Combining system architecture modelling with dynamic process simulation for early stage fault and effect analysis

Linnosmaa, Joonas; Hauge, André; Sechi, Fabien; Sirola, Miki

Published in:
12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT 2021)

Published: 01/06/2021

Document Version
Publisher's final version

COMBINING SYSTEM ARCHITECTURE MODELLING WITH DYNAMIC PROCESS SIMULATION FOR EARLY STAGE FAULT AND EFFECT ANALYSIS

Joonas Linnosmaa
VTT Technical Research Centre of Finland Ltd
P.O.Box 1300, FI-33101, Finland
joonas.linnosmaa@vtt.fi

André A. Hauge, Fabien Sechi
Institute for Energy Technology (IFE)
P.O.Box 173, NO-1751 Halden, Norway
andre.hauge@ife.no; fabien.sechi@ife.no

Miki Sirola
Aalto University
P.O.Box 15400, FI-00076 Aalto, Finland
miki.sirola@aalto.fi

dx.doi.org/10.13182/T124-34311

ABSTRACT

Designing of complex process plants, such as a nuclear power plant, requires the development of the physical process and the automation system controlling it. When dynamics of the physical processes are included, it becomes challenging to identify all possible consequences arising from different component failures, including common cause failures or degraded modes of operation. In this paper, we present a concept for supporting fault and effect analysis using architecture description language capable of modelling software and hardware components and their faults of the system with a dynamic process modelling simulator. We firstly use the error modelling and analysis of the architecture to find potential critical combinations of component faults within a complex system. Secondly, we simulate the effects of combined faults on the controlled process in order to analyse system effects. We test the method on an early design of a safety system, called the Halden Safety Fan, while using Architecture Analysis and Design Language for architecture modelling and Advance PROcess Simulator for the dynamic simulation. The Halden Safety Fan system is an early conceptual design, offering a high-level description of a proposed modernisation of the existing emergency ventilation system of the Halden BWR reactor. Results indicate that proposed early-stage failure assessment can easily be performed using a model as input, gaining confidence on design choices.

Key Words: architecture description language, model-based systems engineering, safety critical systems

1 INTRODUCTION

We consider Model-Based System Engineering (MBSE) or Model-Based Design (MBD) to enable highly valued design characteristics like traceability, assessability and manageability, which increase the quality of designs, especially in complex safety critical systems. In this paper, we present results from an explorative study on the applicability of model-based methods supporting the digitalization of a legacy system (a nuclear emergency ventilation system), from early design stage point-of-view and with a focus on safety assessment of design choices. The overall motivation of our study was to explore in what ways combining iteratively model-based assessment (static analysis) with process simulation (dynamic analysis) can support early-stage safety analysis and provide results that inform the system engineers in the further refinement of their system digitalization design.

This paper documents the exploration of the combined application of Architecture Analysis and Design Language (AADL), acting as the static analysis method, and the Advance PROcess Simulator (APROS), acting as the dynamic physics based simulator, for early design stage development and analysis. We used the Halden Safety Fan (HSF) system concept as an exemplary case. The HSF system is currently at a conceptual stage, offering a high-level description of a proposed modernisation of the existing emergency ventilation system of the Halden BWR reactor (HBWR). This paper extends our previous research working with conceptual model-based design of the HSF system.

2 BACKGROUND

2.1 Model-based system design and assessment

Industrial system design and the engineered systems are more complex and interconnected than ever. The processes by which they are designed, produced, operated, and decommissioned also have become more complex. Thus, different engineering disciplines are using models to digitalise their efforts. Rauzy and Haskins describe this transition as entering the era of Model-Based Systems Engineering (MBSE) [1]. MBSE uses models to help the communication between and inside engineers of various domains. Models help visualise and augment understanding of the problem domain with formalism, instead of using textual statements. Model-based methods are claimed to improve management of information during system development. From the safety and security point of view, clear communication and management of mission critical information are essential.

Developing a system disconnected or loosely connected to safety analyses (or vice versa) makes it difficult for the analysis results to affect the design in a timely manner. Model-Based Safety Analysis [2] pursue synchronization and cooperation between models to integrate the development cycle. MBSA techniques can support effective and robust techniques for automatic safety analysis techniques using the system model as input [3]. Some of the general-purpose Architecture Modelling Languages (ADL), e.g. System Modeling Language (SysML) or AADL, can support MBSA. However, the possibilities for automatic or semi-automatic analysis of models are dependent on the scope of the modelling, the modelling language selected, the analysis perspective needed, tool availability and more. Systems are analysed from various points of view, and the term “safety analysis” usually covers assessments focusing on the performance of the system considering the uncertainties and failures that could occur during operation. System architecture models are essential for model-based analysis.

2.2 Modelling system architecture

Using models to capture system architecture and the design requirements facilitates a focus on the structure of the system in its early stages. Architecture is a complex design discipline which can benefit from automated analyses going through the possibly complex and multi-layered design. Two widely used standard languages that can assist the MBSE and MBSA approaches are AADL and SysML. [4]

AADL is a formal notation for describing a system architecture, standardized in [5]. Mkaouar et al. describe AADL as an industrial architecture language for critical domains such as avionics, automotive electronics and robotics [6]. We have previously worked with AADL in complex design, including nuclear [7] [8]. Different research groups have developed the language further from its standard version, and it has been extended to cover many other domains, and safety-related systems through various domain-related annexes enabling a further detailing of the specification of the architecture. We used the “Annex E” - Error Model V2 (EMV2) of the standard. EMV2 supports: 1) qualitative and quantitative assessments of system concepts such as safety, security, availability, survivability, robustness, resilience, and reliability; 2) assuring compliance of the system design and implementation to the fault mitigation strategies; and 3) specifying errors, error propagations, and failures in the architecture model of the system. For modelling we used the OSATE2 tool, which with the help of Annexes supports safety analysis for Functional Hazard Assessments (FHAs), Fault Tree Analysis (FTA), Failure Modes Effects Analysis (FMEA), Common Mode Analysis, and Reliability Block Diagrams (RBD)/Decision Diagrams (DD). In our study, the focus is on the automatic generation of Fault Tree Analysis (FTA), based on the error modelling performed with EMV2.

2.3 Simulating dynamic system behaviour

Process simulation is a way to virtually model a process in detail without having to physically build and test the design of the system to control the process, saving resources and time. There are various simulation techniques depending on the size and complexity of the process, and the wanted outcomes of the simulation. Main types being steady-state (e.g. mass/energy balance independent of time) or dynamic simulation (e.g. derivatives of mass/energy time-dependent). In this research we are interested in the dynamic behaviour of the process in the presence of fault situations in the control system. There are many such first principle simulation software, examples are Simulink, Dymola or APROS.

APROS calculation is based on first principles, and physical laws realized with differential equations. APROS has its own command language for defining simulation models and for performing simulation experiments [9]. Data is stored into a real-time database, which is made to meet data management requirements for real-time simulations. Data in the database is accessed by modules, and the module structures are associated with variables, attributes, and module type definitions. A solid validation scheme also exists for model building. We use ProcSee [10], a software based on graphical user interface management system for implementing the Human-Machine Interface (HMI) for the APROS simulation models. When building the graphical model, the simulation model in APROS database is constructed automatically and simultaneously. The graphical user interface can also be used simultaneously with the APROS command line. APROS builds in the database corresponding calculation-level components for each process component. All simulation calculations are done on the calculation level.

3 COMBINING MBSA AND PROCESS SIMULATION

Designing of complex process plants, such as a nuclear power plant, requires the development of the physical process and the automation system controlling it. When dynamics of the physical processes are included, it becomes challenging to identify all possible consequences arising from various component or software failures, including common cause failures (CCF). Process simulation, dynamic and physics-based, is often used to analyse and specify the process-related parameters in process plants. Dynamic simulation is a key technology when designing these processes [11], just like ADL supported MBSE(A) is becoming for designing the software/hardware architectures of complex systems. Combining these two has opened interesting possibilities, by adding dynamic properties to often static analyses of ADLs. Also, regulatory authorities usually require both deterministic and probabilistic methods to be used in validating the system design. Such deterministic methods require that the used simulation models are based on natural scientific theory, including first principle simulation models using differential equations based on the laws of physics.

We present in this paper a concept that combines architecture description language modelling and the dynamic process modelling for analysing the dynamic process effects of component faults in the system. The basic idea of the concept is modelled with a flowchart in Figure 1. On one side, we want to use the early system information from design to create an architecture model of the system using a formal model of the system components (including the software and hardware components as far as the information is available) and their error (fault) models. On the process information side, we want to use the dynamic process model, which includes the early information available of the actual process the system is handling, including its behaviour. As discussed above, it is sometimes difficult to interpret the real physical consequences arising from component failures of the control system. We try to support this fault and effect analysis by trying to use the architecture and the related error modelling to search and quantify different possible error states of the system and then use physics-based behaviour model to determine the severity of the possible effect of these faults to the actual process. At some level, this resembles the Failure Mode and Effects Analysis (FMEA), where different components, subsystems or assemblies are reviewed to identify potential failure modes and their effects.

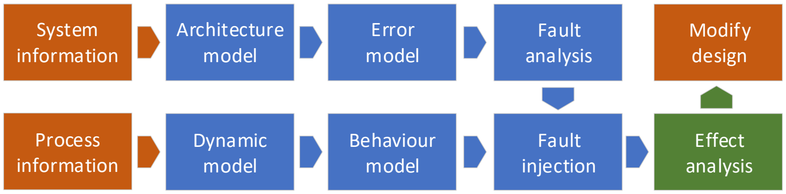

Figure 1. Concept for combining architecture and dynamic models for fault and effect analysis.

There is some research on combining or automating safety analyses with process simulation. Raoni et al. in [12] propose a systematic procedure that uses process simulation for the identification and analysis of hazardous process deviation using HAZOP. The authors point out that process simulation enables the analysis of process behaviours that are caused by device malfunctions, and the deviation analysis that considers the process non-linearities and dynamics. Ramzan et al. in [13] also extended HAZOP with process simulation to study process disturbances and deviations. In [14] and [15], Kummer et al. used MATLAB and a dynamic process simulator to explore hazardous events and their effects in chemical processes, they concluded that the time spending in HAZOP was shortened. AADL has also been extended to cover continuous simulation using Modelica for Cyber-Physical Systems (CPS) and their behaviour validation by Liu et al. [16], they extended the language to cover discrete and continuous behaviour of CPS with new properties, variables, equation and interactive components so that the OSATE tool interact with the simulator. More similar papers have been presented for AADL, e.g. [17], and SysML, e.g. [18], where the discrete and continuous behaviours of the models are combined to create a better understanding of the system.

4 CASE STUDY SYSTEM: HALDEN SAFETY FAN

This paper extends the experimental work started in [19], [20], where we introduced a case study system called the Halden Safety Fan (HSF), which is an initiative to research Digital Instrumentation & Control (DI&C), model-based design, assurance and digitalization of old analogy emergency ventilation system inspired by a real system that is part of the Halden research reactor in Norway. Digitalization steps of the control system, in general, will include establishing a concept description, the development and safety assessment plans, system requirements specification, risk analysis and safety assessment report. The new digital design is based on similar installations in real nuclear reactors[1], and validated by plant engineers. In previous work we have started to describe the overall functions of the system, the main sub-systems and components, and the interconnections between these. The outline for the functional behaviour of the system also exists. These descriptions are enough to start the early-stage safe-by-design assessment on the system.

Th following is a brief summary of the functionality of the case system. When the emergency ventilation system (EVS) is activated it captures air from the airflow of the normal ventilation system and the normal ventilation is deactivated. EVS operates independently, but in conjunction with the normal ventilation system. The EVS has more effective filtration and outflow capabilities and is designed to keep the containment building underpressurized in an accident situation and keep radiation of the outflowing air under set limits. The classification of an EVS is a safety-related system [21]. The concept architecture and the main components belonging to the EVS are shown in Figure 2. It shows the main process lines from the normal ventilation through the emergency ventilation to the exhaust at the main stack (chimney) of the plant. Notably, it comprises of two identical redundant sides; AB (on the left) and CD (on the right), which

[1] Mark II containment, Loviisa Plant, and Oskarshamn 3 Plant

both have filters and fans for moving the contaminated air safely out of the containment, both sides are controlled by an independent PLC.

In [19], we laid down simplified but realistic design principles and started the model-based design and safety assessment of the HSF EVS, an imaginary modernization of the Halden reactor. We first carefully studied the existing emergency ventilation systems of some Scandinavian and US nuclear reactors. From these inspiration sources, a concept for a new emergency ventilation was conceptualized. In the same report, we also created an AADL model to describe the static digital I&C components of the system and an APROS simulation model to describe the dynamic process side of the system. We used the AADL model to study a failstop situation of one the sides of the system using automatic fault tree analysis (FTA) available in the OSATE2 toolset. We used the APROS toolset to simulate the physical effects of the failure in the system. In the next chapter, we explore the idea of a combined use of these models to create a methodology for iterative design and safety assessment, which we believe supports effective model-based development and assessment for critical DI&C systems. More thorough explanations on the HSF EVS system as well as the AADL and APROS models can be found in [20] and its annexes.

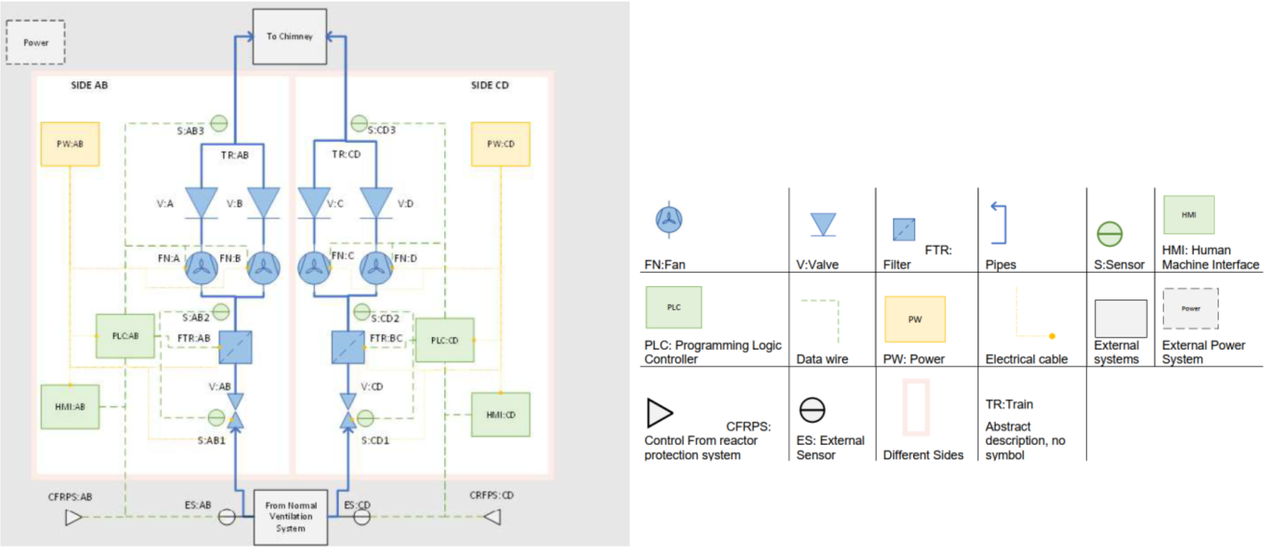

Figure 2. Halden Safety Fan design & components [19].

5 CASE STUDY: COMBINING STATIC AND DYNAMIC MODELLING

In the following, we give a high-level presentation of the AADL and APROS models created for the HSF case, presented in Chapter 4. More importantly, we discuss the assessments carried out using these models as well as present the ideas of combining these two model-based assessments into iterative design and assessment methodology. The errors we are modelling, and analysing are related to a failstop situation of one of the redundant sides of the EVS, which can happen when one or more service errors occur for the components of that redundant side (such as lack of data to the PLC or no power in the operational state). The failure happens during an emergency situation where there was been a radiation leak to the containment building and the EVS has started to clear the radiation through the filters to the main stack.

5.1 Model-based architecture analysis: the static side

We use AADL as a formal notation for describing the EVS design architecture, it contains the information about the hierarchy and layout of the system's components and modules and how these connect and interact with each other. The conceptual modelling was done in OSATE2 including AADL EMV2 annex for extended error modelling. Using the error model, we specified the mechanics for a failstop on one of the sides of the EVS using composite error behaviour and states for the different subcomponents (the failure rates were issued from mixed literature sources). In our model, the PLC acts as the error sink for all the actuators and sensors, which are the error sources. This paper will focus on the FTA, which was then performed based on the modelled error behaviour. FTA is a commonly applied technique for hazard analysis, and OSATE2 supports the event and gates defined by the US-NRC in [15]. The modelling and the assessment process we followed is shown in Figure 3.

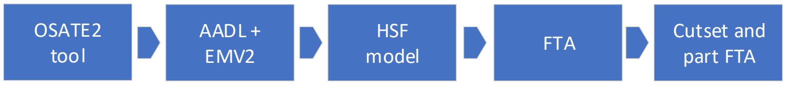

Figure 3. High level description of the AADL modelling process.

FTA uses a top-down approach to failure analysis, starting from a “top-event”. The method assumes failure of the functionality of a component. In the FTA, the goal is to identify the causes of a hazardous event and the root cause of functional failure. The FTA methodology supports the analysts in deducing how the individual or combined lower-level failures or events leads to the top-events (hazard/undesirable event). The FTA analysis in OSATE2 uses the specified error states and the outgoing error propagation in the AADL model as the starting point in the analysis and as basis for producing the fault tree, i.e. the error behaviour. The analysis plugin identifies and interprets composite error state declarations, traces the defined error propagations backwards to its source via the propagation flows, and identifies the failure states and failure behaviour of components to build the fault tree with its basic events and gates. In OSATE2, FTA analysis permit to compute different variants of FTA such as fault tree with computed probability, the minimal cut-sets probability with computed probability, fault contributor trace and parts fault tree with computed probability only the composite error states. The logical condition is that if sub-components such as fans, valve, the filter unit, the PLC, or the power supply fails then the relevant side subsystem (e.g. AB side) reaches the failstop state. Each of these mentioned components has an internal component error behaviour that handles failstop behaviour.

Two different analysis methods are used, the part-fault tree, and the cut-sets analysis. Part-fault tree calculates occurrence probability of a failstop based on the current model configuration using the specified failure probability of the error states of the leaf components (the basic events of the FTA). For the single redundant EVS side there were thirteen cut-sets which can be used to understand the structural vulnerability of a system. As it was only a part of the complete system and which already consists of many redundant components (e.g. independent power, PLC, sensors) most were single points of failure. The longer a minimal cut set is, the less vulnerable the system is. Using the part-fault tree and the cut analysis we got the cut-sets and probabilities for our failstop scenario.

5.2 Process simulation: the dynamic side

To build the dynamic HSF process simulation, components similar to those in the HAMBO simulator (identical to Forsmark nuclear power plant in Sweden) were used as inspiration. The target values for required under pressure in different spaces of the reactor building and the air flow to chimney are comparable with the real values from the Forsmark nuclear power plant in Sweden. When building the APROS process model for HSF, only the basic APROS library process components was used. Automation loops was added for under-pressure control in a reactor building room and for control of output mass flow to the chimney. The features for room simulation and radioactivity simulation were then added. Process model includes control loops for mass flow and under-pressure control, and additional structures for room and radioactivity simulation.

The HSF simulator model is made to fulfil the following three defined functional requirements; 1) maintain under pressure in secondary containment room, 2) limit radiation to chimney, 3) air flow maximum to chimney is defined by the filter capacity.

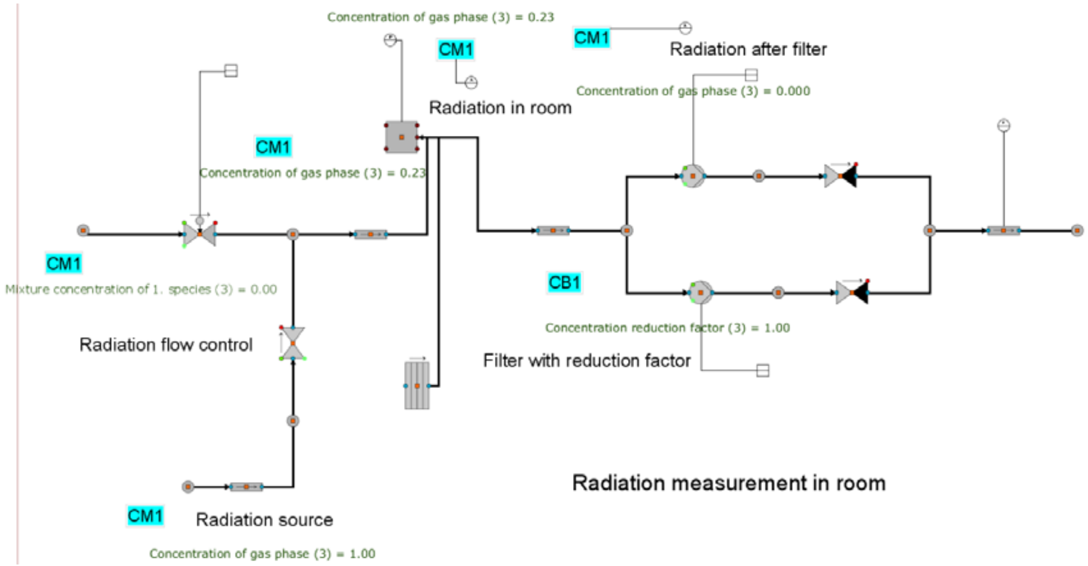
Concentration of gas phase (3) = 0.23
CM1
CM1
Radiation after filter
Radiation in room
Concentration of gas phase (3) = 0.000
CM1
Concentration of gas phase (3) = 0.23
CM1
Mixture concentration of 1. species (3) = 0.00
CB1
Concentration reduction factor (3) = 1.00
Radiation flow control
Filter with reduction factor
Radiation measurement in room
CM1
Radiation source
Concentration of gas phase (3) = 1.00

Figure 4. HSF process model in APROS [19]**.**

To simulate all features to follow and maintain these requirements some additional features are built in the HSF simulator. In order to have realistic reactor room radiation simulation, calculation level component changes to APROS were needed, also to enable radiation release simulation there is an extra branch including radiation source (as seen on the bottom-left in Figure 4). Further studies using APROS for HSF EVS are reported in [22].

5.3 Dynamic analysis of HSF failstop event from FTA

One way to combine the different models is by using the minimal cut-sets from the FTA of the AADL model as input to the definition of failure scenarios in APROS. This can be performed by a stepwise fault injection and simulation run on the basis of each set in the minimal cut-sets and then documenting the system effects as found in the simulation run. The system effects observed at each simulation run will give valuable feedback to revise analysis results, e.g. update a component or sub-system FMEA or the FTA with respect to potential system effects of single and multiple component failure. FTA gives information about the severity and the probability of different cut sets and can help to iterate the most harmful cases first. Figure 5 depicts to process of combining the two HSF models, AADL and APROS, (as was explained in Chapter 3 at general level).

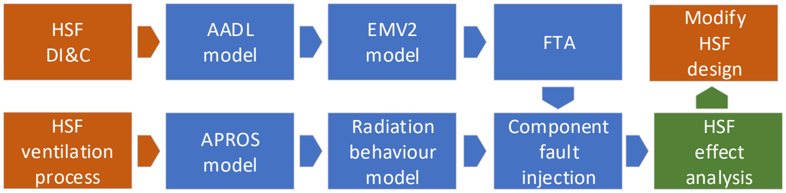

Figure 5. Our concept of combining AADL with APROS for fault effect analysis.

Our example FTA of the AADL model focused on the failstop scenario, giving the different cut-sets leading to failstop at the system level. However, the FTA could be expanded to consider many more top events, e.g. degraded function, given a richer and more detailed error modelling. In order to investigate how APROS could support the FTA analysis with simulating potential failure events in an extended AADL failure model we present here a scenario where one of the fans stops due to a sudden loss of control energy. At the same time a radioactivity release into the reactor building occurs. This represent an event where there is a partial loss of the system function or more specifically a loss of redundancy.

We present the results of our example analysis with the help of the Figure 6, where we use the AADL model introduced in Section 5.1 and see its effect using the APROS model introduces in Section 5.2. The Figure 6 is captured from APROS process simulator. In the beginning of the scenario there has been a leak and some radioactivity is in the reactor building (red curve marked with A in Figure 6). Aften the initial leak there is no release anymore and the radioactivity level in the reactor building room goes down in a couple of minutes (as EVS starts to operate normally). The coal filter of the emergency ventilation system takes care that all activity is filtered out and at this point no radiation goes through the chimney to the environment (cyan curve). Then the defined initiating event occurs (one of the EVS fans stops, the upper branch from Figure 4), and at the same time with the fan failure, the leak activates again (seen as the green curve in the Figure 6).

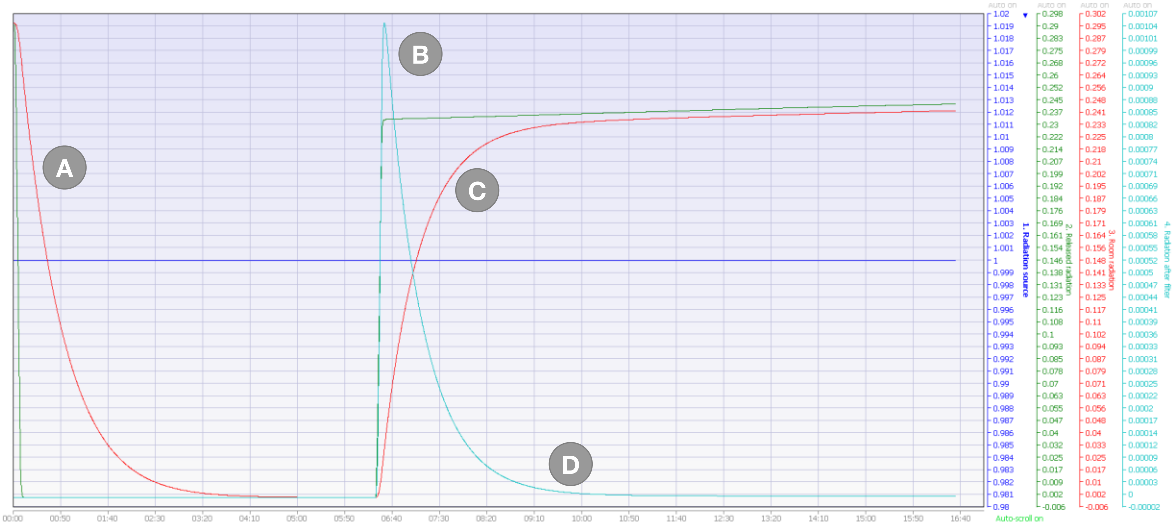

Figure 6. The radioactivity levels in different parts of the reactor building and emergency ventilation system (red curve is the reactor building room).

When one of the fans stops, the mass flow in the corresponding branch goes rapidly to zero. To keep full speed in the filter, the mass flow of the other branch increases rather rapidly to double value due to the flow control. The mass flows in the filter and chimney are affected for a short while, but they reach their desired value levels rather quickly. The sudden radioactivity release (seen as green curve in Figure 6), affects the reactor room radioactivity with some delay, see red curve in Figure 6 (marked with C). A very small amount of radioactivity goes through the filter to the chimney during the first couple of minutes after the initiating event, see Figure 6 turquoise (cyan) curve (marked with B and D), but after that the filter is again capable of filtering out 100% of the released radioactivity and no more activity gets to the environment.

After the needed simulation runs are made and the system effects are observed, they are checked against the safety requirements/margins set to system and critical process parameters (e.g. radiation release limits). If the system response to the analysed accident scenario is as intended, it gives the designer reinforcement that the design seems valid regarding this selected cut-set. Otherwise, if the behaviour is deemed critical, the results can be used to update the system design to handle this scenario better, e.g. modify the parameters related to fan or filter capacities. This will result in a new updated fault tree and cut-sets of the scenario, which can be then used as an input for another simulation run.

6 DISCUSSION AND CONCLUSIONS

We investigated how a model of the DI&C (AADL) of an example system (HSF) and its analysis could be combined with a dynamic process model (APROS) to support early-stage model-based development and safety analysis. The general concept was to analyse how faults may arise in the DI&C system and use that information to define failure scenarios for the process simulation and observe system effects. The HSF case study we presented in this paper, was an example to explore the early fault and effect analysis support. The model of HSF DI&C system was built using standard AADL (including PLC, sensors, actuators, communication flows power flows). We implemented the EMV2 error model to capture error behaviour for AADL model and ran the FTA plugin of OSATE2 toolset to gain the cut-sets leading to failstop situation of the EVS system. We picked one of the cut-sets from the FTA and injected the fault of the cut-set to the first principle physics APROS simulator (including rooms, pumps, valves, pumps, heat structures) to analyse its system effect on the HSF case. The resulting system effects observed through simulation are used as input to refine the EVS system design with respect to critical operation parameters, such as pressure and radiation levels and mass flow, which have effects on the safety of personnel inside and outside of the containment building. From the experience acquired by the authors we advocate that this modelling and performing static analysis of the DI&C in AADL combined with dynamic analysis of system effects in APROS can support modeller, safety expert or assessor to make an informed decision on further refinement of the system as early as possible and with moderate efforts.

This explorative study, extending the work detailed in [19] and [20], focused on the early conceptual stage of the development using Halden Safety Fan (HSF) concept as the example case. The case has been defined at a high level of detail and the overall functionality, the main sub-systems and components, their interconnections and the basic behaviour of system have been outlined. Based on this information, the created AADL model focused on modelling the structural aspects (standard AADL) and non-nominal behaviour (error modelling with EMV2). The assumption of the workgroup is that this kind of AADL model would facilitate early safety assessment. We know that the failstop situation is somewhat simple failure state to analyse, as it is often easy to predict the system effect would be when sub-systems and components are unavailable. Here we used it as an introduction and exercise to study capabilities of the models. However, in the future we are interested to analyse the effects of more complex faults, e.g. common cause failures (CCFs) or degraded operation scenarios in the system (e.g. all of the fans can only work at 25%, or valves are stuck at some position). In scenarios like these, it can be difficult to predict the exact process behaviour and physical consequences of the events unfolding in the fault state. Complex scenarios require sophisticated models to simulate the behaviour of the system.

7 ACKNOWLEDGMENTS

The Finnish Research Programme on Nuclear Power Plant Safety 2018-2022 funded this research (SAFIR2022, http://safir2022.vtt.fi). This work has been also conducted within the OECD Halden Reactor Project MTO research programme 2018-2020, Institute for Energy Technology, Halden, Norway.

8 REFERENCES

1. A. B. Rauzy and C. Haskins, “Foundations for model-based systems engineering and model-based safety assessment,” *Systems Engineering*, **vol. 22, no. 2**, pp. 146–155, (2019).
2. A. Legendre, A. Lanusse, and A. Rauzy, “Toward model synchronization between safety analysis and system architecture design in industrial contexts,” in *Lecture Notes in Computer Science*, **vol. 10437**, pp. 35–49, (2017).
3. S. Sharvia and Y. Papadopoulos, “Integrating model checking with HiP-HOPS in model-based safety analysis,” *Reliability Engineering and System Safety*, **vol. 135**, pp. 64–80, (2015).
4. A. Hauge, J. Linnosmaa, R. Fredriksen, and F. Sechi, “Safety and Security in DI&C Design – Systematic Literature Study,” OECD Halden Reactor Project, Institute for Energy Technology (IFE), Technical Report HWR-1247, p. 40, (2019).
5. SAE International, “SAE AS5506C Architecture Analysis & Design Language (AADL).” (2017).

6. H. Mkaouar, B. Zalila, J. Hugues, and M. Jmaiel, “A formal approach to AADL model-based software engineering,” *International Journal on Software Tools for Technology Transfer*, **vol. 22, no. 2**, pp. 219–247, (2020).
7. G. Dahll and B. A. Gran, “Use of Bayesian belief nets in safety assessment of software based systems,” *International Journal of General Systems*, **vol. 29, no. 2**, pp. 205–229, (2000).
8. J. Linnosmaa, J. Valkonen, P. Karpati, A. Hauge, F. Sechi, and B. A. Gran, “Towards model-based specification and safety assurance of nuclear I&C systems - Applicability of SysML and AADL,” *11th Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC & HMIT 2019*, Orlando, FL, USA, February 9-14, pp. 276–289, (2019).
9. E. Silvennoinen, K. Juslin, M. Hänninen, O. Tiihonen, J. Kurki, and K. Porkholm, *The APROS software for process simulation and model development*. VTT Research Report 618, VTT Technical Research Centre of Finland, Espoo, (1989).
10. “ProcSee - IFE.” https://ife.no/en/Service/procsee/ (accessed Feb. 26, 2021).
11. N. Asprion and M. Bortz, “Process Modeling, Simulation and Optimization: From Single Solutions to a Multitude of Solutions to Support Decision Making,” *Chemie Ingenieur Technik*, **vol. 90, no. 11**, pp. 1727–1738, (2018).
12. R. Raoni, A. R. Secchi, and M. Demichela, “Employing process simulation for hazardous process deviation identification and analysis,” *Safety Science*, **vol. 101**, pp. 209–219, (2018).
13. N. Ramzan, F. Compart, and W. Witt, “Methodology for the generation and evaluation of safety system alternatives based on extended hazop,” *Process Safety Progress*, **vol. 26, no. 1**, pp. 35–42, (2007).
14. A. Kummer and T. Varga, “Process simulator assisted framework to support process safety analysis,” *Journal of Loss Prevention in the Process Industries*, **vol. 58**, pp. 22–29, (2019).
15. A. Kummer and T. Varga, “Dynamic process simulation based process malfunction analysis,” in *Computer Aided Chemical Engineering*, **vol. 43**, pp. 1147–1152, (2018).
16. J. Liu, T. Li, Z. Ding, Y. Qian, H. Sun, and J. He, “AADL+: a simulation-based methodology for cyber-physical systems,” *Frontiers of Computer Science*, **vol. 13, no. 3**, pp. 516–538, (2019).
17. Y. Zhou, J. Baras, and S. Wang, “Hardware Software Co-design for Automotive CPS using Architecture Analysis and Design Language,” Mar. 2016, Accessed: Sep. 04, 2020. [Online]. Available: http://arxiv.org/abs/1603.05069.
18. E. Palachi, C. Cohen, and S. Takashi, “Simulation of cyber physical models using SysML and numerical solvers,” in *SysCon 2013 - 7th Annual IEEE International Systems Conference, Proceedings*, Orlando, FL, USA, April 15-18, pp. 671–675, (2013).
19. F. Sechi, A. Hauge, M. Sirola, S. Olsen, J. Linnosmaa, and S. Sarshar, “Early stage safety assessment using a system model as input,” OECD Halden Reactor Project, Institute for Energy Technology (IFE), Technical Report HWR-1287, (2020).
20. B. A. Gran, A. Hauge, J. Simensen, S. Sarshar, F. Sechi, X. Gao, and M. Sirola, “Halden Safety Fan – Context Description and System Specification,” OECD Halden Reactor Project, Institute for Energy Technology (IFE), Technical Report HWR-1289, (2020).
21. GE, “Boiling Water Reactor - GE BWR/4 Technology - Technology Manual - Chapter 4.0 - Containment Systems,” vol. ML02302012, no. Rev 0196. p. 151, (2002).
22. M. Sirola and P. Karpati, “Simulation support in model-based assessment of conceptual nuclear power plant emergency ventilation system,” OECD Halden Reactor Project, Institute for Energy Technology (IFE), Technical Report HWR-1309, (2020).