A Pattern-based Methodology for Reliability Assessment of Safety Instrumented Systems

Huixing Meng
LIX
École Polytechnique
Palaiseau, France
huixing.meng@polytechnique.edu

Leïla Kloul
DAVID
Université de Versailles
St-Quentin-en-Yvelines
leila.kloul@uvsq.fr

Antoine Rauzy
MTP
Norwegian University of
Science and Technology
antoine.rauzy@ntnu.no

***Abstract*—Safety Instrumented Systems (SIS) act as important safety barriers in industrial systems for preventing hazardous accidents. It is therefore significant to study the reliability issues of SIS. As a matter of fact, SIS have common behaviors such as periodic test policies to discover dangerous undetected failures. Modeling patterns capitalize the experience from modeling SIS. By reusing modeling patterns, modeling mission can be simplified when assessing reliability and availability of systems. Few studies related to SIS have been conducted on patterns for reliability assessment. This paper proposes a pattern-based methodology for reliability assessment of SIS. To demonstrate the applicability, the proposed methodology is applied on an emergency depressurization system provided in an ISO technical report (ISO/TR 12489). The comparison is performed between results obtained using given modeling patterns and the ones from ISO/TR 12489. It is shown that the pattern-based methodology can serve as an effective tool for modeling SIS in a modular way.**

I. INTRODUCTION

Safety Instrumented Systems (SIS) play an important role in industrial plants for preventing hazardous accidents. These systems are composed of sensors (e.g. pressure sensors), logic solvers (e.g. programmable logic controllers), and final elements (e.g. isolation valves). Logic solvers translate signals transmitted from sensors into decisions made on final elements. SIS have attracted a lot of attention from various industrial sectors. Associated standards are proposed in specific industries, such as the process industry, the nuclear power industry, the machinery industry, the automotive systems, as well as the railway systems. The main standard is IEC 61508 [1]. Sound performance of SIS is crucial for Equipments Under Control (EUC). It is therefore significant to study the reliability issues of SIS.

Reliability studies of SIS have been conducted tremendously (see e.g. [2]–[5]). Many aspects related to SIS have been investigated, including proof tests, k-out-of-n voting structures, common cause failures, spurious failures, human and organizational factors, uncertainty, and optimization issues.

Models and modeling experience are expected to be capitalized, otherwise, the modeling activity is hardly profitable. Patterns can be utilized for reusing the stabilized knowledge. Reliability studies can benefit from reusing modeling patterns. However, few studies have been carried out on modeling patterns for reliability assessment of SIS.

The pattern was initially proposed in civil engineering [6]. The concept was adopted in software engineering subsequently as the design pattern [7]. This one promotes design reuse, conforms to a literary style, and defines a vocabulary for discussing design [8].

A modeling pattern is a general means allowing to capture the frequently recurrent component and subsystem behaviors in industrial systems. Some researchers try to provide a general framework of reusing patterns. The pattern based system engineering was proposed [9], whose procedure includes the pattern definition and the system development with patterns [10]. The reuse of systems and subsystems is a common practice in safety-critical systems engineering [11]. To reuse system behaviors, we need to standardize the representation of reusable components and figure out the way they exchange information [12]. The whole point of a pattern is to reuse, rather than to reinvent [8].

An advantage of high-level modeling languages, like AltaRica [13], [14], is to reuse models of components or even systems [13]. The AltaRica modeling language is especially well suited for safety analyses [13], [14]. The AltaRica language is introduced in IEC 61508 as a technique for calculating the probabilities of hardware failures in SIS [1]. The language is also mentioned in ISO/TR 12489 [2].

To reuse modeling patterns, a methodology is the prerequisite when assessing reliabilities of SIS. Two benefits are expected with such a particular procedure: first, one can follow steps to analyze the reliability of a SIS via modeling patterns; second, people can propose their own pattern-based methodology in a similar way.

In this article, we develop a pattern-based methodology for reliability assessment of SIS. We classify modeling patterns into different categories. Proposed modeling patterns are implemented with the AltaRica 3.0 modeling language. The methodology is tested with a SIS in ISO/TR 12489.

The rest of this paper is organized as follows. Section II reviews related works. Section III is dedicated to modeling patterns extracted from SIS in ISO/TR 12489. Section IV develops a pattern-based methodology for reliability assessment of SIS. Section V studies an emergency depressurization system to illustrate the application of the proposed methodology. Finally, Section VI concludes this work.

978-1-5386-3403-5/17/$31.00 ©2017 IEEE

II. RELATED WORKS

Patterns have been discussed in reliability and safety domains [15]. Patterns related to accident analyses are investigated in traffic domain [16] and industrial plants [17], whereas these studies employ statistical methods to discover patterns of accident causes. The dependability pattern is proposed in [10]. It is defined as the description of a particular recurring dependability problem that arises in specific contexts and presents a well-proven generic scheme for its solution. Resilience design patterns are raised to meet the demand of extreme-scale high-performance computing systems [18].

From the modeling experience of several aircraft systems using AltaRica Data-Flow language, Safety Architecture Patterns (SAP) are proposed to simplify modeling missions [19]. SAP are component assemblies used to ensure the safety of architectures [19]. The application of SAP can be found in the avionics domain [19], [20]. Unlike their work [19], first, we use the AltaRica 3.0 language, which has a different mathematical foundation. The mathematical backgrounds of AltaRica Data-Flow and AltaRica 3.0 are mode automata [21] and guarded transition systems [22], separately. Second, we propose patterns for modeling SIS aiming in process industry. However, their work primarily locates in aviation industry. Third, they mainly proposed the structured collection of redundancy based architecture patterns. But we try to describe behavioral, flow propagation, and coordination characteristics of SIS with modeling patterns.

In a recent work [23], we propose the modeling patterns for production-performance analyses. We apply proposed modeling patterns on a practical offshore installation. The two sets of modeling patterns (in [23] and this article) share some patterns, that is, CorrectiveMaintenance, SERIES, PARALLEL, and KooN (k-out-of-n). However, most of patterns are different, which include patterns for performance analyses of production systems and patterns for reliability assessment of SIS.

Few studies related to patterns of SIS have been conducted. Related works can be found in [2], [24], where the Reliability Block Diagram (RBD) driven Petri Nets (PN) are proposed for reliability analyses. The readability of PN is improved by means of RBD.

III. MODELING PATTERNS

A Modeling Pattern (MP) is a general means allowing to capture the frequently recurrent component and subsystem behaviors in process industry. Modeling patterns can be classified according to their purpose, which reflects what a modeling pattern works for. They can have either behavioral, flow propagation, and coordination purpose. Behavioral Patterns (BP) describe the basic behaviors of a component. For instance, the repairable behavior is regarded as a basic character in SIS. Flow Propagation Patterns (FPP) depict the flow propagations inside or between components. Coordination Patterns (CP) represent cooperations or synchronizations in a system, such as repairable units and repair crews.

We choose SIS in ISO/TR 12489 as our running examples. This is because these architectures are general enough to cover most of safety systems [2]. In addition, these systems are representative of most of reliability studies of safety systems performed in petroleum, petrochemical, and natural gas industries, as well as in other industries [2].

A. Behavioral Patterns

In this part, we introduce five BP, as shown in Figure 1, which mainly capture shared component behaviors.

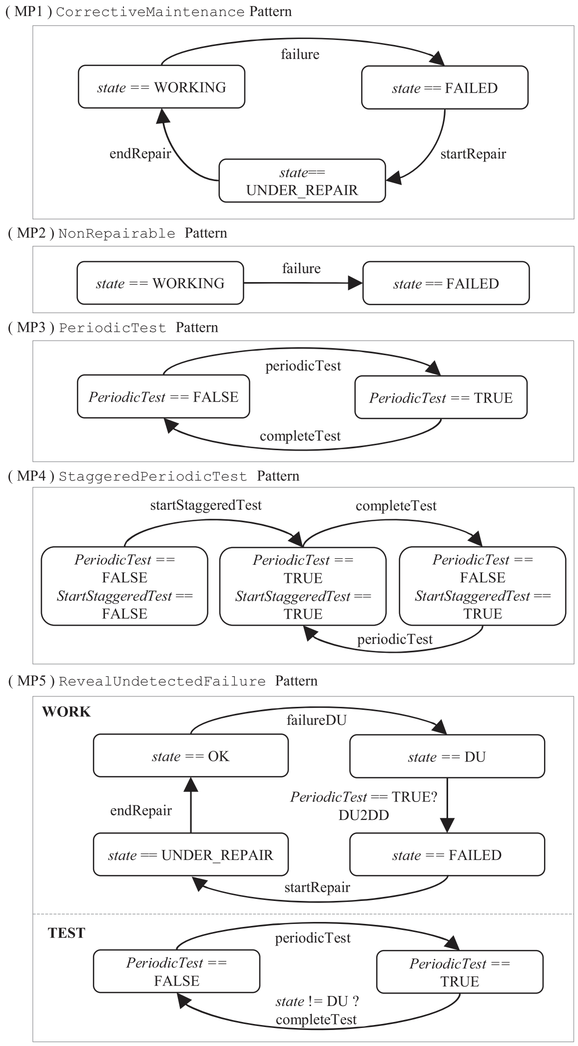

Fig. 1. Behavioral Patterns.

(1) `CorrectiveMaintenance` pattern (Figure 1, MP1): it models components which can be repaired after failure. The component is initially working (*state* == `OK`). Once a failure occurs, the component falls into `FAILED` state. When the corrective maintenance team is available, the component state becomes `UNDER_REPAIR`. Finally, the component returns to the initial state once the repair operation is finished. This pattern is used to model Dangerous Detected (DD) failures. DD failures are detected a short time after their occurrence by automatic diagnostic testing [3].

(2) `NonRepairable` pattern (Figure 1, MP2): it models components which cannot be repaired after failure. The component is initially in `OK` state. Once a failure occurs, the component becomes `FAILED`. In SIS, Dangerous Undetected (DU) failures are preventing activation on demand and can be revealed only by periodic tests (i.e., proof tests) [3]. Part of DU failures cannot be covered by imperfect periodic tests (i.e., the proof test coverage $< 100\%$), such uncovered DU failures can be modeled using this pattern. The rest part of DU failures are covered by periodic tests, which are modeled by means of the following pattern.

(3) `PeriodicTest` pattern (Figure 1, MP3): it models the periodic test which can detect DU failures. Periodic tests are conducted at predefined intervals and durations.

(4) `StaggeredPeriodicTest` pattern (Figure 1, MP4): it models the staggered periodic test, which is thought to allow obtaining higher availability than simultaneous tests. Compared with a reference periodic test, the duration of the first test interval in the staggered periodic test is different from the duration of following test intervals. Initially, the *startStaggeredTest* is triggered. Subsequently, the rest of the pattern architecture becomes similar to the `PeriodicTest` pattern.

(5) `RevealUndetectedFailure` pattern (Figure 1, MP5): it models the process to detect DU failures and is based on the `CorrectiveMaintenance` and `PeriodicTest` patterns. Three issues of this pattern deserve to be underlined: first, DU failures can only be discovered once the *PeriodicTest* is true; second, the periodic test can be completed only after DU failures are detected; third, revealed DU failure works following the `CorrectiveMaintenance` pattern.

B. Flow Propagation Patterns

Flow Propagation Patterns (FPP) depict flow propagations inside and between components. In the following, we illustrate five FPP, as shown in Figure 2.

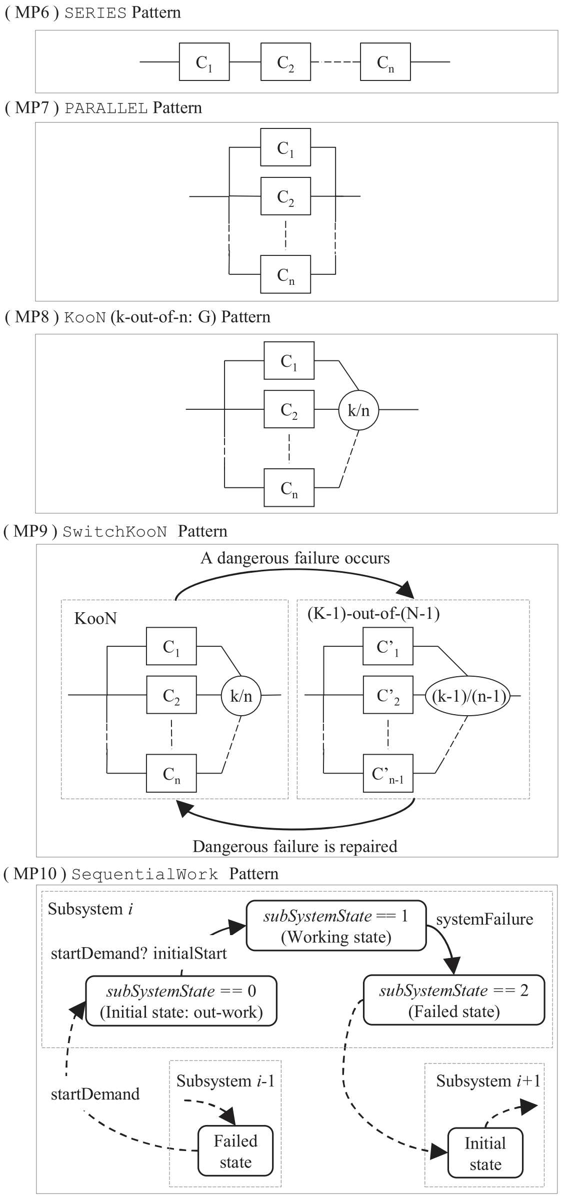

Fig. 2. Flow Propagation Patterns.

(6) `SERIES` pattern (Figure 2, MP6) describes the series structure, which models series connection of several basic patterns. The average unavailability of the `SERIES` pattern $\bar{U}_{\text{SERIES}}$ is:

$$\bar{U}_{\text{SERIES}} = 1 - (1 - \bar{u}_1)(1 - \bar{u}_2) \cdots (1 - \bar{u}_n) \qquad (1)$$

where $\bar{u}_1$, $\bar{u}_2$, $\cdots$, $\bar{u}_n$ are average unavailabilities of components C_1, C_2, $\cdots$, C_n, respectively.

(7) `PARALLEL` pattern (Figure 2, MP7) depicts the parallel structures. It models the parallel connection of several `SERIES` patterns. The average unavailability of the `PARALLEL` pattern $\bar{U}_{\text{PARALLEL}}$ is:

$$\bar{U}_{\text{PARALLEL}} = \bar{u}_1 \bar{u}_2 \cdots \bar{u}_n \qquad (2)$$

where $\bar{u}_1$, $\bar{u}_2$, $\cdots$, $\bar{u}_n$ are average unavailabilities of components C_1, C_2, $\cdots$, C_n, respectively.

(8) `KooN` (k-out-of-n: G) pattern (Figure 2, MP8) describes the structure which works when at least k of the total number n of items must be functioning. The average unavailability of the `KooN` pattern $\bar{U}_{\text{KooN}}$ is:

$$\bar{U}_{\text{KooN}} = 1 - \sum_{x=k}^{n} \binom{n}{x} (1 - \bar{u})^x \bar{u}^{n-x} \qquad (3)$$

where components in KooN are usually identical, and $\bar{u}$ is the average unavailability of each component. Some typical configurations of KooN structure are 1oo1 (i.e. single item), 1oo2, 2oo2, and 2oo3 [1].

(9) `SwitchKooN` pattern (Figure 2, MP9) depicts the behavior of switching a KooN structure into (K-1)-out-of-(N-1) structure when a DD or DU failure occurs. Once the

failure is repaired, the structure is normally restored to KooN structure.

The switched configuration, (K-1)-out-of-(N-1), can increase the system availability. If there is no such a switch, the structure is supposed to work as a K-out-of-(N-1) structure after a failure. According to Equation (3),

$$\bar{U}_{\text{(K-1)-out-of-(N-1)}} - \bar{U}_{\text{K-out-of-(N-1)}} = -\binom{n-1}{k-1}(1-\bar{u})^{k-1}\bar{u}^{n-k} \tag{4}$$

where $\bar{U}_{\text{(K-1)-out-of-(N-1)}}$ and $\bar{U}_{\text{K-out-of-(N-1)}}$ are the unavailabilities of (K-1)-out-of-(N-1) and K-out-of-(N-1) structures, respectively.

Since $-\binom{n-1}{k-1}(1-\bar{u})^{k-1}\bar{u}^{n-k}$ is a negative number, $\bar{U}_{\text{(K-1)-out-of-(N-1)}} < \bar{U}_{\text{K-out-of-(N-1)}}$. That is, the availability of the (K-1)-out-of-(N-1) structure increases after switch, when compared with the K-out-of-(N-1) structure.

Typically, if a dangerous failure (DD or DU) occurs in a 2oo3 structure, the logic solver changes the policy from 2oo3 to 1oo2.

(10) `SequentialWork` pattern (Figure 2, MP10) depicts the multiple SIS which work in a sequential order.The failed state of the previous subsystem $i-1$ triggers the successive subsystem i. This one is initially out of work (*subSystemState* == 0). If the trigger action (startDemand) from subsystem $i-1$ is perfect, the subsystem i becomes working (*subSystemState* == 1). If the subsystem i fails (*subSystemState* == 2), it can trigger the working of subsystem $i+1$. Note that if the trigger action is perfect, `SequentialWork` is equivalent to the `PARALLEL` pattern.

C. Coordination Patterns

Coordination Patterns (CP) represent cooperations or synchronizations in a system.

(11) `Repairable unit/Repair crew Coordination` pattern (Figure 3): it models limited repair crews in SIS. The working state of the repair crew (*RepairCrewWork*) is FALSE initially. If the number of busy repair crews (*numberBusyCrew*) is smaller than the total number of repair crews (*totalNumberCrew*) and a repair is required by a repairable unit, the repair is started. Simultaneously, 1 is added to *numberBusyCrew*. Adversely, 1 is decreased to *numberBusyCrew* when a repair is completed.

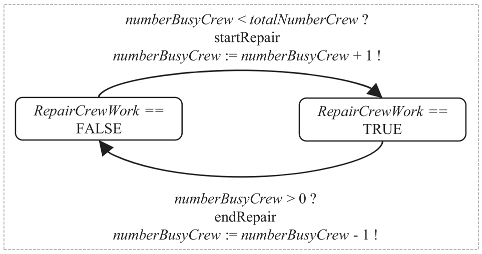

Fig. 3. Modeling pattern (MP11): `Repairable unit/ Repair crew Coordination`.

IV. PROPOSED METHODOLOGY

Figure 4 describes the methodology to model SIS using modeling patterns. This methodology is composed of four steps: classification, pattern-based model, AltaRica 3.0 model, and experimental results. We take typical application (TA) 1-1 in ISO/TR 12489 [2] as an example to illustrate this methodology. As a basic architecture of SIS, TA 1-1 is formed by a pressure sensor, a logic solver, and an isolation valve working in series.

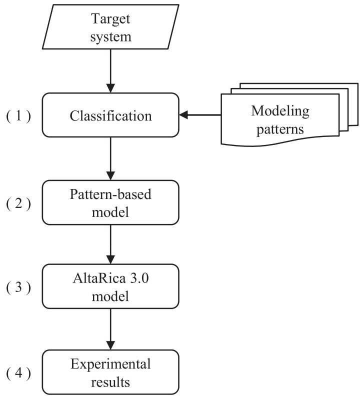

Fig. 4. Pattern-based methodology for reliability assessment of safety instrumented systems.

(1) *Classification*: In this step, we identify units to be modeled and recognize corresponding modeling patterns. The target system is initially decomposed into components and subsystems. We identify modeling patterns that are required to construct these components and subsystems.

Two components are modeled in TA 1-1, where the protected system is shut down during periodic tests and repairs. Thus the activities related to the maintenance/repair are negligible when calculating the system unavailability. Since the system unavailability of TA 1-1 is only generated by DU failures, thus the logical solver (which only has DD failures) has not been considered. The pressure sensor and isolation valve are modeled by the `RevealUndetectedFailure` pattern. These two components work in series, thus SERIES pattern is used as well.

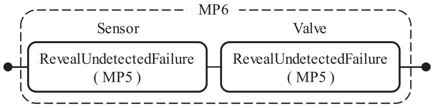

Fig. 5. Pattern-based model of the typical application 1-1 in ISO/TR 12489.

(2) *Pattern-based model*: Based on classification results, a pattern-based model can be obtained. This model is illustrated with the form of schematic diagrams. That is, we use such diagrams to exhibit classification results. The pattern-based model of TA 1-1 is shown in Figure 5. The pattern-based model is prepared for constructing the concrete model with a modeling language.

(3) *AltaRica 3.0 model*: AltaRica 3.0 modeling language is employed to model safety instrumented systems. The pattern-based model can be implemented with AltaRica 3.0.

(4) *Experimental results*: The obtained AltaRica 3.0 model is firstly translated and flattened into a GTS (Guarded Transition Systems) model. Subsequently, experimental results are acquired by analyzing the GTS model with the stochastic simulator [25], [26].

V. CASE STUDY

In order to validate the solidity of the proposed approach, we have modeled all SIS (13 systems with different architectures and assumptions) in ISO/TR 12489 with the proposed methodology and modeling patterns. The results applying proposed approach agree rather well with those from ISO/TR 12489. Because of the limited length of the paper, we consider an Emergency DePressurization (EDP) system (Figure 6) of a hydrocracking unit in ISO/TR 12489 as a case study.

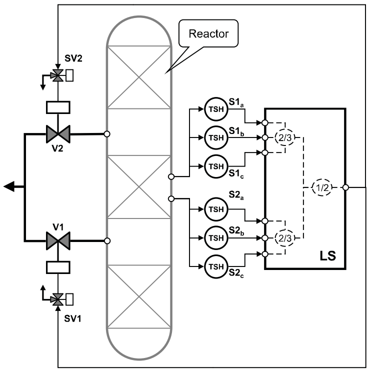

Fig. 6. An emergency depressurization (EDP) system [2].

The EDP system is composed of two groups of temperature sensors (S1a, S1b, and S1c; S2a, S2b, and S2c) organized in 2oo3, one Logic Solver (LS) and two corresponding isolation Valve (V1 and V2) in parallel and piloted by two corresponding Solenoid Valves (SV1 and SV2). This safety system aims to quickly depressurize the reactor when the temperature increases and reaches a predetermined threshold, thus to avoid a runaway of the exothermic chemical reaction.

The assumptions used for the EDP system are:

- DD and DU failures of a given component are independent.
- Constant failure rates are assumed.
- Components are as good as new after repairs.
- Periodic tests are performed when the reactor is stopped.
- Installation is paused during repair of DU failures.
- Installation is shut down during periodic tests and repair of the logic solver.
- Failures that are not covered by periodic tests will not be detected and repaired.
- The 2oo3 logic of a group of sensors is switched to 1oo2 in case of one dangerous detected failure in the group.

In the following, we illustrate how to assess the reliability of the EDP system when applying the pattern-based methodology in Figure 4.

(1) *Classification*: We identify the modeling patterns matching components and subsystems in EDP system. Modeling patterns classification for EDP system is provided in Table I.

TABLE I
MODELING PATTERNS CLASSIFICATION FOR EDP SYSTEM.

Components/Subsystems	Modeling patterns
• S1a, S1b, S1c, S2a, S2b, S2c	MP1, MP2, MP5
• {S1a, S1b, S1c},{S2a, S2b, S2c}	MP8, MP9
• {S1, S2}	MP7
• LS, SV1, V1, SV2, V2	MP2, MP5
• {SV1, V1},{SV2, V2}	MP6

We employ a 2oo3 structure (S1a, S1b, and S1c) as an example to elaborate the results. Since DD and DU failures of a component are assumed to be independent in EDP system, the DD failure of a component (e.g., S1a) can be modeled using `CorrectiveMaintenance` pattern (MP1). Since the uncovered DU failure cannot be repaired, it is constructed with the `NonRepairable` pattern (MP2). The covered DU failure by periodic tests is considered with the `RevealUndetectedFailure` pattern (MP5). The subsystem composed by these three components, {S1a, S1b, S1c}, can be modeled by both `KooN` pattern (MP8) and `SwitchKooN` pattern (MP9). The two groups of 2oo3 structures, {S1, S2}, in the EDP system can be modeled with `PARALLEL` pattern (MP7). Note that S1 and S2 stand for the 2oo3 subsystems. The rest of classification results can be interpreted in the similar way.

(2) *Pattern-based model*: On the basis of results in Table I, we establish the pattern-based model of EDP system, as it is shown in Figure 7. Associated modeling patterns are assigned for each component/subsystem in the diagram. The pattern-based model simplifies the task of constructing the AltaRica 3.0 model.

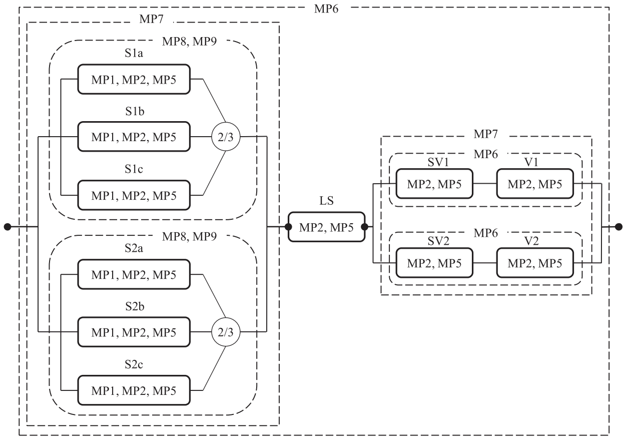

Fig. 7. Pattern-based model of the EDP system.

(3) *AltaRica 3.0 model*: In this step, we translate the pattern-based model of the EDP system into the corresponding AltaRica 3.0 model. Modeling patterns are firstly presented in the AltaRica environment. Subsequently, the AltaRica 3.0 model of the EDP system is constructed with identified modeling patterns.

(4) *Experimental results*: The mission time (length of histories) of this simulation experiment is $131,400$ h (15 years). The number of the Monte Carlo simulations (number of histories) is 10^6. The results comparison can be found in Table II. The AltaRica 3.0 (Stochastic simulator) and ISO/TR 12489 (Fault tree) give almost the same results, where the percentage difference is 1.14%.

TABLE II
EXPERIMENTAL RESULTS OF THE EDP SYSTEM.

Approaches	Average unavailability
Fault tree [2]	3.50E-4
AltaRica 3.0	3.46E-4

VI. CONCLUSION

This paper has presented a pattern-based methodology for reliability assessment of Safety Instrumented Systems (SIS). First, based on a series of SIS provided in ISO/TR 12489, a set of modeling patterns is proposed. Modeling patterns are categorized into behavioral patterns, flow propagation patterns, and coordination patterns. Second, a pattern-based methodology is put forward and illustrated with a simplified SIS. Eventually, the proposed methodology is tested with a complex SIS in ISO/TR 12489. The corresponding AltaRica model has been developed to assess the system reliability. The result obtained from AltaRica model using modeling patterns is in good agreement with that from ISO/TR 12489. It is concluded that the proposed methodology is capable of constructing targeted systems in a modular way.

Raised modeling patterns are based on a limited set of SIS. Even if they are declared to cover most of reliability studies [2], these patterns can be improved with new system behaviors. The current paper is restricted to study SIS and EUC (Equipments Under Control) separately. Further research may consider EUC as an integral part of SIS. New modeling patterns are therefore expected with such integrations.

REFERENCES

[1] IEC, “IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems,” 2010.

[2] ISO, “ISO/TR 12489 Petroleum, petrochemical and natural gas industries: Reliability modelling and calculation of safety systems,” 2013.

[3] M. Rausand, *Reliability of Safety-Critical Systems: Theory and Applications*. John Wiley & Sons, 2014.

[4] M. Rausand and A. Høyland, *System reliability theory: models, statistical methods, and applications*. John Wiley & Sons, 2004.

[5] Y. Dutuit, A. Rauzy, and J.-P. Signoret, “A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems,” *Proc. Inst. Mech. Eng. Part O-J. Risk Reliab.*, vol. 222, pp. 371–379, 2008.

[6] C. Alexander, *A pattern language: towns, buildings, construction*. Oxford University Press, 1977.

[7] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, *Design patterns: elements of reusable object-oriented software*. Addison-Wesley Professional, 1995.

[8] E. Gamma, “Design patterns—ten years later,” in *Software pioneers*. Springer, 2002, pp. 688–700.

[9] D. Cook and W. D. Schindel, “Utilizing MBSE patterns to accelerate system verification,” *INSIGHT*, vol. 20, no. 1, pp. 32–41, 2017.

[10] B. Hamid and J. Perez, “Supporting pattern-based dependability engineering via model-driven development: Approach, tool-support and empirical validation,” *J. Syst. Softw.*, vol. 122, pp. 239–273, 2016.

[11] A. Ruiz, G. Juez, H. Espinoza, J. L. de la Vara, and X. Larrucea, “Reuse of safety certification artefacts across standards and domains: A systematic approach,” *Reliab. Eng. Syst. Saf.*, vol. 158, pp. 153–171, 2017.

[12] N. Kajtazovic, C. Preschern, A. Höller, and C. Kreiner, “Towards pattern-based reuse in safety-critical systems,” in *EuroPLoP*. , 2014.

[13] T. Prosvirnova, “Altarica 3.0: a model-based approach for safety analyses,” Ph.D. dissertation, Ecole Polytechnique, Palaiseau, France, 2014.

[14] T. Prosvirnova, M. Batteux, P.-A. Brameret, A. Cherfi, T. Friedlhuber, J.-M. Roussel, and A. Rauzy, “The AltaRica 3.0 project for model-based safety assessment,” in *Proceedings of 4th IFAC Workshop on Dependable Control of Discrete Systems*, 2013, pp. 127–132.

[15] C. Preschern, N. Kajtazovic, A. Höller, and C. Kreiner, “Pattern-based safety development methods: overview and comparison,” in *EuroPLoP*. , 2014.

[16] Q. Guo, P. Xu, X. Pei, S. Wong, and D. Yao, “The effect of road network patterns on pedestrian safety: a zone-based bayesian spatial modeling approach,” *Accid. Anal. Prev.*, vol. 99, pp. 114–124, 2017.

[17] A. Verma, S. D. Khan, J. Maiti, and O. Krishna, “Identifying patterns of safety related incidents in a steel plant using association rule mining of incident investigation reports,” *Saf. Sci.*, vol. 70, pp. 89–98, 2014.

[18] S. Hukerikar and C. Engelmann, “Resilience design patterns - a structured approach to resilience at extreme scale,” Oak Ridge National Laboratory, Tennessee, US, Tech. Rep., 2016.

[19] C. Kehren, “Motifs formels d’architectures de systèmes pour la sûreté de fonctionnement,” Ph.D. dissertation, Ecole nationale superieure de l’aeronautique et de l’espace, Toulouse, France, 2005.

[20] M. Morel, “Model-based safety approach for early validation of integrated and modular avionics architectures,” in *IMBSA, Munich, October, 2014*. LNCS, 2014, pp. 57–69.

[21] A. Rauzy, “Mode automata and their compilation into fault trees,” *Reliab. Eng. Syst. Saf.*, vol. 78, pp. 1–12, 2002.

[22] A. Rauzy, “Guarded transition systems: a new states/events formalism for reliability studies,” *Proc. Inst. Mech. Eng. Part O-J. Risk Reliab.*, vol. 222, no. 4, pp. 495–505, 2008.

[23] H. Meng, L. Kloul, and A. Rauzy, “Modeling patterns for performance analyses of offshore production systems,” in *The Proceedings of the 27th International Ocean and Polar Engineering Conference*. San Francisco: ISOPE, June 2017.

[24] J.-P. Signoret, Y. Dutuit, P.-J. Cacheux, C. Folleau, S. Collas, and P. Thomas, “Make your Petri nets understandable: Reliability block diagrams driven Petri nets,” *Reliab. Eng. Syst. Saf.*, vol. 113, pp. 61–75, 2013.

[25] B. Aupetit, M. Batteux, A. Rauzy, and J.-M. Roussel, “Improving performances of the AltaRica 3.0 stochastic simulator,” in *ESREL*, Zurich, Switzerland, 2015.

[26] M. Batteux and A. Rauzy, “Stochastic simulation of altarica 3.0 models,” in *ESREL*, Amsterdam, Netherlands, 2013.