The final publication is available at IEEEXplore via http://dx.doi.org/10.1109/ISSREW.2014.49

Towards Safety Risk Assessment of Socio-technical Systems via Failure Logic Analysis

Barbara Gallina and Edin Sefer
IDT, Mälardalen University,
Västerås, Sweden

Atle Refsdal
SINTEF ICT
Oslo, Norway

***Abstract*— A thorough understanding of the safety risks of a system requires an understanding of its human and organizational factors, as well as its technical components. Analysis approaches that focus only on the latter without considering, for example, how human decision makers may respond to a technical failure, are not able to adequately capture the wide variety of safety risk scenarios that need to be considered. In this paper, we propose a model-based analysis approach that allows analysts to interpret humans and organizations in terms of components and their behavior in terms of failure logic. Our approach builds on top of CHESS-FLA, which is a tool-supported failure logic analysis technique that supports analysis of component-based system architectures to understand what can go wrong at the system level and to identify the causes (i.e. faulty components). However, CHESS-FLA currently deals only with hardware and software components and thus it is not adequate to reason about socio-technical systems. We therefore provide an extension based on a preexisting classification of socio-failures and combine it with the one used in CHESS-FLA for technical failures, thereby giving birth to a novel approach to analysis of socio-technical systems. We demonstrate our approach on an example from the petroleum domain.**

Keywords*— Risk assessment, failure logic analysis, CHESS-FLA, socio-technical systems, human and organizational factors.

I. INTRODUCTION

Identifying the things that may go wrong and the ways in which this may happen is an essential part of risk analysis [1]. Several techniques are at disposal for addressing this [2]. These techniques offer different advantages (e.g. presence of tool-support, focus on linear relationships, focus on both linear and non-linear relationships, focus on technological factors, focus on human factors, etc.), which rarely are combined into a unified technique. In this paper, we propose a novel approach to risk identification aimed at socio-technical systems, with specialized support for classification of human and organizational as well as technical failures.

The approach builds on CHESS-FLA [3], which is a plugin within the CHESS toolset allowing users to decorate component-based architectural models with safety related information (i.e. specification of failure behaviour), execute Failure Logic Analysis (FLA) techniques, and get the analysis results back-propagated onto the original model. CHESS-FLA allows architects and safety engineer to jointly analyse linear relationship-based failure propagation and thus intervene when necessary. Currently, CHESS-FLA only targets architectures composed of hardware and software components.

In the framework of the CONCERTO project [4], we are interested in reasoning about socio-technical systems, where human and organizational factors play an important role. To do that, CHESS-FLA needs to be extended. Besides the two technological (hardware and software components) entities handled by CHESS-FLA, additional entities need to be considered. More precisely, we propose a method called CONCERTO-FLA that permits architects to interpret human and organizations in terms of components and their behavior in terms of failure logic. CONCERTO-FLA includes, as in a concert, more voices: not only technological components but also human and organizational components.

Our proposal builds on top of a pre-existing classification of typical organizational and human failures and combines it with the typical and entity independent failure classification provided in and used in CHESS-FLA.

The contribution of this paper is a novel approach to model-based safety risk identification that

- is specifically aimed at socio-technical systems,
- supports capture of human, organizational and technical components in a common model, thus facilitating unified analysis of complex socio-technical systems,
- builds on existing classifications of human, organizational and technical failures, thereby exploiting existing domain knowledge, and
- facilitates automated analysis of complex failure propagations and transformations, with back-propagation of analysis results to the component model in order to ease understanding of the results.

To show the usage and effectiveness of our method, we then demonstrate it to a simple socio-technical system. More specifically, we introduce essential information to be able to architect parts of an offshore petroleum installation and consider humans, organizations, and technological entities.

Then, based on a hypothetic scenario we perform our analysis and we give our lessons learned.

The rest of the paper is organized as follows. In Section II, we provide essential background information. In Section III we present our method for performing failure logic analysis on

socio-technical systems. In Section IV, we demonstrate our method. In Section V, we discuss our achievements. In Section VI we discuss related work. Finally, in Section VII we present some concluding remarks and future work.

II. BACKGROUND

In this section, we recall some background information onto which our worked is based. More specifically, we briefly recall essential characteristics of socio-technical systems, CHESS-FLA and MTO-oriented risk assessment methods.

A. Socio-technical Systems

Socio (of people and society) and technical (of machines and technology) is combined to give socio-technical. Socio-technical refers to the interrelatedness of 'social' and 'technical' [5]. Successful (or unsuccessful) system performance depends on this interrelatedness, which comprises linear 'cause and effect' relationships, and 'non-linear', complex, even unpredictable relationships.

B. CHESS-FLA

CHESS-FLA [3] is a plugin within the CHESS toolset (developed in the framework of the CHESS project [6]) allowing users to decorate component-based architectural models (specified using the CHESS modeling language, called CHESS-ML) with safety related information, execute Failure Logic Analysis (FLA) techniques (precisely FPTC [7] and FI^{4}FA [8]), and get the analysis results back-propagated onto the original model. FLA can be used at the early stages of the design phase to achieve a robust architecture with respect to linear relationships. CHESS-FLA targets architectures constituted of hardware and software components.

In this paper we limit the attention to FPTC. FPTC (Failure Propagation Transformation Calculus) is a compositional technique to qualitatively assess the dependability/safety of component-based systems. FPTC allows users to calculate the behaviour at system-level, based on the specification of the behaviour related to individual components.

A component can behave as a source (e.g. meaning that a component generates a failure in output due to activation of internal faults) or as a sink (a component is capable of avoiding failure propagation by detecting and correcting the failure in input). Moreover the failures that arrive in a component can propagate (passing on a failure from input to output) and can also be transformed (changing the nature of the failure from one type to another from input to output).

The behaviour of the individual components, established by studying the components in isolation, is expressed by a set of logical expressions (FPTC rules) that relate output failures (occurring on output ports) to combinations of input failures (occurring on input ports). The syntax supported in CHESS-FLA to specify the component's behavior is:

behaviour = expression +
expression = LHS '→' RHS
LHS = portname'.' bL | portname '.' bL (',' portname '.' bL) +
RHS = portname'.' bR | portname '.' bR (',' portname '.' bR) +
failure = 'early'| 'late' | 'commission' | 'omission' | 'valueSubtle' | 'valueCoarse'
bL = 'wildcard' | bR
bR = 'noFailure' | failure |

Thus, an example of a compliant expression is:

C1_R1.noFailure→C1_P1.valueCoarse

The above rule should be read as follows: if the component C1 receives on its port R1 a normal behaviour, it generates on its output port P1 a coarse (i.e. clearly detectable) value failure (a failure that manifests itself with a value failure mode).

From a semantics point of view, the inter-connected components are considered as a token (failure/no-failure)-passing network. To determine the behaviour at system level, it is necessary to consider the set of all possible behaviours (failure and or normal behaviour) that can be propagated along a connection (called tokenset). More specifically, the behavior at system level is obtained through a fixed-point calculation that calculates the maximal tokenset on any connection in the network. Further explanation on FPTC semantics can be found in [7].

FPTC combines and automatize traditional risk identification techniques (i.e., Failure Modes and Effects Analysis, Fault Tree Analysis). Since these techniques are often suggested within safety standards, FPTC represents and interesting means to be considered for the provision of safety certification artefacts.

C. MTO-oriented Risk Assessment Methods

The MTO (Man, Technology and Organization) concept, which originated in Sweden, is similar to the Human Factors (HF) concept developed in the USA [9]. It was the intent that the explicit mention of the three interrelated elements in the concept would stimulate a comprehensive "system view" on safety. Man, Technology and Organization are interrelated and should all be considered in safety assessment. Various MTO-oriented results for supporting risk assessment methods exist. As reviewed in [2], Rasmussen's Socio-Technical Framework is a system-oriented approach that allows modelling the organizational, management and operational structures that create the preconditions for accidents. In Rasmussen's hierarchical model, accidents are caused by decisions and actions made by decision makers at all levels, not only on process control layer. A vertical information cycle in the hierarchy creates the relation between each entity, Organization, Human and Technology.

MTO-oriented failure classifications are used to better classify what can go wrong. HFACS and SERA, for instance, are two MTO-oriented classifications. HFACS (Human Factors Analysis and Classification System) [10] is based on Reason's concept of latent and active failures and embraces all aspects of human failures, including the conditions of operators and organizational failures. According to Reason, an individual fails (produces an active failure/unsafe act) as a consequence of latent failures (seen as preconditions for unsafe acts) that originate from organizational factors. Thus, the investigation of latent failures is crucial to avoid the unfair criminalization of individuals [11]. HFACS describes four levels of failures: 1) *Unsafe Acts*, 2) *Preconditions for Unsafe Acts*, 3) *Unsafe Supervision*, and 4) *Organizational Influences*.

SERA (Systematic Error and Risk Analysis) [12] extends HFACS and provides a set of active failures that human can produce. As HFACS, SERA considers four levels of failures. SERA specializes the level of Unsafe Acts. According to SERA, a human can produce 12 categories of active failures (unsafe acts). These failures may be caused by preconditions, which include: the state of the humans, task and working conditions, command, control, supervision and the organizational influences. In this section, we only recall one category (namely, *attention failure*) and a corresponding precondition (namely, *time pressure*) that we use in Sections III-IV. *Attention failure* means that the required information is available, but a human fails to attend relevant information due to, for example, insufficient time to attend. Fixation on one aspect of the task (selective attention) is also an example of the attention failure. One precondition that may lead to attention failure is the time pressure from the organization. *Time pressure* is related to the tempo of the task and it means that there is no or little time to think and react.

III. TOWARDS CONCERTO-FLA

In this section, we introduce CONCERTO-FLA, which is a novel method for the analysis of failure logics in socio-technical systems. First, we provide an overview of CONCERTO-FLA, then we explain its support for socio-entities. Finally, we explain how socio-behaviour can be interpreted in terms of FPTC.

A. CONCERTO-FLA Overview

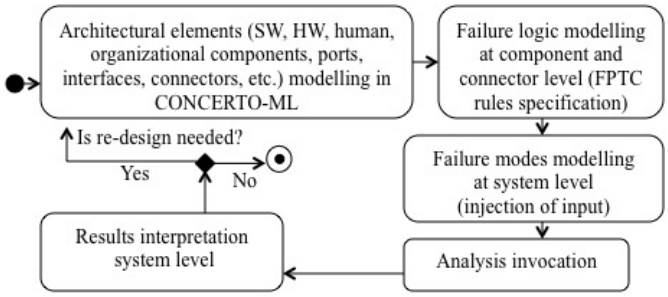

Fig. 1. Activity Diagram Related to CONCERTO-FLA

As the name highlights, CONCERTO-FLA is aimed at harmonizing the co-existence of humans, organizational entities and technological components. To make socio-technical "voices" work in concertation, the complete system, including human and organizational entities, must be properly architected and then analysed with respect to what can go wrong in the case of misbehaving components or connections. Fig.1 shows a high-level view of the overall method we propose to enable architects and safety managers to calculate the failure behaviour at socio-technical system level, based on the failure behaviour specified via FPTC rules at component and connector level.

B. Support for Socio-entities and Corresponding Connections

To enable the modeling of socio-entities, we propose to consider two additional types of component: human and organizational, which in turn can be further specialized according to the SERA preconditions. Thus, our modelling language (called CONCERTO-ML) should have at disposal two additional stereotypes to be able to distinguish the different voices that participate in the architectural concertation. More precisely, human and organizational components should be represented as composite components. The motivation for this choice stems from the SERA classification. By inspecting thoroughly the twelve categories of human failures (e.g. attention failure), we realized that these failures are related to two types of human functionalities: internal functionalities responsible of sensing, perceiving, deciding, etc. and functionalities responsible of acting. Thus, we propose to model human beings as composite components comprising their inter-related internal functionalities (e.g. sensor-like) and actuator-like functionalities (atomic components). As a simple initial proposal, each of the twelve SERA categories of human failures can be represented as an internal component, named accordingly to the category (e.g., *attention* is the name of an internal component accordingly to the category *attention failure*). In our proposal, based on SERA, these components affect an action-related component, that we call *Action*. Input ports of the human composite component should be connected to the appropriate input port of the logical (or sensor-like) component, and the output of the action-related component should be connected to the output port of the human component. Several logical components can be connected to the action-related component, and only one action-related component should be allowed for one human component. Similarly to what we observed for the human categories, when we inspected thoroughly the preconditions of the human failures, we realized that these preconditions could be modeled as a composite component representing globally organizational factors and specializations of these factors (preconditions) can be modeled as interconnected subcomponents (atomic or composite). In our extended architectural model, organizational composite components should be connected to human composite components using appropriate ports to capture organizational influences on human behavior. Human composite components are then connected to technical (composite) components.

C. Interpretation of Socio-behaviour in Terms of FPTC

The previous subsection proposed a possible evolution of CHESS-ML towards CONCERTO-ML. This evolution enables architects to model socio-technical architectures. In order to facilitate analysis, we need to decorate the architectural elements (components and connectors) with safety-related information concerning the nominal/failure behavior according to FPTC syntactical rules. To do that the language constructs [3] that are at disposal for decorating SW and HW components should be available also for human and organizational composite components and related sub-components. These language constructs should also be at disposal for decorating connectors since, as stated in [2], accidents in complex systems do not simply occur due to independent component failures; rather they occur when external disturbances or dysfunctional interactions among system components are not adequately handled. Moreover, at the instance level, it should be possible not only to inherit the FPTC rules, but also to refine them, if needed since the risk identification should be analysed for the specific installation and not at type level in a generic way [13].

By thoroughly inspecting the human failures and their preconditions, we realized that the twelve categories of human failures and corresponding preconditions identified by SERA do not specify in which way these failures/preconditions could manifest themselves. We therefore propose to characterize the human/organizational failures in terms of the failure modes proposed in [14] and then extended in [15].

As result, an incidence matrix can be drawn to synthesize the possible combinations of failure modes with respect to the propagation flow from organizational sub-components to human-related subcomponents. The filled-in incidence matrix could represent generic as well as domain-specific possible propagation flows of failure-modes and thus can guide system designer in modeling a system. Table 1 shows a simplified example of such an incidence matrix, where gray cells denote valid propagation flows from organizational failures to human failures. From Table 1, bottom-left gray cell, we can retrieve that if an internal organizational component related to time pressure produces a valueCoarse, that failure can be stopped by the human attention-related internal component.

Table 1 Matrix Relating Socio-behaviour in FPTC-terms

			Organization		
			Time Pressure		
		FPTC failure	valueCoarse	valueSubtle	noFailure
Human	Attention	omission			
		noFailure			

IV. Applying CONCERTO-FLA

In this section, we apply CONCERTO-FLA on a petroleum domain-related socio-technical system. Thus, first we provide a description of our system, then we follow the process depicted in Fig.1 i.e. we model in CONCERTO-ML our system, we decorate it with safety information and finally we manually perform FPTC analysis.

A. Petroleum Domain-related System

Offshore petroleum installations (called rigs) are complex socio-technical systems that involve several major hazards to health, safety, and the environment [16]. In this section, we present (as done in [17]) a simplified subsystem that will be used to illustrate our modelling and analysis approach. This subsystem concerns work permits and is part of an overall barrier function to prevent safety incidents such as ignition of hydrocarbons.

Workers that need to do non-routine work on the rig, including hot work such as welding, have to apply for a work permit (WP) by filling out a standardized form. The purpose is to avoid potential conflicts between tasks that may represent increased risk, to ensure that potentially risky work is not initiated unless all safety barriers are in good shape, and to ensure that safety precautions are followed. Every 12th hour, decision makers go through all incoming WP applications and decide which ones to release (i.e. accept) or reject. The time slot for this meeting is fixed and the number of applications can be high, meaning that the decision makers may have very little time for each decision.

A database stores information about all deviations related to safety on the rig. This includes, for example, information about errors that have been detected on components but not yet fixed, components that are overdue for periodic maintenance, and so on. A database administrator is responsible for ensuring that the information in the database is up-to-date and correctly reflects the current state of the rig. Information from the database must be "pulled" by those who need it when they need it on their own initiative.

We now consider a hypothetic scenario where the gas detectors in an area on the rig (area A) are unreliable due to being long overdue for maintenance. A worker applies for a WP for performing hot work, such as welding, in area A. Hot work may lead to ignition if there is gas present and should not be allowed unless the gas detectors are known to be in a good state. Hence, a decision to release the WP would be considered a failure. In the following we demonstrate our analysis approach by considering two scenarios where major contributing factors to such a failure are 1) the decision makers failing to check the current state of the gas detection, and 2) the deviations database not correctly reflecting the actual state of the gas detection.

B. Modeling

To model the socio-technical subsystem described in Section IV-A, we first identify the (composite) components and how they are interconnected. Fig.2 shows how this simple subsystem, called WP_Decision_System, can be modelled in CONCERTO-ML.

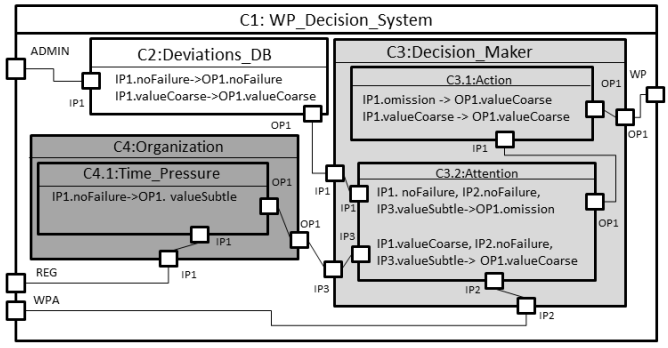

Fig. 2. CONCERTO-FLA architectural model

Identified components of WP_Decision_System are: a composite component (in light gray) to represent the human (named Decision_maker); a technological component to represent the database (named Deviations_DB); and a composite component (in dark gray) to represent the organization (Organization). Decision_maker is composed of two subcomponents: Attention (sensory-like component) and Action (Action-like component). For sake of simplicity, Organization is only composed of one subcomponent: Time_Pressure. Decision_maker is connected to the database (since he/she relies on data coming from it) and to the organization, which establishes the Decision_maker's working pace via Time_Pressure.

As Fig.2 shows, WP_Decision_System is represented as a composite component with three input ports: WPA (which

stands for Work Permit Application), ADMIN (which denotes the connection with database administrator) and REG (which represents potential influence from regulation authorities on the organization). WP_Decision_System is modelled with one output port named WP, which denotes the decision for the work permit. After having studied the behaviour of each component in isolation or after having performed a speculative brainstorming analysis on its potential behaviour, a set of FPTC rules can be provided to specify such behaviour. For space reasons, in Fig.2, each component is characterized by only two rules. The rules that characterize Decision_maker partially stem from the incidence matrix introduced in Section III-C. Since the time pressure on the human can cause the attention failure, the attention component will produce an omission. Concerning Deviations_DB, we assume that it behaves as a propagator.

C. Analysis

In this section, we illustrate how the behaviour at system level can be calculated based on the behaviour of individual components. To do that, we consider two scenarios.

Scenario 1, represented in Fig. 2, describes the case when Decision_maker fails to check the current state of the gas detection. To better follow the failure propagation, under the assumption that the system is fed by normal behaviour (i.e., database administrator enters correct data; there is no regulation pressure on the organization and there is no failure in the work permit application), Fig. 3 shows underlined transformation rules, which are those rules that are activated. The FPTC rule of the Time_Pressure component is activated and produces valueSubtle at the output port, reflecting time pressure originating from the organization. NoFailure on the ADMIN port will be propagated through the Deviations_DB component to the Decision_Maker component. NoFailure from Deviations_DB and valueSubtle from Time_Pressure are then forwarded to the Decision_Maker composite and to its Attention subcomponent. These two in combination with noFailure from WPA port will trigger first propagation rule that produces an omission on the Attention output port. This rule represents the situation in which Decision_Maker omits to attend deviations from the database. The Omission failure from the Attention component is forwarded to the input port of the Action component, and triggers the first rule. As a consequence of the omission, Decision_Maker takes a wrong decision by approving a work permit for hot work in an area where gas detectors may be unreliable. This wrong decision is represented by valueCoarse as output of Action as well as output of the system composite on the WP port.

Scenario 2 describes the case when the database is not correctly reflecting the actual state of the gas detection. In this scenario, the system has: noFailure on the WPA port and the REG port, and valueCoarse at the ADMIN port. As in scenario 1, noFailure on the REG port propagates to valueSubtle on the Organization output port. ValueCoarse from the ADMIN port propagates through Deviations_DB to Decision_Maker, activating the second rule of Attention. By receiving valueCoarse from the Deviations_DB, valueSubtle from the Time_Pressure, and noFailure from the WPA, the Attention component produces valueCoarse on its output port. The Action component propagates valueCoarse to the WP port, as in Scenario 1.

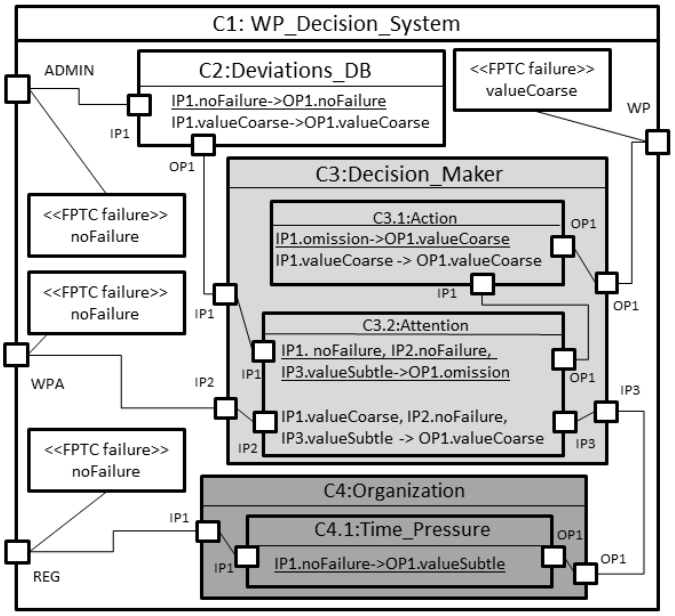

Fig. 3. Scenario 1: CONCERTO-FLA analysis results

V. Discussion

In this section, we present the lessons learned that we have derived by manually applying CONCERTO-FLA to a simplified socio-technical sub-system. The lessons concern the following main bolded aspects**. Socio-technical concepts coverage-** From a coverage point of view, CONCERTO-FLA allows architects and safety managers to model all socio technical concepts that might be of interest to perform a detailed identification of risk within socio-technical systems and thus reconsider design decisions if needed. By using composite components to model humans as well as organizations, architects and safety managers have at disposal a means to reveal all the facets in terms of functional units that may play a role. **Analyzability of the spectrum of socio-technical behavior-** By combining SERA and CHESS-FLA, CONCERTO-FLA offers a powerful means for analyzing the entire spectrum of socio-technical behavior. Socio and technical failures can be analysed in a fine-grained way by considering essential failure modes and thus specific-countermeasures can be introduced if needed. **Scalability-** From a scalability point of view, CONCERTO-FLA is rather powerful. Hierarchical architectures, for instance, can be analyzed by applying “divide and conquer” strategy (i.e., by analyzing level after level the entire system). Similarly complex flat architectural models can be divided in various pieces and conquered piece after piece. **Analyzability of interactions between human, organizational and technical factors that may lead to failures**- CONCERTO-FLA allows linear interactions to be analysed. Moreover, by allowing for modeling the behavior of connectors, it also enables the detections of unintended connections.

VI. Related Work

In the past three decades, several research works on risk assessment techniques have been proposed. Early approaches were targeting single components in isolation, while, together with the growth of the system complexity, more recent approaches have targeted the complete system behavior.

In [18], authors propose a new technique called System-Theoretic Process Analysis that allows losses arising from component (technical, or socio) interactions to be captured. The system is seen as a set of control and feedback loops which interact with each other. Within CONCERTO-FLA, systems are not modeled in the same way. However, our proposal allows linear component interactions to be captured.

In [19], authors criticize the feasibility of Human Reliability Analysis (HRA) by pointing out that human and technological functions cannot be decomposed in the same manner. To limit uncertainty, authors state that a small number of subcomponents should be used to interpret a human as a composite. Our decomposition is currently coarse-grained. The trade-off in terms of granularity will depend on the stage of application of CONCERTO-FLA i.e. speculative vs. empirically grounded FPTC rules.

In [20] authors propose some perspectives and a possible research agenda to achieve a Safety Management System (SMS)-oriented approach combined with human factors to understand and control the overall system safety. Our approach is not SMS-oriented in itself, however it is supposed to be deployed within an SMS.

VII. Conclusion and Future Work

In this paper, we have introduced a novel model-based approach to perform failure logic analysis on socio-technical systems. Our approach, which is built on top of CHESS-FLA and SERA, supports architects and safety engineers in manually analyzing the failure propagation within systems constituted of not only hardware and software components but also organizational and human components.

In the future, we aim to validate the approach through application on more complex systems/scenarios. A major challenge will be to develop a comprehensive SERA-based failure types matrix and to provide detailed guidelines to support architect and safety managers in modeling (pre-analysis) as well as in taking appropriate design decisions (post-analysis), based on the analysis results. We also aim at implementing our approach within the in progress CONCERTO toolset to offer automatic failure propagation analysis.

Acknowledgment

This work has been partially supported by the CONCERTO project [4], and by the Norwegian part of CONCERTO funded by the Research Council of Norway (232059).

References

[1] AS/NZS ISO 31000:2009 Risk management-Principles and guidelines.

[2] Z. H. Qureshi. A Review of Accident Modelling Approaches for Complex Socio-Technical Systems. in Twelfth Australian Conference on Safety-Related Programmable Systems (SCS), Adelaide, Australia, 2007.

[3] B. Gallina, M.A. Javed, F.U. Muram, S. Punnekkat. A Model-Driven Dependability Analysis Method for Component-Based Architectures, Software Engineering and Advanced Applications (SEAA), 38th EUROMICRO Conference, pp.233-240, 5-8 Sept. 2012.

[4] ARTEMIS-JU CONCERTO - Guaranteed Component Assembly with Round Trip Analysis for Energy Efficient High-integrity Multi-core systems. http://www.concerto-project.org

[5] G. Walker, N. Stanton, P. Salmon and D. Jenkins. A Review of Sociotechnical Systems Theory: A Classic Concept for New Command and Control Paradigms, Human Factors Integration Defence Technology Centre, U.K. Ministry of Defence Scientific Research Programme, HFIDTC/2/WP1.1.1/2, 2007.

[6] ARTEMIS-JU-100022 CHESS- Composition with guarantees for High-integrity Embedded Software components assembly.

[7] M. Wallace. Modular architectural representation and analysis of fault propagation and transformation, vol. 141, no. 3, pp. 53–71, 2005.

[8] B. Gallina, S. Punnekkat. FI4FA: A Formalism for Incompletion, Inconsistency, Interference and Impermanence Failures' Analysis, Software Engineering and Advanced Applications (SEAA), 37th EUROMICRO Conference, pp.493-500, 30 Aug. 2011- 2 Sept. 2011.

[9] O. Andersson and C. Rollenhagen. The MTO Concept and Organisational Learning at Forsmark NPP, Sweden, in IAEA International Conference on Safety Culture in Nuclear Installations, Rio de Janeiro, Brazil, 2002.

[10] S. A. Shappell, and D. A. Wiegmann. The Human Factors Analysis and Classification System-HFACS. Office of Aviation Medicine, Washington, DOT/FAA/AM-00/7, Feb. 2000.

[11] S. W. A. Dekker. When human error becomes a crime. Human Factors and Aerospace Safety, 3(1), 83-92, 2003.

[12] K. C. Hendy. A tool for Human Factors Accident Investigation, Classification and Risk Management. Defence R&D Canada, Toronto, DRDC Toronto TR 2002-057, March 2003.

[13] HSE Information sheet. Guidance on Risk Assessment for Offshore Installations, Offshore Information Sheet No. 3/2006.

[14] A. Avizienis, J.C. Laprie, B. Randell, C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. In: IEEE Trans. Dependable Sec. Comput. 1(1): 11-33, 2004.

[15] J. A. McDermid, M. Nicholson, D. J. Pumfrey, and P. Fenelon. Experience with the application of HAZOP to computer-based systems. Proc. of the 10th Annual Conference on Computer Assurance, Gaithersburg, MD, pp. 37-48, IEEE, 1995.

[16] A.B. Skjerve. The use of mindful safety practices at Norwegian petroleum installations, Safety Science, vol. 46, no. 6, pp. 1002-1015, July 2008

[17] A. Refsdal, Ø. Rideng, B. Solhaug, and K. Stølen. Divide and Conquer-Towards a Notion of Risk Model Encapsulation. In Engineering Secure Future Internet Services, Vol. 8431, London: Springer, 2014.

[18] T. Ishimatsu, N. G. Leveson, J. P. Thomas, C. H. Fleming, M. Katahira, Y. Miyamoto, R. Ujiie, H. Nakao, and N. Hoshino. Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis. Journal of Spacecraft and Rockets, Vol. 51, No. 2, pp. 509-522, 2014.

[19] E. Hollnagel. Human reliability assessment in context. Nuclear Engineering and Technology; v. 37(2), Issue 24; ISSN 1738-5733; p. 159-166; Apr 2005.

[20] C. Lowe. A Human Factors Perspective on Safety Management Systems. In “Improvements in System Safety”,Ed. F. Redmill and T. Anderson, pp. 139-153,Springer London, 2008.