as well as technical systems. It is largely acknowledged that systems which are developed using a socio-technical approach are more likely to be acceptable to end-users and to deliver real value to stakeholders. There are notable differences between IT systems and socio-technical systems modeling and engineering approaches in terms of interactions (figure 1):

(1) IT systems modeling focuses on the technical description of the components of the systems and the interactions between them in order to deliver a certain service.
(2) Social systems include all human interactions and cooperation, on social and cultural values.
(3) Information systems include all users' interactions with the IT systems, integrating their organization, implementation and management.
(4) Social-technical systems provide a way of understanding all human interactions with the various IT systems, their components, as well as cooperation with other systems. Socio-technical systems approach also the interactions between the systems, all the stakeholders and their organization and the entire social environment, both the cyber and the physical worlds.

These dimensions define the information in terms of interactions among actors, which can be: social reliance (actors rely on others to achieve their goals), and information exchange (actors exchange relevant information). As it will be detailed later on, many security issues arise from the interaction between actors, and on how the exchanged information is accessed. Therefore, user experiences are a main concern when analyzing security.

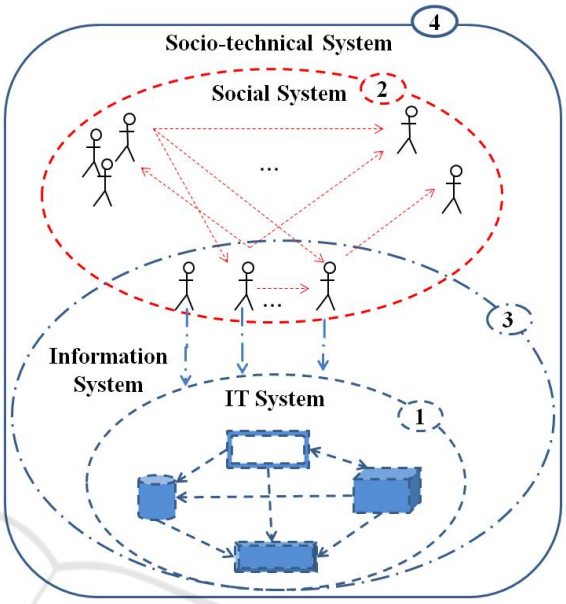

Figure 1: Socio-technical system representation.

2.2 Security and Privacy in Socio-technical Systems

In socio-technical systems, a set of human and automated agents (organized or not) interact to complete tasks, according to a certain objective. These have characters converging and/or diverging characters or conflicting objectives. Feelings and conflict situations are quickly transposed into the socio-technical systems.

In other words, users of the systems can be animated by malicious intents. This is the case of hackers who find their playground in the socio-technical systems. At the same time, the systems process personal data, sensitive data and very private character data. The tasks and data are sensitive and highly valuable.

In socio-technical systems, privacy is an important matter as well and must be protected. Actually, in the case of medical health data, the privacy requires special attention in terms of confidentiality. This is one of the objectives of security. Another objective of security is to guarantee the safety, the integrity and the reliability in processing all tasks. Difficulties of security in socio-technical systems arise in ensuring these objectives, due to two reasons.

First, solutions of security (a too constraining usage) may constitute security vulnerability or may prevent the completion of tasks. Secondly, users' behavior (errors, unintentional actions) may constitute security vulnerability. Human factors are a main source of operational risk in companies (Ferrary, 2014), and the trust of users in the socio-technical system is necessary (IBM, 2014). Clarke and Furnell's work reports success of security from the human aspect point of view (Clarke, 2014).

2.3 Usability Difficulties in Socio-technical Systems

Socio-technical systems expose users to social issues and to technology issues. Users resort to technology to deal with social issues and vice versa. Usability is a property that depends on interactions among users, systems, tasks, and environments where processes are operated in both the cyber and the physical words. Human factors are the main source of operational risk in companies (Ferrary, 2014). Usability concerns human factors. Usability is not a specific property of persons or of things, which we may measure by a "usability thermometer", or evaluate by applying widely accepted scientific formulas (Lewis, 2014).

Usability difficulties are focused on: Personal human factors experiments; Measuring behaviors and attitudes captured when users complete the key tasks; Measuring capabilities of the systems to provide adequate conditions for carrying out tasks (Cranor, 2015).

3 FOUNDATIONS

In this section, we define the concepts of resilience applied to socio-technical systems, usability and of security as well as the interplay between them.

3.1 Resilience Applied to Socio-technical Systems

Resilience is a major concern nowadays, in order to prevent an accident and more to restore a safer state after an accident or intentional fault (Laprie, 2008) and (ReSIST, 2015). Resilience, actually in relation to the concern of accident (Hollnagel, 2006), is applied in many domains such as socio-technical systems engineering.

Luzeaux (Luzeaux, 2011) wrote that "resilience is obtained via the capacity to monitor conditions at the edges of the performance envelope, and the ability to adapt the operational behavior of the system to potential developments in this envelope".

Luzeaux (Luzeaux, 2011) defined the four functions of the resilience, which are "avoidance (capacity for anticipation), resistance (the capacity for absorption), adaptation (the capacity for reconfiguration) and recovery (the capacity of restoration)". Figure 2 illustrates the resilience as an active virtue integrated in all operations and systems, in the field of defense (Palin, 2013).

Figure 2: Illustration of resilience in the field of defense (Palin, 2013).

Resilience is also applied in the field of information technology and security. In this case, resilience is defined as "the capacity to perform during an incident (unintentional accident or intentional fault) and then to come back to a normal state" (ANSSI, 2014).

In this context, we define resilience as the capacity to prepare and adapt facing perpetuating evolutionary conditions and to restore full capability after an accident or an attack.

3.2 Usability Models

HCI researchers have suggested different approaches in usability studies. Hertzum and his colleagues included cultural aspects in usability studies (Hertzum, 2007). Bevan suggested including flexibility and safety to create a more comprehensive quality-of-use model (Bevan, 2009). Seffah and his colleagues suggested quality-of-use schemes that included 10 factors, 26 sub-factors, and 127 specific metrics (Seffah, 2006); see also (Braz, 2007). Winter and his colleagues proposed a two-dimensional model of usability that associated a large number of system properties with user activities (Winter, 2007).

In socio-technical systems, usability rhymes with both the absence of usability problems and the measurements of effectiveness, efficiency, and satisfaction. Usability implies the ergonomic quality

of the Human Computer-Interaction, regardless of the type of access media.

In terms of ergonomic requirements, the ISO has published a number of standards. The ISO 9241-12 published in 1998 (ISO 9241-12, 1998) explains the seven principles for the presentation of information. We define them briefly: *Clarity* (the content is displayed quickly and accurately), *Discriminability* (the information can be distinguished with precision), *Brevity* (only the information required for the task are displayed), *Consistency* (the same information is presented identically on the entire application), *Detectability* (information is properly encoded in the right place), *Readability* (the information is easy to read), *Comprehensiveness* (the meaning of terms is clearly understandable). The ISO 9241-110, published in 2006 (ISO 9241-110, 2006), describes seven high-level principles for the design of dialogues: suitability for the task, self-descriptiveness, controllability, conformity with user expectations, error tolerance, suitability for individualization, and suitability for learning.

Shackel proposed three criteria to measure usability: performance of the task, user satisfaction and costs of use (Shackel, 2009). For the performance of the task, we consider the effectiveness and efficiency of interaction. An interaction is effective if users can perform the task successfully. An interaction is efficient if users can perform the task successfully for an acceptable period, with a consumption of acceptable resources. Satisfaction of users during the interaction considers the performance of the task and subjective feelings. The cost of the use considers, beyond the consumption of acceptable resources, the impact of the interaction on the health and safety of users, and on the reputation integrity of users in the socio-technical systems. The system must adapt to any user, within the predefined population, without distinction of age, size, ethnicity, educational or linguistic level, as well as those who have difficulty with some physical or cognitive operations. This adaptation must also comply with security requirements.

3.3 Security and Privacy Models

The family of standards ISO 2700x (ISO/IEC 2700x, 2010) is entirely dedicated to information security including the organizational dimension (private or public companies). The standards present how to establish, implement, maintain and continually improve a management system for information security. These standards model security in terms of confidentiality, integrity and availability of information by applying a risk management process. They give to all interested parties (users, operators and owners of socio-technical systems) the insurance that security risks are managed appropriately.

On one hand, we noticed how security risks are managed using a harmonized process, and secondly we noticed the three fundamental criteria of security that are confidentiality, integrity and availability of information. Briefly, we develop each of these four points:

1- The process incorporates the interested parties and their respective requirements. It takes into account the interfaces and dependencies between the activities of the organization and its stakeholders within the extended enterprise.
2- Confidentiality (Information should neither be made available or disclosed to a user, entity or unauthorized process).
3- Integrity (The information must not be modified, altered or destroyed in an unauthorized manner).
4- Availability (Access by an entity, an authorized user or process to the services offered by the socio-technical system must always be possible; Operations to illegally occupy the processing time must be detected). Other properties of the security of Information Systems, such as Proof, Traceability and Authenticity derived from these three basic criteria.

The security criteria characterize constraints or properties on system assets, describing their security needs. The harmonious process brings the answer, dealing with company issues that are human, financial, branding, regulatory and legal. Goudalo and Seret (Goudalo, 2009) define the process for the engineering of security of enterprise information systems in seven major activities designated by the term *Security Acts*. The first two of them (*Identifying business assets* and *Defining security goals to achieve*) assess security needs on corporate assets. Other international standards also address security and security risks of information system. This is the case of the ISO 15408 (Common Criteria, CC) focusing on three audiences that are producers, evaluators and users, the ISO 13335 and ISO 21827. We also identify local standards and norms as Cramm (in the United Kingdom), Mehari and Ebios (in France), Octave (USA and Canada). The basic criteria of security remain the same, and to them are added the various properties and attributes of security such as proof, trace, non-repudiation, identification, authentication, privacy, trust and others.

In socio-technical systems, the attributes of *Privacy* and *Trust* undeniably join to security. Westin, in his notable book "Privacy and freedom" opening the modern field of law and privacy, defined Privacy as "the request of individuals, groups and institutions to determine for themselves (on their own) when, how and to what extent information about them can be communicated to others" (Westin, 1968). Alain Westin adds that "every individual is constantly engaged in personal adjustment process in which balance the desire for intimacy with the desire of disclosure and communication." Moreover, Privacy is a legal topic with a critical issue, since disruption of Privacy deals with penal/criminal law (French Penal Code, 2015). We use Privacy as both the confidentiality and the integrity of information dealing with the private aspects of individuals, groups and institutions in society. In her course materials (Cranor, 2006) and (Cranor, 2015), Cranor defines different views on privacy: Privacy as limited access to oneself (the extent to which we are known to others and the extent to which the others have a physical access to us); Privacy as control of information (beyond limit of what others know about us, we must control, which implies individual autonomy, we can control the information in a meaningful way).

The presence of respect for the privacy policy (Privacy) builds consumer confidence. Rousseau et al. (Rousseau, 1998) define the trust as a psychological condition including the intention to accept vulnerability based on positive expectations of the intentions or behavior of another. Trustworthiness (reliability from the point of view of security) defines the property of a system which performs only what is required (except for an interruption of the environment, user errors and human operators, and attacks by hostile parts) and that does not make things (Schneider, 1998).

3.4 User Experience in Socio-technical Systems

The socio-technical system approach facilitates the identification and formulation of user experiences. A positive user experience is usually based on convenience (time savings or reduced physical or mental work), the confidence that the socio-technical system "works properly", and the perception of its usefulness. The concept of "works properly" implies (instills) the trust. According to Sasse (Sasse, 2007), the user experience takes into account all the usability criteria, with additional factors (Cranor, 2015). Birge (Birge, 2009) emphasizes the lack of research on the design of technical solutions for communication and information technology in the field of "user experience and security" (Trust and User eXperience - TUX).

In summary, the security objective is to evaluate, eradicate and prevent errors, faults and attacks. If occurrences, the resilience objective is to tolerate and outdo the impacts, and to guarantee services in degraded mode according to the conditions of the service layer agreements. The objectives of security and resilience must be ensured, while maintaining a positive user experience.

We specify that a good usability (HCI and positive user experience) should promote the success of the security and resilience. It is although vice versa.

4 A RESILIENT BUILT-IN APPROACH OF SOCIO-TECHNICAL SYSTEMS, BASED UPON DESIGN PATTERNS

Today, most of the security built-in systems are not usable. Users who have to use these systems bypass the security devices and this behavior generates security gaps.

The issue is to replace a security built-in system approach by a resilient built-in socio-technical system approach based on design patterns. This socio-technical approach takes into account interdependence between security and usability.

In such a way, this approach allows to adapt facing perpetuating evolutionary usage conditions and usability problems. Figure 3 portrays the underlying process in the proposed approach.

We use patterns to describe the problems and the solutions of security/usability problem. Patterns have been widely considered in many human endeavors that require a combination of skill and training. In the 70's architect Alexander pioneered the recognition, naming, and use of patterns, while working on urban planning. In the late 80's computer scientists working in the field of object-oriented design discovered Alexander's work and adapted design patterns to software (Salloway, 2002). Schumacher (Schumacher, 2003) argues that the security engineering can benefit from the use of patterns, but he fails to present specific patterns to accomplish this goal. The Open Group has edited a book on security design patterns (Blakley, 2004), but

has not addressed the alignment between usability and security.

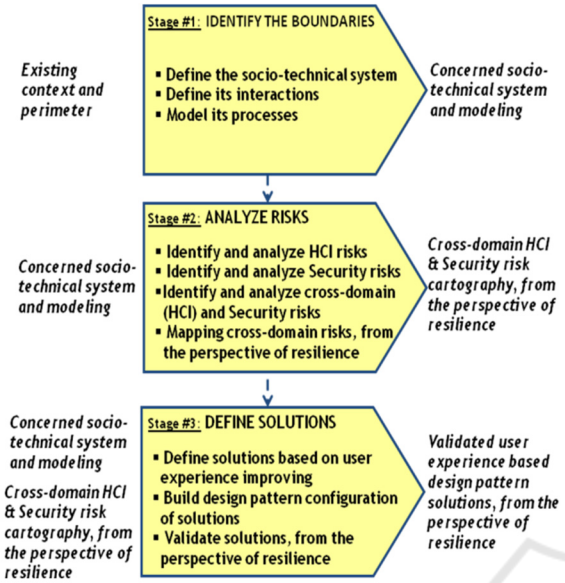

Figure 3: User experience based design pattern approach.

4.1 Stage #1: Identify the Boundaries

This stage consists in defining the boundaries of the eco-systems including the entire social environment and the various actors. We integrate their interactions in both the cyber and the physical worlds, using BPMN (Business Process Modelling Notation) to model the processes, activities (sub-processes) and individual tasks performed by each actor involved in the process. The detailed description of the interactions between the technical components of the information system is described using UML diagrams including use cases. Links between the BPMN and UML diagrams (misuse cases) are also described during this stage (Pietre-Cambacèdés, 2010).

4.2 Stage #2: Analyze Risks

This stage produces the list of potential problems. We use different methods to analyze the description of the socio-technical system produced during the previous stage including cognitive walkthrough (Wharton, 1994) (Mahatody, 2010), marked Petri Nets, simple and cross-domain risk analysis methods (DCSSI, 2009). Risks include on the one hand security threats (such as faults, frauds, blackmail, identity usurpation) and on the other hand usability issues. They lead to malfunction, denial of service or destruction of the socio-technical system.

The study focuses on the problem, the origins and the reasons as well as the consequences of not improving some aspects. This study highlights the relations of proximity and interdependence between the HCI and the privacy security. Our proposal uses firstly a multi-domain approach to risk analysis, and secondly it focuses on human factors. Problems are documented using for instance a storytelling approach detailing user experience, its failures and its possible improvement points (other methods are available in the literature). Problem documentation is based on learning and operational feedback about any other kind of incidents dealing with these risks.

4.3 Stage #3: Define Solutions

In the final stage, we resort to user experience in order to define the solutions that solve the points highlighted during the second stage. Actually, we look for the best improvement of user experience that underlies these identified points. The significant question addressed here is what makes the solution seen as a better – or worse – design concept, from a usable security perspective. Thus, how to detect a bad design in order to correct it?

We base the actions of this step on various experiments both in industry and academic research. As mentioned in section 3.3, Goudalo defined seven *security acts* constituting the engineering of information security (Goudalo, 2011). Although several researchers have discussed usable security design, Kai-Ping Yee has proposed a list of guidelines for addressing valid and nontrivial problems specific to usable security design (Yee, 2002): path of least resistance, active authorization, revocability, visibility, self-awareness, trusted path, expressiveness, relevant boundaries, identifiability and foresight.

This stage consists also in documenting each pattern using the format:

- Name of the design pattern;
- Description of the problem (or class of problems);
- Description of the solution;
- Consequences of applying the design solution;
- Validity of the solution. Qualitatively, each pattern should improve the user experience, e.g. according to one of the guidelines given by Kai-Ping Yee. Quantitatively, patterns should enhance in a measurable way the compromise between usability and security.

The design patterns for resilient built-in socio-technical systems must integrate both usability and security concerns in order to design efficient and usable security systems. These design patterns have to complete other works dealing with security architecture of systems (Ruault, 2015).

5 CASE STUDY

The case study, called *FI MedLab*, is related to the information system in a medical laboratory, also called clinical laboratory. Credibility of medical laboratories is paramount to the health and safety of the patients relying on the testing services provided by these labs. The international standard in use today for the accreditation of medical laboratories is ISO 15189 – Medical laboratories – particular requirements for quality and competence. A laboratory conducts tests on clinical specimens in order to get information about the health of a patient as pertaining to the diagnosis, treatment, and prevention of disease. Such information is highly security-sensitive, any error may have a direct impact on patient safety, privacy and the reputation of the laboratory.

An information system is in use in most laboratories today. It allows collecting data about patients, test records and the interpretation of test results. Information security and privacy risks have grown with the rapid growth in the number and types of people who have a legitimate role to provide access, use and transform the information and medical records. Tension often exists between security, privacy controls and usability needs. For example, access to the information system can be delayed by the need to first authenticate to ensure he/she is legitimate, and is provided with the right level of system access he or she requested. Some information has to be quickly available to a physician in the case of an emergency situation, but has not to be communicated broadly, since it deals with health and privacy. On the other hand, disclosing such information is a punishable offence, in many countries, for instance the article 226-22 of the French Penal Code.

The same can be said about anyone who wants to enter data in the system. Data entry errors because of a usability issue have fatal impact on the integrity of data, which is a key measure of security and privacy.

5.1 Stage #1: Identifying the Boundaries

FI MedLab is a socio-technical system which involves patients, internal and external operators, laboratories or medical partners, medical equipment suppliers, regulatory agency as well as IT services and applications providers, sometimes datacenters. The socio-technical system comprises various operational business processes (BP) that are grouped into three categories: pre-analytical, analytical and post-analytical processes (see Table 1).

Some operators have to access to certain kinds of information, but not to other ones. This depends upon the level of authorization and the user authentication. So, within the organizations, groups of users with respective roles and responsibilities have to be defined. Figure 4 shows a simplified model of these business processes using BPMN (Business Process Modeling Notation).

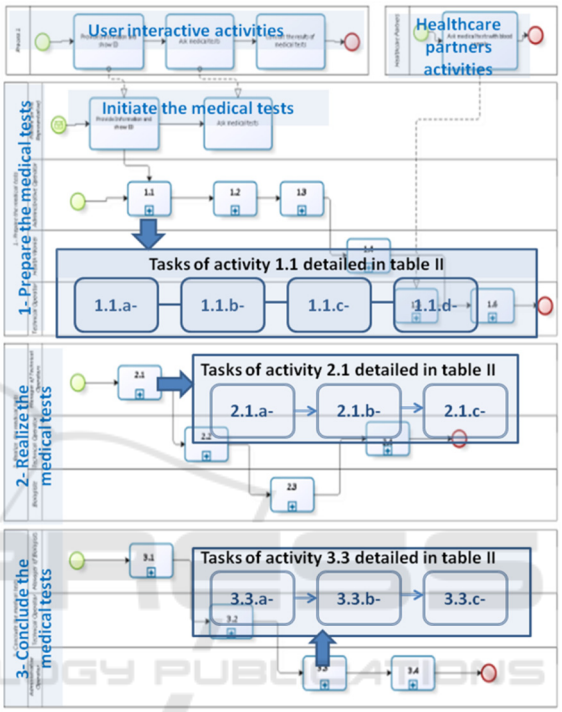

Figure 4: Modelling Business Processes (with focus on tasks with potential problems).

Table 1: Three business processes of FI MEDLAB.

1-	**Prepare the medical tests**
1.1-	*Manage the patient file (Create, Update, or Archive) (see Table 2)*
1.2-	Register a request for medical tests
1.3-	Charge the demand for medical tests
1.4-	Collect and sample the blood of a patient,
1.5-	Receive the blood sample extracted elsewhere
1.6-	Process and store the blood samples prior to analysis
2-	**Realize the medical tests**
2.1-	*Switch on and calibrate the devices (see Table 2)*
2.2-	Pass a series of tests (technical analysis)
2.3-	Validate the technical tests
2.4-	Maintain the equipments
3-	**Conclude the medical tests**
3.1-	Interpret the biological validation tests
3.2-	Archive the blood samples
3.3-	*Communicate the results (see Table 2)*
3.4-	Archive the results

The activities (sub-processes) consist of tasks. We will detail some activities, that illustrate Stage#2 "Analyzing risks" (see Figure 2).

5.2 Stage #2: Analyzing Risks

Table 2 is a detailed description of three of the sub-processes detailed in the previous section. We will use this description to explain how we have been analyzing risks of usability, privacy and security in the socio-technical system of *FI MedLab*.

Such risks are due to the interdependence between usability and security. Users need to access to information, function of their role and their task. But the modality to access this information depends upon the context of the task (indoor/outdoor, time pressure…), the quality of the security device, its adequacy to the task and its context.

Table 2: Three detailed activities.

1.1-	***Manage the patient file (Create, Update, or Archive)***
	Input : Identity document of patient or his representative
	Output: Updated patient record
	Tasks:
1.1.a-	The patient or his representative indicates the required information to the administrative operator of *FI MedLab*, including address for sending medical analysis results.
1.1.b-	The administrative operator of *FI MedLab* enters information in the *FI MedLab* socio-technical system, for creation and/or update of the patient's record.
1.1.c-	A scheduled event triggers and alerts the administrative operator to archive records of some patients.
1.1.d-	The administrative operator carries out the administrative processing and archives the corresponding patients' records.
2.1-	***Switch on and calibrate the devices***
	Input: Identity document of the manager of technical operators.
	Output: Devices switched on and calibrated for operating medical tests.
	Tasks:
2.1.a-	The manager performs biometric authentication (retinal scan and scan of the identity document).
2.1.b-	The authenticated manager starts and calibrates the devices.
2.1.c-	The devices initialize and load the signatures of the biologists' managers (who interpret the biological validation of tests).
3.3-	***Communicate the results***
	Input : Results validated and interpreted.
	Output: Results communicated by three ways (sent to the physician, sent to the patient by mail, made available on the secure website of FI MeddLab).
	Tasks:
3.3.a-	Administrative operator sends the results to the physician.
3.3.b-	Administrative operator sends the results to the patient address by mail.
3.3.c-	Administrative operator puts the results on the secure website of *FI MedLab*.

As a matter of example, we have investigated more deeply the following scenarios.

Scenario T1: The patient gives his business address. He does not notice that the results of his medical tests will be sent to this address and the administrative operator does not indicate this helpful clarification to the patient. When results reach the patient, he is absent and his assistant handles the mail, like any business mail. This is a serious problem in terms of privacy and confidentiality that we detect during this phase. This scenario deals with the confusion between professional and personal information, within the professional email box. The assistant can open the email box and read the emails in this box, since these emails are supposed to be professional.

Scenario T2: The manager of technical operations faces serious difficulties in being accepted by the biometric authentication system. The camera system is not well positioned for this manager sportsman who measures 1.92m (for information, the average height of his colleagues is 1.76m). The manager is not comfortable in such a situation; he can no longer find his good inclination to be authenticated. In this context, he runs the backup procedure; he logs into the system and activates the devices. The devices are initialized, but do not load the signatures of the biologists' managers (who interpret the biological validation of tests). There is no alert. The manager does not notice the error. We are faced with a problem of usability and ergonomics (first on the internal procedures of the system and secondly, on the communication user interfaces). This problem creates security vulnerability on all the medical tests that will be performed during the day (no traceability and no respect for integrity on the interpretation and validation of medical test results).

The security device does not fit to the task and to the users. The user bypasses the security device, using a backup procedure. Moreover, there is no alarm alerting this barrier bypassing. This kind of behavior deals with barriers bypassing rules, it is a critical security issue.

Scenario T3: The patient is on vacation when medical analysis results are ready. From his vacation

location (Cayman Islands), he decides to access the secure website of *FI MedLab*. He receives a message asking to enter the code that has just been sent to his phone via SMS. This may lead to three problems: a privacy problem (the vacation location could be a "non-public information", but is found out by the web site security system of *FI MedLab*, leading to potential rumor about the reputation of the patient); a trust and confidence problem (one category of patients could say: "*I have too much confidence in the FI MedLab system, as I feel that my data is protected*", another category of patients could say: "*I do not have any trust in the FI MedLab system, I feel spied*"); a problem of comfort and simplicity (due to the additional verification).

This scenario deals with the context of the task, namely, vacation. Moreover, it deals with the low level of the security device that can open to fraudulent access to information with bad consequences such as identity usurpation or blackmail ("I feel spied").

5.3 Stage #3: Developing Solutions

The previous three scenarios describe a user experience; each one of them highlights a usability security or privacy problem.

Scenario T1, for example, details a typical problem of privacy and confidentiality, due to misunderstanding of the use made of the information requested to the user (the patient or responsible). Table 3 details possible solutions of this problem.

Table 3: Design Pattern Solution for Trouble T1.

Name	Awareness
Description of the problem	Misunderstanding and poor knowledge of the use made with the information requested from the user.
Description of the Design Pattern solution	Provide users with the explanation, understanding and analysis of any of the information indicated in the socio-technical system. This will require an individualized support and pedagogy. Operationally, we can put flyers and (interactive) information terminals in the lobby of *FI MedLab*. An alternative solution should be to "send all mail of the results via letters". Another solution consists to add a tag "confidential personal information" in the object of the message, and a note presenting the law inside the text of the message, in order to alert the assistant and "to increase" its awareness.
Consequences	The alternative solution has the direct benefit of avoiding another person in handling mail (recommended letter). But in the era of service industry, of socio-technical systems and of Big Data, the main solution should address the fundamental problem of our time in accompanying users in improving their vigilance skills.

In Scenario T2, it is a more complex problem with several interrelated dimensions: T2.1- Bad usability of the biometric authentication system; T2.2- Non-effectiveness of the emergency procedure; T2.3- Difficulties in understanding the emergency procedure by the manager; T2.4- Detecting barrier bypassing by the manager. Table 4, Table 5, Table 6 and Table 7 describe four possible solutions.

Table 4: Design Pattern Solution for Trouble T2.1.

Name	Anticipation
Description of the problem	Bad usability of biometric authentication system.
Description of the Design Pattern solution	Repositioning the camera and reconfiguring the biometric authentication system to account for all employees of the team. People need to use secure solution, in simple and efficient way.
Consequences	Simple and efficient usage of secure solution is an important step, for ensuring the security in the context of a socio-technical system.

Table 5: Design Pattern Solution for Trouble T2.2.

Design pattern solution for Trouble T2.2	
Name	Regular test of the procedures
Description of the problem	Non-effectiveness of the emergency procedure.
Description of the Design Pattern solution	The repetition frequency of the tests and their results should be integrated into the systems of controlling and auditing.
Consequences	This problem is well-known in safety issues of critical systems. The repetition of exercises develops more confidence of operators, and in case of failure they still trust the procedures. Regularly testing the emergency procedures is a way to improve the user operator experiences.

Table 6: Design Pattern Solution for Trouble T2.3.

Design pattern solution for Trouble T2.3	
Name of the Design Pattern solution	Training of operators
Description of the problem	Lack of mastering the emergency procedure by the manager.
Description of the Design Pattern solution	Training of operators in all the procedures they will face. These training activities should be embedded in the systems of controlling and auditing.
Consequences	This problem is well known in critical systems. Operator training helps improve their user experience.

Table 7: Design Pattern Solution for Trouble T2.4.

Design pattern solution for Trouble T2.4	
Name of the Design Pattern solution	Detection and alert following barrier bypassing
Description of the problem	Due to usability problems, the security device is bypassed, using a backup procedure.
Description of the Design Pattern solution	Usage of security device has to be monitored in order to detect barrier bypassing and to alert the system security administrator. Then, the security administrator can improve security device usability and adapt it to the current usage.
Consequences	This problem is also well-known in critical systems in which such a pattern is suggested.

In Trouble T3, we are faced with three problems again: T3.1- Feeling of privacy problem; T3.2- Feeling of trust and confidence problem; T3.3- Comfort and simplicity problem. The search for improved user experience provides an effective response to all of these three points (Table 7).

Table 8: Design Pattern Solution for Trouble T3.

Design pattern solution for Trouble T3 (T3.1, T3.2, T3.3)	
Name of the Design Pattern solution	Sensitization and pedagogy.
Description of the problem	Eventual stress of the user.
Description of the Design Pattern solution	In the early stages, provide users with the explanation, understanding of the operating of the socio-technical systems.
Consequences	In the era of service industry, personalized monitoring and pedagogy are a good way to improve user experience.

These representative scenarios illustrate that usability problems impact security, and conversely. By identifying business processes, the roles and tasks of users, as well as their needs for private information or, on the opposite, the inability to access to this private information, context of use and other usability issues, we have elaborated design patterns. Such design patterns are the keystone of resilient built-in socio-technical systems, since they integrate security and usability issues together.

6 CONCLUSION AND FUTURE WORK

Various tools have been proposed to provide a more usable interface for a specific security problem or a more easy-to-use security technology. However, there is still a need for engineering approaches to designing and to ensuring security and usability trade-offs. We strive to provide an answer to this lack. We have introduced a socio-technical approach in order to engineer the compromise between security and usability that we considered as a sub-factor of security. The socio-technical system approach connects the system and its services with people, users and stakeholders included. We suggest using BPMN and UML to model and describe the various interactions in socio-technical systems. Such a description is used then to identify possible usability and security problems and their solutions. We propose to use patterns to document these solutions and design resilient built-in socio-technical systems.

One important added value of the proposed socio-technical systems approach is that the humans and their experiences are explicitly considered. This will overcome somehow the lack of training and experience in security, the lack of security in terms of corporate strategy (operations, proceedings) and the difficulties of communicating about security issues.

One of the remaining challenges is to raise awareness and effectively convey a good sense of usability as a security attribute, facilitating a weighted consideration of security in the thoughts, decisions and activities done. We have proposed to address this issue in the future while considering the user experience for all stakeholders of the socio-technical systems (end users, operators, managers, etc.). Patterns will be extended also to integrate explicitly measures of trust, privacy and other subjective criteria measuring user experiences, user feeling.

ACKNOWLEDGEMENTS

The authors thank Prof. Ahmed Seffah (Lappeenranta University of Technology) for his numerous relevant remarks and suggestions on preliminary versions of this paper. They thank also warmly Dr. Jean-René Ruault for his strong contribution to the last versions.

REFERENCES

Alexander, C, Ishikawa, S & Silverstein, M 1977, *'A Pattern Language: Towns, Buildings, Construction'*, Oxford University Press, New-York.

ANSSI, 2014, *'Résilience de l'Internet français'*, Internet resources http://www.ssi.gouv.fr/ [Accessed: 11/11/2015].

Bevan, N 2009, 'Extending quality in use to provide a framework for usability measurement', In *M. Kurosu (ed), Human centered design, HCII 2009*, pp.13–22, Heidelberg, Germany, Springer-Verlag.

Birge, C 2009, 'Enhancing Research into Usable Privacy and Security', SIGDOC 09: *Proceedings of the 27th ACM international conference on Design of communication*, October 2009.

Blakley, B, Heath, C and members of The Open Group Security Forum 2004, 'Security design patterns', Technical Report G031, The Open Group, Apr. 2004. URL http://www.opengroup.org/publications/catalog/g031.htm, [Accessed: 13/11/2015].

Braz, C, Seffah, A, Raihi, DM, 2007, *'Designing a Trade-Off Between Usability and Security: A Metrics Based-Model'*, In Proc. Interact, LNCS 4663, pp. 114–126.

Clarke, N & Furnell, S 2014, *'8th Int'l Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)'*, Nathan Clarke, Steven Furnell (eds), Plymouth, UK, July 8-9, 2014. ISBN: 978-1-84102-375-5.

Cranor, L 2006, 'Usable Privacy and Security', Lorrie Cranor's courses, Internet resources http://cups.cs.cmu.edu/courses/ups-sp06/ [Accessed: 13/11/2015].

Cranor, LF & Blase, U 2015, 'Usable Privacy and Security', Lecturer materials, Courses January 2015, Carnegie Mellon University, CyLab. http://cups.cs.cmu.edu/courses/ups-sp14 [Accessed: 13/11/2015].

Cranor, LF & Garfinkel, S 2005, *'Security and Usability: Designing Secure Systems that People Can Use'*, Ed. O'Reilly, ISBN-13: 978-0596008277.

DCSSI 2009, *'Fiche d'expression rationnelle des objectifs de sécurité'*, http://circulaire.legifrance.gouv.fr/pdf/2009/04/cir_1982.pdf [Accessed: 14/11/2015].

Emery, E 1967, *'The next thirty years: concepts, methods and anticipation'*, Human relations #20, pp. 199-237.

Ferrary, M 2014, *'Management des ressources humaines: Marché du travail et acteurs stratégiques'*, Ed. Dunod, Paris, France, ISBN-13: 978-2100713172.

French penal code 2015, *'De l'atteinte à la vie privée'*, article 226-1, [Accessed: 14/11/2015].

Goudalo, W & Seret, D 2008, 'Towards the Engineering of Security of Information Systems (ESIS): UML and the IS Confidentiality', Proceedings at the *Second International Conference on Emerging Security Information, Systems and Technologies*, pp. 248-256, IEEE Computer Society Washington, DC, USA.

Goudalo, W & Seret, D 2009, *'The Process of Engineering of Security of Information Systems (ESIS): The Formalism of Business Processes'*, SECURWARE 2009, 3rd Int'l Conf on Emerging Security Information, Systems and Technologies, IARIA, pp.105-113.

Goudalo, W 2011, 'Toward Engineering of Security of Information Systems: The Security Acts', *Proc. 5th Int'l Conf. Emerging Security Information, Systems and Technologies, IARIA*, *2011,* pp.44-50.

Hertzum, M, Clemmensen, T, Hornbæk, K, Kumar, J, Qingxin, S & Yammiyavar, P 2007, 'Usability constructs: A cross-cultural study of how users and developers experience their use of information systems', In *Proceedings of HCI International 2007*, pp. 317–326, Beijing, China: Springer-Verlag.

Hollnagel, E, Woods, D, D & Leveson, N 2006, *'Resilience engineering. Concepts and precepts'*, Ashgate, Aldershot.

IBM Corporation 2014, *'Understanding big data so you can act with confidence'*, Doc. Ref. IMM14123USEN, June 2014, http://www-01.ibm.com, [Accessed: 13/11/2015].

ISO 9241-110 2006, *'Ergonomics of human-system interaction'*, Part 110 Dialogue principles.

ISO 9241-12 1998, *'Ergonomic requirements for office work with visual display terminals (VDTs)'*, Part 12 Presentation of information.

ISO/IEC 2700x 2010, *'Information technology Security techniques'*.

KPMG International 2014, *'Managing the data challenge in banking. Why is it so hard?'*, Document published on June 2014, http://www.kpmg.com, [Accessed: 13/11/2015].

Laprie, JC 2008, "From dependability to resilience", dans Proceedings of the 38th Annual *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2008)*, *Supplemental Volume*, Anchorage, USA, june 2008.

Larson, RC 2008, 'Service science: At the intersection of management, social, and engineering sciences', *IBM Systems Journal*, 47, pp.41–51.

Lewis, JR 2014, 'Usability: Lessons Learned … and Yet to Be Learned', *International Journal of Human-Computer Interaction*, 30:9, pp. 663-684.

Luzeaux, D 2011, 'Engineering Large-Scale Complex Systems', In Luzeaux D., Ruault J.-R. & Wippler J.-L. (eds), *Complex Systems and Systems of Systems Engineering*, ISTE-Wiley, London, pp.3-84.

Mahatody, T, Sagar, M & Kolski, C 2010, 'State of the Art on the Cognitive Walkthrough method, its variants and

evolutions', *International Journal of Human-Computer Interaction*, 26 (8), pp.741-785.

Palin, PJ 2013, 'Resilience: Cultivating the virtue', Internet resources http://www.hlswatch.com/2013/08/29/resilience-cultivating-the-virtue/ [Accessed: 11/11/2015].

Piètre-Cambacèdés, L 2010, *'Des relations entre sûreté et sécurité*', Ph.D in Software and Network, Paris.

ReSIST 2015, *'Resilience for Survivability in IST',* A European Network of Excellence, http://www.resist-noe.org, [Accessed: 13/11/2015].

Rousseau, DM, Sitkin,S, B, Burt, R, S & Camerer, C 1998, *'Not So Different After All: A Cross-Discipline View Of Trust*', Academy of Management Review,vol.23 no.3 pp.393-404.

Ruault, J.R, Kolski, C, Vanderhaegen, F & Luzeaux, D, 2015, 'Sûreté et sécurité : différences et complémentarités', Conférence *C&ESAR 2015*, Résilience des systèmes numériques, Rennes, France.

Salloway, A & Trott, J, R 2002, *'Design patterns par la pratique*', Eyrolles, Paris.

Sasse, MA 2007, 'Red-Eye Blink, Bendy Shuffle, and the Yuck Factor: A User Experience of Biometric Airport Systems', *IEEE Security & Privacy, vol. 5*, no. 3, May/June 2007, pp.78-81.

SBIC (Security for Business Innovation Council) 2008, *'The Time is now: making information security strategic to business innovation'*, RSA Security, Bedford MA.

Schneider, FB 1998, *'Trust in Cyberspace'*, Committee on Information Systems Trustworthiness, National Research Council, Washington, D.C.

Schumacher, M 2003, *'Security engineering with patterns: origins, theoretical models, and new applications'*, Springer, 2003, LCNS 2754

Seffah, A, Donyaee, M, Kline, R,B, Padda, H, K 2006, *'Usability measurement and metrics: A consolidated model',* Software Quality Journal, vol. 14, pp.159–178.

Shackel, B 2009, 'Usability—Context, Framework, Definition, Design, and Evaluation', Human Factors for Informatics Usability, B. Shackel and S. Richardson (eds), Cambridge Univ. Press, pp.21–37.

Singh, MP 2013, 'Norms as a basis for governing sociotechnical systems', *ACM Transactions on Intelligent Systems and Technology (TIST) - Special Section on Intelligent Mobile Knowledge Discovery and Management Systems and Special Issue on Social Web Mining archive. Volume 5* Issue 1, December 2013. New York, NY, USA.

Sperber, D, Wilson, D 1995, "Relevance: Communication and Cognition", *2nd Edition, ISBN*: 978-0-631-19878-9, 338 pages, December 1995, Wiley-Blackwell

Trist, EL, Higgin, G,W, Murray, H & Pollock, A,B 1963, 'Organizational Choice: Capabilities of Groups at the Coal Face under Changing Technologies', The Loss, Rediscovery & Transformation of a Work Tradition, Tavistock Publications, London.

Umhoefer, C, Rofé, J & Lemarchand, S 2014, 'Le big data face au défi de la confiance', Document published on June 2014 http://www.bcg.fr, [Accessed: 13/11/2015].

Westin, AF 1968, 'Privacy And Freedom', 25 Wash. & Lee L. Rev. 166, http://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20 [Accessed: 13/11/2015].

Wharton, C, Rieman, J, Lewis, C & Polson, P 1994, 'The cognitive walkthrough method: A practitioner's guide', In J. Nielsen & R. L. Mack (Eds.), *Usability inspection methods*, John Wiley & Sons, New York, pp.105-140.

Winter, S, Wagner, S & Deissenboeck, F 2007, 'A comprehensive model of usability', In *Engineering Interactive Systems,* pp.106–122, Heidelberg, Germany: International Federation for Information Processing.

Yee, KP 2002, 'User Interaction Design for Secure Systems', Proc. *4th Int'l Conf. Information and Communications Security*, Springer-Verlag, 2002, pp. 278–290.