Towards generating contextualised fault scenarios for reliability risk analysis of cyber-physical systems

Lufeng Wei†, Zhi Li†*, Yuansong Qin†
†School of Computer Science and Engineering, Guangxi Normal University, Guilin, China
Email: weilf@stu.gxun.edu.cn, zhili@gxnu.edu.cn, wyjfqys@gmail.com

***Abstract*—This paper proposes an approach that combines Fault Tree Analysis with Problem Frames to present the latent reliability risks of Cyber-Physical Systems. By extracting causality within each, this approach associates the atomic events of the Fault Tree with the shared phenomena of the Problem Diagram, in order to generate scenarios with contexts that may lead to the occurrence of faults.**

***Index Terms*—Cyber-Physical Systems, Problem Frames, Requirements Engineering, Fault Tree Analysis**

I. Background and motivation

The Problem Frames (PF) approach is primarily used to explain how the machine to be built will interact with the external world to meet the customer's needs. Typically, when describing requirements using PF, forward reasoning is used - that is, triggering the modeling process from the perspective of the requirements and constructing machine behaviors by studying the properties and behaviours of the real-world domains. This modeling method is effective for Cyber-Physical Systems (CPS), but lacks the evaluation of faults caused by environmental failures. Lin et al. [1] [2] proposed the concept of Abuse Frames to introduce external attacks into the modeling process, but did not clarify the role of causalities arising from shared phenomena between domain interactions.

Fault Tree Analysis (FTA) is typically used to evaluate the failure of system components by decomposing top-level faults into intermediate events and primary events connected by logic gates in a layered manner. However, this approach often fails to represent information about the system's requirements and other relevant factors. Additionally, according to Smith et al. [3], if the analysts neglect or do not adequately consider the contextual information of the system, they may lose the ability to determine whether combinations of system behaviors beyond the Fault Tree (FT) will lead to failures.

In the Problem Diagram (PD), shared phenomena describe interactions among domains and the machine, forming forward chains of causalities. In the FT, the generation of upper-level events is composed of lower-level events through the combination of logic gates, which can be considered to occur on backward chains of causalities. The approach proposed in this paper combines the forward and backward chains of causalities, enabling the generation of fault information with contextualised scenarios, which facilitates the detection of potential reliability problems in early analysis.

*corresponding author: zhili@gxnu.edu.cn
DOI reference number: 10.18293/SEKE2023-229

II. The Approach

A. Check the Fault Tree and Create the Mapping Table

When the FT is initially constructed, its leaf nodes may be composite events [4]. To ensure that these leaf nodes have the same granularity as the shared phenomena in the PD, the first step is to check the leaf nodes in the FT and split composite events into atomic events combined by logic gates. After completing the fault tree check, and associating the FT and the PD, the fault information mapping table (FIMT) is created. For each leaf node, domain experts should look for the corresponding shared phenomena in the PD, thus shared phenomena that can be matched to atomic events are set as associated elements in the FIMT.

B. Minimum Cut Sets Extraction

The top event in the FT can be generated by a combination of different leaf nodes. In this paper, a top down method and Boolean algebra operation rules are used to split the top event into an event set composed of leaf nodes, and then reduce the redundant items in the event set to obtain minimum cut sets. Minimum cut sets will be used for further analysis in step D.

C. Causal Chain Set Extraction

The causal attributes of the domain in the PD are part of causal chains. To obtain causal chains in the PD, the following cases: $a \rightarrow (b \wedge c)$, $a \rightarrow (b \vee c)$, and $(a \vee b) \rightarrow c$ should be split into one-to-one causalities, where a, b, and c are shared phenomena in domains. This paper regards the causal transformation of shared phenomena in the PD as a directed acyclic graph and represents it as an adjacency matrix. The DFS algorithm is used to obtain a set of causal chains that start from the initial shared phenomenon and end at the terminal shared phenomenon. To obtain a set of causal chains that include all shared phenomena, this paper also treats each shared phenomenon that does not participate in causal transformation as a causal chain containing only one element.

D. Fault Scenario Generation

If all events in a minimal cut set occur, the top event of the FT is guaranteed to occur. For each atomic event in a given cut set, this paper search for the corresponding shared phenomenon in the causal chain set of the PD based on the FIMT. If a corresponding shared phenomenon can be found in the FIMT for each atomic event, the cut set can be triggered by the known domain in the PD. Treating

TABLE I
PART OF FIMT

ID	Name	Type	Domain	Shared Phenomenon
E1	X1	Detectable	Car	Car_in
E3	X3	Detectable	Train	$Train\_in$
E5	X5	Detectable	Fence	$Fence\_closed$

the mapping information in the FIMT as connecting nodes, with the predecessors being the shared phenomena that can be associated with the causal chain set and the successors being the events in the minimal cut set of the fault tree, a contextualised fault scenario starting from the initial shared phenomenon and ending at the top event of the FT can be obtained. If the atomic events included in a fault scenario can form a minimal cut set and the cut set can be triggered by the known domains in the PD, we can draw the conclusion that the ending of this scenario is reachable, and this scenario is suitable to describe the system's fault trace.

III. CASE STUDIES

This section presents an example of railway barrier control system. In this example, a sensor is set to detect the distance between train and crossing. The barrier gates are required to keep open before and after the train passes through the crossing, allowing cars to pass the crossing normally; when the train is about to arrive, both sides of the barrier gates need to be closed to prevent cars from entering the crossing. The PD, FT, full version of causal chain set and minimal cut sets for this example are shown at GitHub[1], the FT of this example indicates that a traffic accident will occur when a car enters the crossing, the barrier gates closed, and the train enters the crossing.

Matching the shared phenomena in the PD to the relevant FT leaf nodes, we can get the FIMT partly shown at Table I, which means event $X1$, $X3$ and $X5$ in the FT can be found in the PD.

Traversing the causal transformations in the PD, the following parts of causal chains can be extracted:

$$Train\_approach \rightarrow Train\_approaching \rightarrow Fence\_off \rightarrow Fence\_closed \quad (1)$$

$$Train\_in \quad (2)$$

$$Car\_in \quad (3)$$

By comparing with the FIMT, it can be found that for the minimum cut set $\{X1, X2, X3\}$, the causal chains extracted from the PD contain shared phenomena that make all three atomic events hold. Therefore, the following fault scenario with contextual information can be obtained.

[1] $https://github.com/Wei-GXNU/Railway-Example$

$$Causal\ Chain\ (3) \rightarrow \underline{\mathbf{E1}} \rightarrow X1 \searrow$$
$$Causal\ Chain\ (1) \rightarrow \underline{\mathbf{E5}} \rightarrow X5 \rightarrow Cutset \rightarrow Top\ event$$
$$Causal\ Chain\ (2) \rightarrow \underline{\mathbf{E3}} \rightarrow X3 \nearrow$$

This scenario illustrates that the combination of the car's entrance into the crossing, the train's approach from distance and entrance into the crossing can lead to a fault, even though all three behaviors are normal in the system. Therefore, compared to the causal transformation information obtained solely from the PD (predecessors of connecting nodes E1-E3), this method can reveal whether the combination of normal behaviors within the system will cause a fault.

In addition, this scenario also demonstrates a fact that $Fence\_closed$ is caused by $Train\_approach$, which could not be found in the FT. Therefore, compared to purely considering the combination of atomic events in the FT (successors of connecting nodes E1-E3), this approach can identify the contextual information when the top event occurs. By generating fault scenarios from two perspectives, analysis personnel can discover defects in software architecture in the early stages of a project and avoid introducing potential reliability issues into the development phase.

IV. CONCLUSION

This paper combines the Problem Frames with the Fault Tree Analysis to overcome the shortcomings of both methods and obtain a more complete description of fault scenarios by leveraging the advantages of both, which is crucial for reducing latent errors in the requirements analysis phase. In future work, we will refine the extraction of causalities from the Problem Diagram and attempt to refine the approach used to describe the domain properties and extract causal information from outside the machine, in order to obtain more reasonable causal contextual scenarios.

ACKNOWLEDGMENT

This work is partially supported by the National Natural Science Foundation of China (61862009), Guangxi "Bagui Scholar" Teams for Innovation and Research.

REFERENCES

[1] L. Lin, B. Nuseibeh, D. C. Ince, M. Jackson, and J. D. Moffett, "Introducing abuse frames for analysing security requirements," in *11th IEEE International Conference on Requirements Engineering (RE 2003), 8-12 September 2003, Monterey Bay, CA, USA*. IEEE Computer Society, 2003, pp. 371–372.

[2] L. Lin, B. Nuseibeh, D. C. Ince, and M. Jackson, "Using abuse frames to bound the scope of security problems," in *12th IEEE International Conference on Requirements Engineering (RE 2004), 6-10 September 2004, Kyoto, Japan*. IEEE Computer Society, 2004, pp. 354–355.

[3] D. Smith, B. Veitch, F. Khan, and R. Taylor, "Understanding industrial safety: Comparing fault tree, bayesian network, and fram approaches," *Journal of Loss Prevention in the Process Industries*, vol. 45, pp. 88–101, 2017.

[4] O. el Ariss, D. Xu, and W. E. Wong, "Integrating safety analysis with functional modeling," *IEEE Trans. Syst. Man Cybern. Part A*, vol. 41, no. 4, pp. 610–624, 2011.