Extending SafeConcert for Modelling Augmented Reality-equipped Socio-technical Systems*

Soheila Sheikh Bahaei, Barbara Gallina
School of Innovation, Design and Engineering
Mälardalen University
Västerås, Sweden
soheila.sheikhbahaei, barbara.gallina@mdh.se

***Abstract*—With the emergence of new technologies such as augmented reality in socio-technical systems, traditional risk assessment methods may fail to have a comprehensive system modeling, because these technologies extend human's capabilities, which might introduce new types of human failures caused by failing these extended capabilities and new types of faults leading to human failures. Current state-of-the-art modeling techniques do not contemplate these capabilities and augmented reality-caused faults leading to human failures. In our previous work, we proposed an extension for modeling safety-critical socio-technical systems, to model augmented reality-extended humans by using a taxonomy that contains AR-specific human's failure behavior. In this paper, we continue our extension by investigating faults leading to human failures including faults because of augmented reality. Our extension builds on top of a metamodel for modeling socio-technical component-based systems, named SafeConcert. We illustrate our extension on two fictitious but credible systems taken from air traffic control and rail industry. In order to model augmented reality-equipped socio-technical systems, we need to consider human and organization as parts of the system and augmented reality as a technology used in the system.**

***Index Terms*—augmented reality, immersive visual technology, socio-technical systems, safety-criticality, risk assessment, safety modeling.**

I. Introduction

Augmented reality (AR) can enhance humans' capabilities to see, hear, probably touch, smell and taste more than other humans [1], thus it provides the possibility to have AR-extended humans. In visual augmented reality, computer-generated suitable pieces of information are superimposed on the real world view of the user [2]. For example, using navigation metaphors of landmarks and routes in augmented reality mobile systems can improve human wayfinding and human will have an extended capability that was absent before using this technology [3]. Based on the experiment conducted in [4], context-adaptive augmented reality enhances air traffic controllers' performance and provides new opportunities for air traffic management [4].

New technologies improve human performance, meanwhile they might introduce new failures and faults to socio-technical systems, which should be considered during risk assessment. Throughout this paper, we consider a human as a component in a component-based architecture. Based on Avizienis et al. [5] terminology, human failure is deviation in human functioning and fault is the cause of the human failure. Failure might act as fault in a subsequent component. Faults leading to human failures can be external, if they emanate from subcomponents of other components, or internal, if they emanate from other subcomponents of human component itself. An experiment conducted in [6], shows that presence of augmented cueing aid for expected target detection on the display may distract the viewer from the presence of unexpected targets in the environment and leads to human failures. Another experiment conducted in [7], indicates that augmented reality information on the head up display (HUD) with less than 8 deg (angular degree) from information in the real world would cause cognitive tunneling. Cognitive tunneling means locked attention on AR information and neglecting the real world, which would lead to human failure.

To do risk assessment in the presence of augmented reality, the first step is identification of what can go wrong while there is augmented reality and how it would effect on modeling techniques used for risk analysis. Currently, there are different modeling languages for safety-critical socio-technical systems. However, there is no detailed investigation of the effect of new technologies such as augmented reality. Consequently, the concept is not considered in modeling of new faults leading to human failures that would be introduced to the system while using these technologies. Human failures and faults classification in SafeConcert metamodel is based on SERA (Systematic Error and Risk Analysis) [8] taxonomy. In [9], we proposed AREXTax, which is an AR-extended human function taxonomy by considering state-of-the-art failure taxonomies and AR-extended human functions. In [10], we incorporated this taxonomy while performing a first step towards a substantial extension of SafeConcert human modeling elements used in risk analysis tools, to enable modeling of AR-extended human capabilities. In [11], we proposed AREFTax, a taxonomy of faults leading to human failures, which contains AR-caused faults leading to human failures. In this paper, we extend SafeConcert metamodel to provide the ability of modeling faults leading to human failures including AR-caused faults to empower this metamodel for risk assessment in AR-equipped socio-technical systems. Our extension consists of extension in human modeling elements and extension in organization

This work is funded by EU H2020 MSC-ITN grant agreement No 764951.

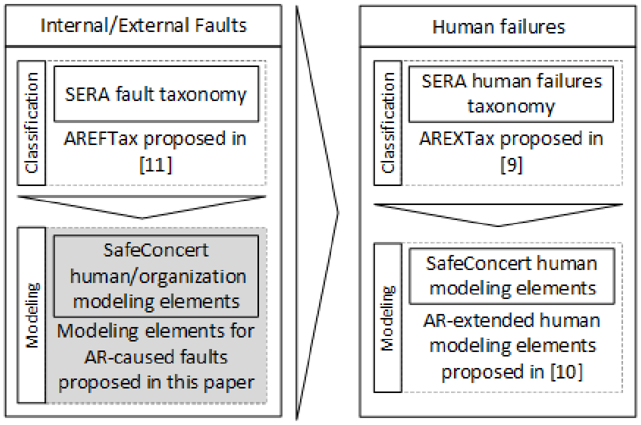

Fig. 1. Contribution of this paper.

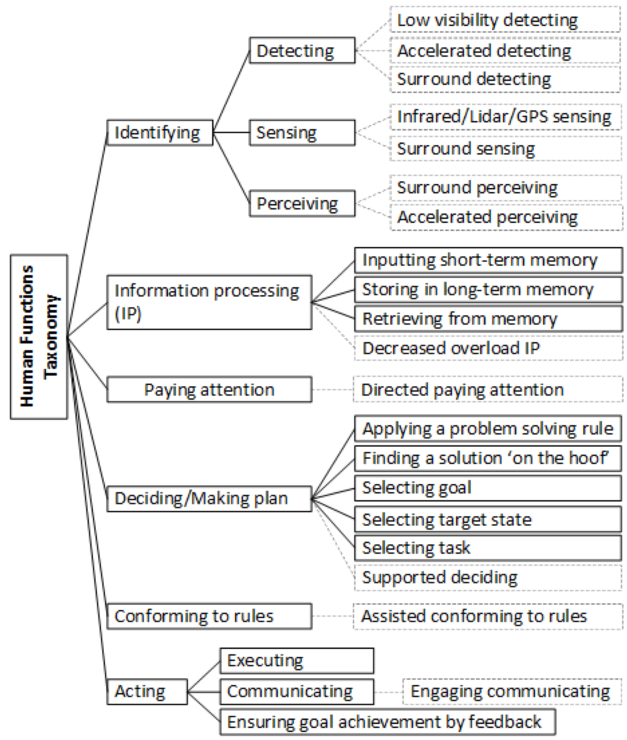

Fig. 2. Function classification of AR-extended humans adapted from [9].

modeling elements. To clarify the contribution of this paper, the extension made in this paper is shown by gray color in Fig. 1. In addition, we show our extension on two fictitious but credible systems within aerodrome control environment and train driving context.

The rest of the paper is organized as follows. In Section II, we provide essential background information. In Section III, we propose our extension on SafeConcert metamodel, based on a taxonomy of faults leading to human failures including AR-caused faults. In Section IV, we model two AR-equipped socio-technical systems from air traffic control and rail industry using the extended metamodel. In Section V, we discuss about the strengths and limitations of the proposed extension. In Section VI, we provide related works. Finally, in Section VII, we present some concluding remarks and discuss about future work.

II. Background

In this section, we provide the background information about AREXTax on augmented reality-extended humans, AREFTax on faults leading to human failures, SafeConcert and its implementation and extended SafeConcert.

A. AREXTax on Augmented Reality-extended Humans

In [9], we proposed a taxonomy of human functions based on state-of-the-art human failure taxonomies and by considering effect of augmented reality and we called it AREXTax. Our taxonomy, presented as a feature diagram, synthesizes the historical evolution of the previously proposed taxonomies (Norman [12], Reason [13], Rasmussen [14], HFACS (Human Factor Analysis and Classification System) [15], SERA [8] and Driving [16] human failure taxonomies) and it also considers AR-specific characteristics. More specifically, we extended the taxonomy for socio-technical systems containing visual augmented reality-extended humans.

Based on this taxonomy, we have a list of human functions that is extracted from the above-listed failure taxonomies. For example *paying attention* function is extracted from *attention failure*. The list of human functions is shown in Fig. 2 and functions characterizing AR-extended humans are shown by dotted border, which are extracted from studies and experiments on augmented reality. For example, if AR information is shown on the windshield of a car, it helps the driver to detect the presence of a person in blind spots [17]. Thus, *surround detecting* can be considered as an extended function. These functions can be considered as subcomponents within the composite component representing the human in socio-technical systems.

B. AREFTax on Faults Leading to Human Failures

In [11], we proposed a taxonomy of faults leading to human failures based on state-of-the-art taxonomies. In addition to the faults extracted from previous taxonomies including Rasmussen [14], HFACS [15], SERA [8], Driving [16] and SPAR-H (Standardized Plant Analysis Risk Human Reliability Analysis) [18], we added faults stemmed from AR, based on related studies and experiments to have a comprehensive taxonomy useful for AR-equipped socio-technical systems. This taxonomy, which is called AREFTax, is shown in Fig. 3. For example, social faults (problems in communicating with others) are personnel faults, categorized based on state-of-art taxonomies, which might lead to human failures. Using augmented reality may decrease social presence and a new type of fault (social presence fault) may lead to human failures [19]. Thus we added this new type of fault as AR-caused fault (shown by dotted border) to the taxonomy.

C. SafeConcert and Its Implementation

SafeConcert [20] is a metamodel that facilitates unified analysis of interdependencies between socio and technical

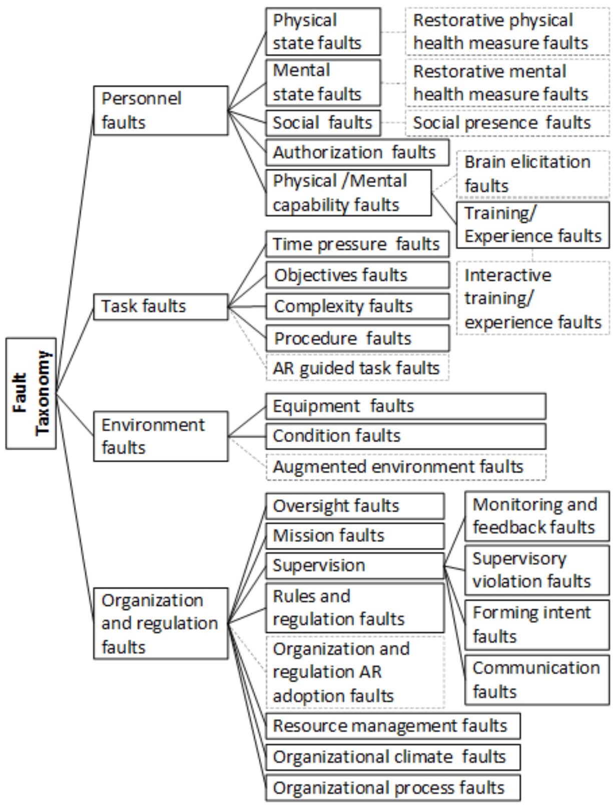

Fig. 3. Classification of faults leading to human failures adapted from [11].

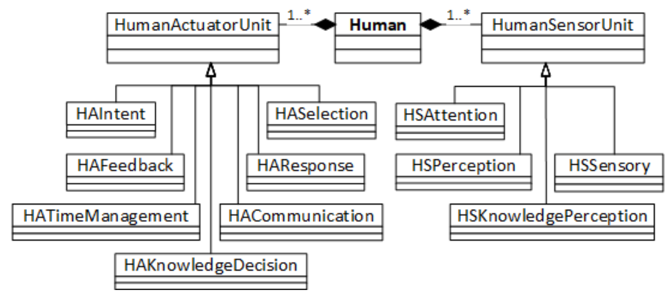

Fig. 4. SafeConcert modeling elements to model human components [20].

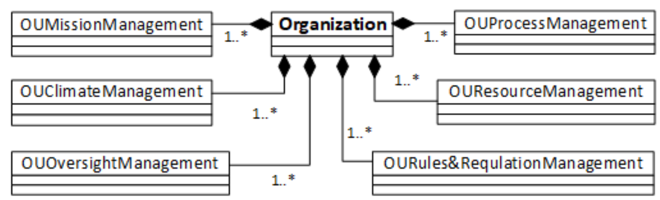

Fig. 5. SafeConcert modeling elements to model organization components adapted from [20].

entities, because it offers constructs for modeling both of them in a common model. This metamodel is a subset of CHESS ML (CHESS Modeling Language) [21], which is a UML (Unified Modeling Language)-based modeling language.

In SafeConcert metamodel, socio-technical systems can be modelled as component-based systems, where components can be software, hardware or socio entities. For socio components, which can be human or organization, the metamodel is based on SERA [8] taxonomy.

Human components are represented as composite components and subcomponents are twelve categories of human failures in SERA taxonomy. These twelve categories are divided into two types based on human functionalities (Fig. 4). Functionalities responsible for acting (HumanActuatorUnit), with prefix ”HA”, including: *selection*, *response*, *knowledge decision*, *time management*, *communication*, *intent* and *feedback* and functionalities responsible for sensing (HumanSensorUnit), with prefix ”HS”, including: *perception*, *attention*, *sensory* and *knowledge perception*.

Organization components are represented as composite components and subcomponents are six categories based on SERA taxonomy (Fig. 5). These subcomponents which are called units in this metamodel are named with prefix ”OU” to represent organizational unit.

Based on SafeConcert metamodel failures are propagated from/to entities in a socio-technical system through ports and failure modes are associated to ports. Failure modes are assigned to ports by defining failure mode groups and based on domain [20].

SafeConcert is implemented in CHESS toolset [22] developed within CHESS [23] and Concerto [24] projects. This toolset offers modelling and analysis capabilities targeting high integrity systems as well as socio-technical systems. Socio entities modeling elements, which are human and organization modeling elements are based on SERA classification in this toolset. Users can define component-based architectural models composed of hardware, software, human and organization and for each component, FPTC (Failure Propagation Transformation Calculus) [25] rules (logical expressions that relate output failures to input failures) are used to model component's failure behavior. This toolset supports SafeConcert metamodel and can be extended based on the extensions provided for SafeConcert.

D. Extended SafeConcert

Based on the function classification of AR-extended humans [9], shown in Fig. 2, we extended the human modeling elements for AR-extended human capabilities' [10]. As it is shown in Fig. 2, there are six categories of human functions that can be divided to three types of human functionalities: functions for gaining situational awareness (SA) containing *identifying* and *paying attention*, functions for *information processing* and *deciding* and functions for *acting* and *conforming to rules*. We show these three categories by *HumanSAUnit*, *HumanProcessUnit* and *HumanActuatorUnit*. Extended human modeling elements are shown in Fig. 6. Modeling elements that are the same as SafeConcert are shown with gray color and extended elements are shown with white color. Modeling elements characterizing AR-extended human functions are shown by dotted line border.

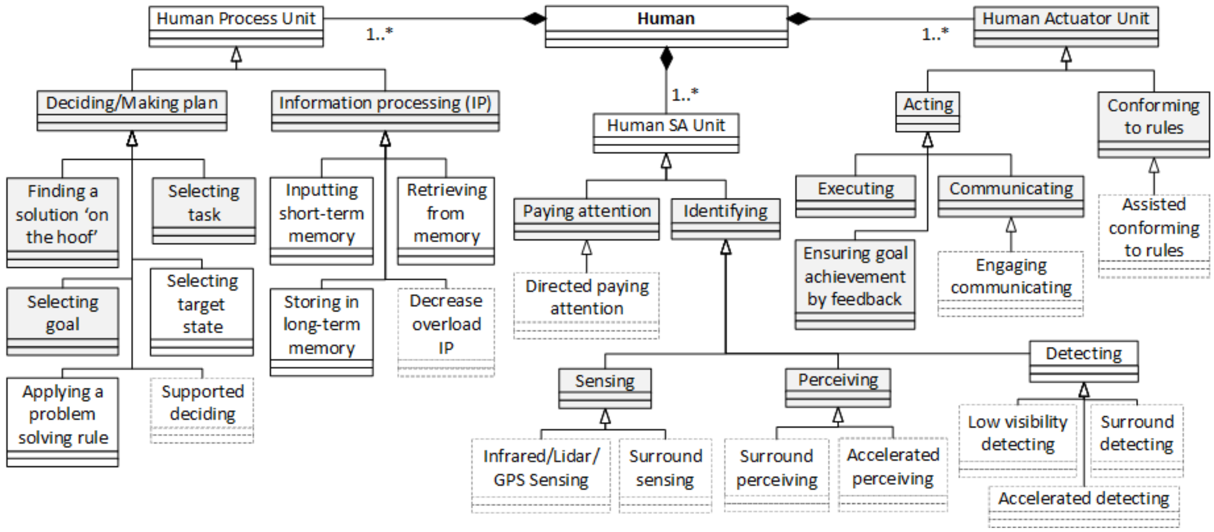

Fig. 6. Proposed model elements to model human components [10].

III. Extending SafeConcert

In this section, we extend SafeConcert with the aim of enabling modeling of possible faults leading to human failures including AR-stemmed faults. Some of these faults emanate from human subcomponents, which needs extension in human modeling elements and other faults emanate from organization subcomponents, which needs extension in organization modeling elements.

A. Extending SafeConcert Human Modeling Elements

In this subsection, we extend the human modeling elements by considering human internal faults leading to human failures. To do that, we incorporate the personnel faults in fault taxonomy shown in Fig. 3 in human modeling elements. The result of the extension is shown in Fig. 7. Extended modeling elements are shown with white color and AR-stemmed modeling elements are shown with dotted line border. For example, interactive training is provided by using augmented reality [26]. If there is problem in AR, this would cause failure in interactive training subcomponent, which is an internal fault for human function subcomponent and causes human failure.

B. Extending SafeConcert Organization Modeling Elements

In this subsection, we extend organization modeling elements by considering organization, task and environment faults leading to human failures. To do that, we incorporate the organization, task and environment faults in fault taxonomy shown in Fig. 3 in organization modeling elements. The result of the extension is shown in Fig. 8. Extended modeling elements are shown with white color and AR-stemmed modeling elements are shown with dotted line border. For example, task procedure and environment conditions are provided by organization and their faults should be detected and corrected by organization, otherwise these faults may lead to human failures.

As it is shown in Fig. 8, elements related to task and environment were not available in SafeConcert. Thus faults related to these categories could not be modelled either.

IV. AR-equipped Socio-technical System Modeling

In this section, we use our extended SafeConcert to model two fictitious but credible AR-equipped socio-technical systems. The first system is AR-equipped assisted tower controlling system and the second system is AR-equipped signal passing at danger system.

A. AR-equipped Assisted Tower Controlling System Modeling

Since head down times for tower controllers could lead to catastrophic consequences, an AR tower controller assistance system is helpful for air traffic controllers (ATCOs) to provide useful information regarding air traffic and flight data projected in the front view of the aerodrome controller [4]. Development of AR displays have been taken into advisement by U.S air force to improve performance and situational awareness of ATCOs. ATCOs' duties are controlling ground traffic and air traffic within the airport traffic control area. They obtain information by observing front view through the window and using displays, patterns and other controllers. AR displays are beneficial to prevent diverting attention from front view, which is the most important source of information [27].

Within the AdCoSCo project in DLR institute, adaptive information management is combined with augmented reality to decrease information overload [4]. AR tower controller assistance system contains three main parts: context-adaptive information presentation, management of integrated information and display using augmented reality. Inputs of assistance system are from sensors and information systems. Data sources such as operator input, environment data, flight plan data and surveillance data from aerodrome surveillance ground radar are used for context-based adaptation [4].

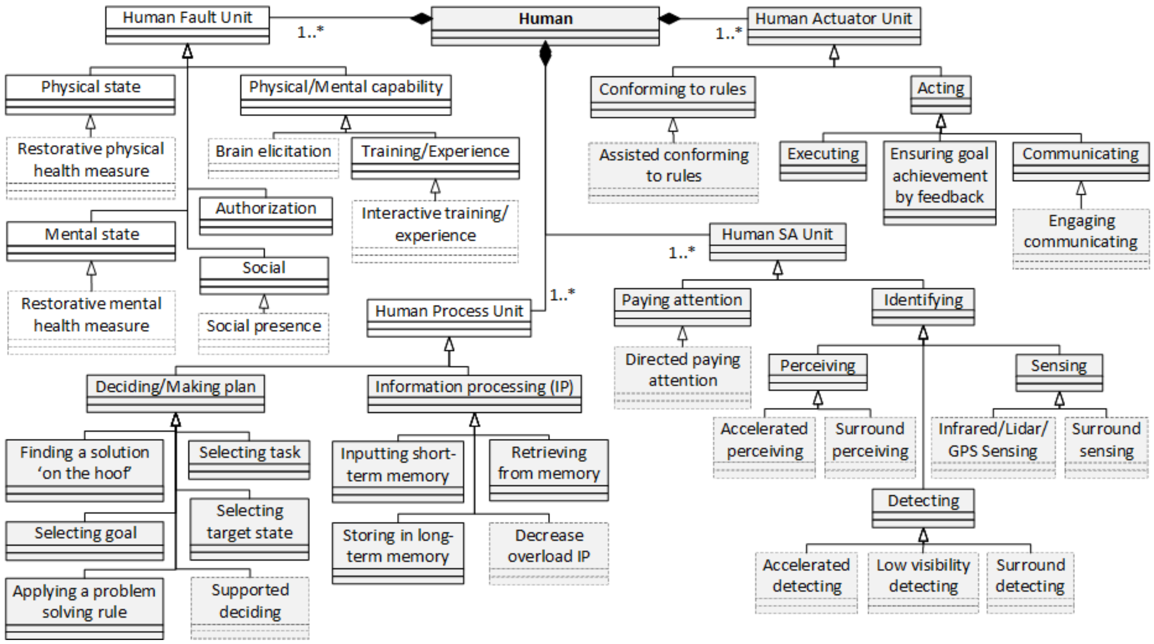

Fig. 7. Extended model elements to model human components.

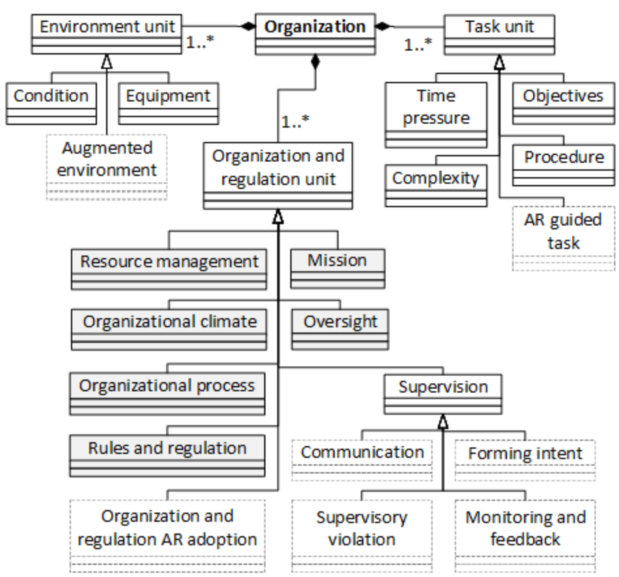

Fig. 8. Extended model elements to model organization components.

If we consider a component-based architecture, AR tower controller assistance system, is a composite component including context-adaptive system, information management and AR display subcomponents.

A human, which is ATCO in this system is a composite component including subcomponents from AR-extended human modeling elements. Each of the model elements in Fig. 7, can be represented as a subcomponent. We consider physical/mental capability, deciding and acting for this system.

Civil aviation organization can be considered as organization composite component with AR adoption subcomponent. We consider AR adoption subcomponent to show the possibility of modeling AR-stemmed faults in organization.

This hypothesised model is shown in Fig. 9. The CHESS toolset can be used to analyze the system, by defining FPTC rules. Rules are defined based on component functions and error model of them. For example, if the probability of generating failure in a subcomponent is less than a threshold and based on the related standard this failure probability is accepted, then we can assume this component will not generate fault and it may transfer the fault from input to output, or it may detect the fault in input by fault detection techniques and prevent its propagation. Thus, defining these rules depends on each subcomponent and should be done by safety analyzer.

We assume three scenarios to show the fault propagation in model using extended modeling elements. In the first scenario (S1), there is failure in AR device, which is tower controller assistance system. Thus, the output of this component will propagate an external fault to AR-extended human, which is ATCO. This external fault would cause failure in physical/mental capability of the human and failure in deciding and finally failure in acting.

In the second scenario (S2), failure in organization component, which is civil aviation organization, will propagate an external fault to human component causing failure in physical/mental capability, deciding and acting. For example, failure in AR adoption, would cause this problem in the organization if they do not adopt AR and do not provide regulations related to AR to assist human operation. This AR adoption failure is an AR-stemmed external fault causing human failure.

In the third scenario (S3), failure in physical/mental capability of human, for example lack of required skill or attitude,

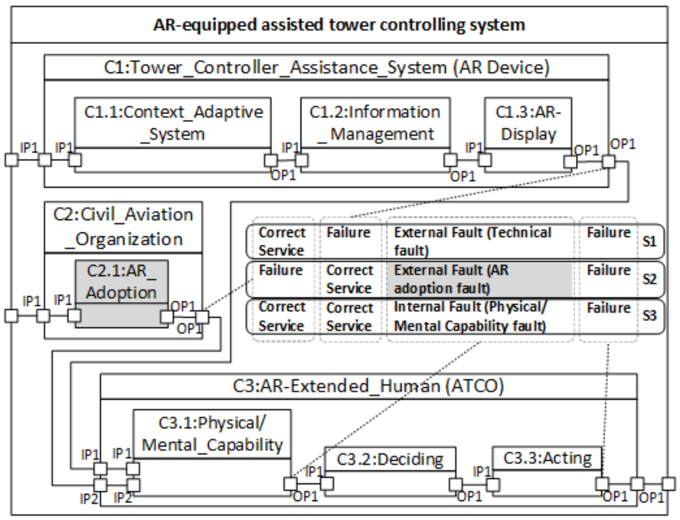

Fig. 9. AR-equipped tower controlling system modelled with the extended SafeConcert.

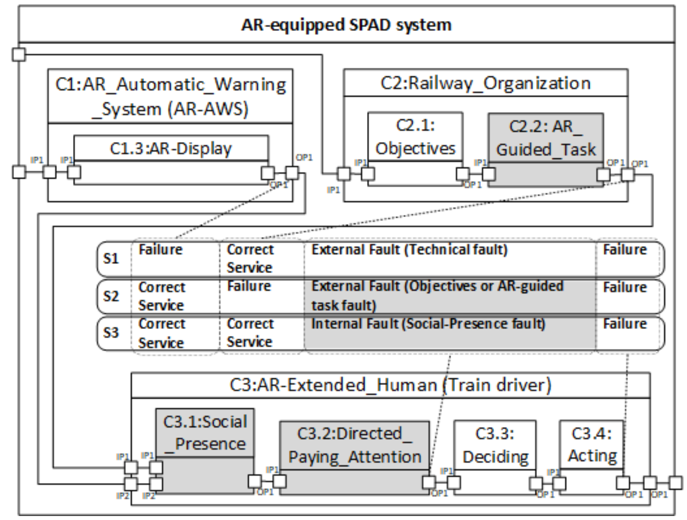

Fig. 10. AR-equipped SPAD system modelled with the extended SafeConcert.

is an internal fault in human component causing failure in deciding and acting.

Modeling element representing AR-caused fault is shown by gray color to illustrate the contribution of the extended modeling elements.

B. AR-equipped Signal Passing at Danger System Modeling

SPAD (signal passed at danger) is an incident when the train enters a high risk mode. There are Automatic Warning Systems (AWS) to provide an alarm for driver. We consider augmented reality alarm that provides an AR-AWS for the rail system [28].

Since driving a train is demanding, drivers have to tolerate high mental load and they should be strong in paying attention to the correct direction, for correct amount of time and with the correct priority. One of the reasons for SPADs is driver distraction or inattention. Based on a study [29] on Australian and New Zealand rail industry key factors leading to SPADs are time pressure, sighting restriction, station dwell, controller interaction and distraction.

Similar to the system considered in Subsection IV.A, in this system we need to model human, organization and technical entities. We model this socio-technical system using the extended modeling elements with gray color for AR-extended modeling elements.

AR-AWS, which is a composite component within a component-based architecture representing a socio-technical system contains technical components such as AR-display.

Train driver, representing the human entity of the system is a composite component containing acting, deciding and directed paying attention functions based on the extended modeling elements in [10], and social presence based on the modeling elements extension presented in Fig. 7.

Organization is a railway organization, which is a composite component containing objective and AR guided task subcomponents derived by elaborating on the possible behavior of the system. These two subcomponents are based on the organization extended modeling elements presented in Fig. 8.

Similar to Subsection IV.A, we consider three scenarios depicting failure in each of the three entities causing human failures. This hypothesized model is shown in Fig. 10.

In the first scenario (S1), there is failure in AR display, which is failure in AR-AWS and an external fault for human failure. In this scenario, AR device, which is a technical entity produces an external fault leading to human failure.

In the second scenario (S2), AR device is working properly, but there is failure in organization. For example objectives are not defined correctly or AR guided task is not defined correctly. Thus, objective fault or AR guided task fault is an external fault leading to human failures. These two subcomponents are based on the proposed extended modeling elements in this paper (Fig. 8).

In the third scenario (S3), AR device and organization are providing outputs without failure, while there is failure in subcomponents of the human itself, for example in social presence, which is an internal fault leading to human failure and it is based on the proposed extended modeling elements in this paper (Fig. 7). As it is shown in this example, we can use various extended modeling elements to model internal and external faults leading to human failures, including AR-stemmed faults.

V. Discussion

One of the challenges in our research is that the techniques that we are extending are not used by industry and we can not use their feedback for improvement of techniques. The traditional methods such as FTA, FMEA and FMECA are still used in most of the companies for risk assessment. These methods neither provide the explicit possibility of modeling human and AR-extended humans, nor AR-related faults leading to human failures in socio-technical systems. The issues related to AR-equipped socio-technical systems need cross-field expertise in human, AR and risk assessment and have largely remained unaddressed in techniques used in industry.

Another challenge is that augmented reality is a new technology, which is not implemented in some of the safety-critical applications that we want to have evaluation on. In addition, in some implemented cases, we do not have access to confidential information regarding the architecture of these systems to be used for evaluation. To do the risk assessment in a system, high number of scenarios with several failures of various components are required to improve safety based on these knowledge [30].

Despite the limited illustration given in Section IV, we see that our proposed extension for SafeConcert can help safety engineers during the modeling process of socio-technical systems in several ways. First, it provides the means for modeling failure behaviors of AR extended-humans and influencing factors on these failures, which are important parts of AR-equipped socio-technical systems. Second, it provides modeling elements based on human functions, AR-extended human functions and faults leading to human failures which are in compliant with state-of-the-art human failure and faults taxonomies reviewed in [9] and [11].

There are some limitations in the proposed extension. We can not claim that human and organization components modeling elements are mutually exclusive, because sometimes it is not possible to exactly classify the human functions or organization elements involved in doing the task that are causing human failures, into one specific category and it makes the process of human and organization modeling sophisticated. Evaluation of the proposed extension is also another important issue that should be expanded to confirm its usefulness on industrial case studies.

VI. Related works

There are several works in the literature regarding risk assessment and modeling of socio-technical systems. With the growth of utilizing new technologies in socio-technical systems, assessing the risk of using these technologies and their interaction with human in these systems is required.

In [4], authors provide risk and benefit assessment for context-adaptive augmented reality aerodrome control towers through aerodrome controllers' ratings. Several specified criteria are used for risk assessment, including transparency, complexity, interference, disruptiveness, distraction potential, failure modes and trust/complacency. Air traffic controllers were asked to rate all criteria in the range 1 to 5. Results show that context-adaptive augmented reality is helpful for controllers and improves their performance. The provided assessment is useful for demonstrating effectiveness of using augmented reality in this industry. In contrast, we try to model failure behavior of the system to overcome problems in design or implementation while developing the system.

In [31], the author proposes Safe-AR, which is a method for risk analysis of systems containing augmented reality. This method analyzes AR failures at three levels: perception, comprehension, and decision-making. To consider the safety effects of AR/user interface in risk analysis process, Safe-AR integrates failure modes related to user's mental information-processing phases. In risk assessment, likely risks and their severity are based on previous reports and the intended use of the AR. To evaluate the effectiveness of this method for other AR applications, failure modes should be generalized. In comparison to this method, our modeling method uses more general human functions and failure modes and can be considered in more AR applications.

In [32], authors propose a modelling methodology for complex socio-technical systems while new technologies are used by humans. In this method, technology modelling is used to consider its impact on system's behavior and it consists of CWA (Cognitive Work Analysis) and SD (System Dynamics) approaches [33] to capture effect of humans and dynamic interactions in complex systems. The difference of this work with ours is that the focus in this work is on complex socio-technical systems for systems engineering.

In [34], authors propose SD-BBN, which is a method that combines Bayesian belief networks (BBN) [35] and system dynamics (SD) [36] for socio-technical predictive modeling. In BBN, probabilities of causes and effects are shown by conditional probabilities. Expert opinion is used for defining the probabilities. To consider feedback loops and dynamic interactions of causal factors, this method combines BBN with SD. SD is a simulation-based modeling technique that is useful for modeling organizational behavior, dynamics and feedback. This SD-BBN method is integrated with classical probabilistic risk analysis (PRA) [37] techniques and fault tree and event tree are used to model system risk. This model is used to predict happening of accidents in a period of time and guide managers to schedule their activities, while our model is used during the system development process for eliminating design failures incrementally and iteratively.

VII. Conclusion

In this paper, we performed an additional step towards assessing risk of safety-critical socio-technical systems containing augmented reality. As known, risk assessment starts with the identification of what can go wrong. Our previously proposed human failure and fault taxonomies may act as helpful means during the identification by offering AR-specific keywords. Their coherent incorporation (proposed in this paper) within SafeConcert, a metamodel targeting socio-technical systems, helps in getting the component-level view of what can go wrong and enables compositional analysis tools to calculate what can go wrong at system level. We illustrated our extension on two fictitious but still credible systems from air traffic control and rail domains.

As future work, we aim at implementing the conceptual extension of SafeConcert within CHESSML [21]. In addition, we aim at extending current compositional analysis techniques to be able to calculate what can go wrong at system level. Specifically, our starting point will be Concerto-FLA [38], which is a plugin within the CHESS toolset, part of the, recently released, open-source AMASS platform for certification [39].

References

[1] D. Van Krevelen and R. Poelman, "A survey of augmented reality technologies , applications and limitations," *The International Journal of Virtual Reality*, vol. 9, no. 2, pp. 1–20, 2010.

[2] B. F. Goldiez, N. Saptoka, and P. Aedunuthula, "Human performance assessments when using augmented reality for navigation," University of Central Florida Orlando Inst for Simulation and Training, Tech. Rep., 2006.

[3] B. F. Goldiez, A. M. Ahmad, and P. A. Hancock, "Effects of augmented reality display settings on human wayfinding performance," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 37, no. 5, pp. 839–845, 2007.

[4] H. Gürlük, O. Gluchshenko, M. Finke, L. Christoffels, and L. Tyburzy, "Assessment of risks and benefits of context-adaptive augmented reality for aerodrome control towers," in *Digital Avionics Systems Conference (DASC)*. IEEE, 2018, pp. 1–10.

[5] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE transactions on dependable and secure computing*, vol. 1, no. 1, pp. 11–33, 2004.

[6] M. Yeh and C. Wickens, "Attention and trust biases in the design of augmented reality displays," *University of Illinois at Urbana-Champaign, Aviation Research Lab*, 2000.

[7] S. R. Dowell, D. C. Foyle, B. L. Hooey, and J. L. Williams, "The effect of visual location on cognitive tunneling with superimposed hud symbology," in *Proceedings of the human factors and ergonomics society annual meeting*, vol. 46, no. 1. SAGE Publications Sage CA: Los Angeles, CA, 2002, pp. 121–125.

[8] K. C. Hendy, "A tool for human factors accident investigation, classification and risk management," Defence Research And Development Toronto (Canada), Tech. Rep., 2003.

[9] S. Sheikh Bahaei and B. Gallina, "Augmented reality-extended humans: towards a taxonomy of failures – focus on visual technologies," in *European Safety and Reliability Conference (ESREL)*. Research Publishing, Singapore, 2019.

[10] S. Sheikh Bahaei and B. Gallina, "Towards assessing risk of safety-critical socio-technical systems while augmenting reality," As annex on the International Symposium on Model-Based Safety and Assessment (IMBSA) website, 2019. [Online]. Available: http://easyconferences.eu/imbsa2019/proceedings-annex/

[11] S. Sheikh Bahaei, B. Gallina, K. Laumann, and M. Rasmussen Skogstad, "Effect of augmented reality on faults leading to human failures in socio-technical systems," in *International Conference on System Reliability and Safety (ICSRS)*. in press.

[12] D. A. Norman, "Errors in human performance," California Univ San Diego LA JOLLA Center For Human Information Processing, Tech. Rep., 1980.

[13] J. Reason, *The human contribution: unsafe acts, accidents and heroic recoveries*. CRC Press, 2017.

[14] J. Rasmussen, "Human errors. a taxonomy for describing human malfunction in industrial installations," *Journal of occupational accidents*, vol. 4, no. 2-4, pp. 311–333, 1982.

[15] S. A. Shappell and D. A. Wiegmann, "The human factors analysis and classification system–HFACS," Civil Aeromedical Institute, Tech. Rep., 2000.

[16] N. A. Stanton and P. M. Salmon, "Human error taxonomies applied to driving: A generic driver error taxonomy and its implications for intelligent transport systems," *Safety Science*, vol. 47, no. 2, pp. 227–237, 2009.

[17] M. T. Phan, "Estimation of driver awareness of pedestrian for an augmented reality advanced driving assistance system," Ph.D. dissertation, Université de Technologie de Compiègne, 2016.

[18] D. Gertman, H. Blackman, J. Marble, J. Byers, C. Smith *et al.*, "The SPAR-H human reliability analysis method," *US Nuclear Regulatory Commission*, vol. 230, 2005.

[19] M. R. Miller, H. Jun, F. Herrera, J. Y. Villa, G. Welch, and J. N. Bailenson, "Social interaction in augmented reality," *PloS one*, vol. 14, no. 5, p. e0216290, 2019.

[20] L. Montecchi and B. Gallina, "SafeConcert: A metamodel for a concerted safety modeling of socio-technical systems," in *International Symposium on Model-Based Safety and Assessment*. Springer, 2017, pp. 129–144.

[21] CONCERTO D2.7 – analysis and back-propagation of properties for multicore systems – final version. [Online]. Available: http://www.concerto-project.org/results

[22] A. Cicchetti, F. Ciccozzi, S. Mazzini, S. Puri, M. Panunzio, A. Zovi, and T. Vardanega, "Chess: a model-driven engineering tool environment for aiding the development of complex industrial systems," in *Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering*. ACM, 2012, pp. 362–365.

[23] ARTEMIS-JU-100022 CHESS – composition with guarantees for high-integrity embedded software components assembly. [Online]. Available: http://www.chess-project.org/

[24] ARTEMIS-JU-333053 CONCERTO – guaranteed component assembly with round trip analysis for energy efficient high-integrity multi-core systems. [Online]. Available: http://www.concerto-project.org

[25] M. Wallace, "Modular architectural representation and analysis of fault propagation and transformation," *Electronic Notes in Theoretical Computer Science*, vol. 141, no. 3, pp. 53–71, 2005.

[26] K. Lee, "Augmented reality in education and training," *TechTrends*, vol. 56, no. 2, pp. 13–21, 2012.

[27] J. W. Ruffner and J. E. Fulbrook, "Usability considerations for a tower controller near-eye augmented reality display," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 51, no. 2. Sage Publications Sage CA: Los Angeles, CA, 2007, pp. 117–121.

[28] A. Naweed, S. Rainbird, and J. Chapman, "Investigating the formal countermeasures and informal strategies used to mitigate spad risk in train driving," *Ergonomics*, vol. 58, no. 6, pp. 883–896, 2015.

[29] A. Naweed and S. Rainbird, "Risk factors moderating driving-related distraction and inattention in the natural rail environment," in *3rd International Conference on Driver Distraction and Inattention*, 2013.

[30] E. Zio, "The future of risk assessment," *Reliability Engineering and System Safety*, vol. 177, pp. 176–190, Sep. 2018. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01988966

[31] R. R. Lutz, "Safe-AR: Reducing risk while augmenting reality," in *2018 IEEE 29th International Symposium on Software Reliability Engineering (ISSRE)*. IEEE, 2018, pp. 70–75.

[32] R. Oosthuizen and L. Pretorius, "Assessing the impact of new technology on complex sociotechnical systems," *South African Journal of Industrial Engineering*, vol. 27, no. 2, pp. 15–29, 2016.

[33] R. Oosthuizen and L. Pretorius, "Modelling methodology for engineering of complex sociotechnical systems," in *INCOSE International Symposium*, vol. 24, no. s1. Wiley Online Library, 2014, pp. 268–281.

[34] Z. Mohaghegh, "Combining system dynamics and bayesian belief networks for socio-technical risk analysis," in *2010 IEEE International Conference on Intelligence and Security Informatics*. IEEE, 2010, pp. 196–201.

[35] J. Pearl, "Bayesian networks: A model of self-activated memory for evidential reasoning," in *Proceedings of the 7th Conference of the Cognitive Science Society, 1985*, 1985, pp. 329–334.

[36] J. Sterman, *Business Dynamics: System Thinking and Modeling for a Complex World*. Irwin McGraw-Hill, 2000.

[37] T. Bedford, R. Cooke *et al.*, *Probabilistic risk analysis: foundations and methods*. Cambridge University Press, 2001.

[38] B. Gallina, E. Sefer, and A. Refsdal, "Towards safety risk assessment of socio-technical systems via failure logic analysis," in *2014 IEEE International Symposium on Software Reliability Engineering Workshops*. IEEE, 2014, pp. 287–292.

[39] AMASS open platform. [Online]. Available: https://www.polarsys.org/opencert/news/2018-12-05-download_p2_preview/