Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Atteindre un SIL 3 permanent sans compromettre la disponibilté de production

Reaching a permanent SIL3 target without compromising production availability

BERNE Nicolas
LGM
Bordeaux
nicolas.berne@lgm.fr

CLAVE Nicolas
TotalEnergies
CSTJF (Pau)
nicolas.clave@totalenergies.com

I. RÉSUMÉ / SUMMARY

***Résumé* —** Les systèmes de protection d'intégrité élevée (HIPS en anglais) agissent comme barrières ultimes et uniques pour protéger les installations pétrolières et gazières contre des scénarios dangereux (notamment le scénario de surpression) entraînant des événements aux conséquences « catastrophiques » ou « désastreuses » selon le référentiel TotalEnergies. Dans ces circonstances, la règle interne de TotalEnergies spécifie qu'un « SIL3 permanent » (SIL = Niveau d'Intégrité de Sécurité, selon la norme IEC 61508/511) doit être atteint pour les HIPS, c'est-à-dire PFD(t) < 10^{-3} pendant toute la période de calcul (PFD = Probabilité de Défaillance à la Demande).

Cet objectif n'étant pas atteint pour le système étudié ici, les options conventionnelles pour atteindre la cible de SIL entraînent soit une augmentation des dépenses d'exploitation (OPEX) et des pertes de production (augmentation de la fréquence des tests), soit une augmentation des dépenses d'investissement (CAPEX) (ajout d'une troisième valve).

Les conditions de fonctionnement et la configuration du système nous ont amenés à utiliser les réseaux de Petri pour sa modélisation (selon le technical report ISO/TR 12489 Figure 2). Cela nous a permis d'évaluer une troisième option désignée sous le nom de « fréquence de test adaptée ». Elle consiste à augmenter la fréquence de test uniquement lorsque le système fonctionne en mode dégradé suite à la détection de l'une ou plusieurs défaillances (capteurs ou valves).

La « fréquence de test adaptée » s'est avérée être une solution efficace pour atteindre le niveau de SIL requis et pour réduire l'impact sur la disponibilité par rapport à une fréquence de test fixe augmentée.

En ce qui concerne l'approche en elle-même, modifier la stratégie de test d'un système de sécurité dans des conditions données pendant/à l'intérieur de la simulation ne peut être modélisé que par des techniques de modélisation dynamique. Les réseaux de Petri étant l'un des outils les plus flexibles et puissants, il a été facile de traiter cette spécificité correctement.

Mots-clefs — Petri nets, PFD, Disponibilité, HIPS, Test, SIL, Sécurité

***Abstract* —** High Integrity Protection Systems (HIPS) act as sole and ultimate barriers to protect the Oil & Gas installations against hazardous scenarios (notably overpressure scenario) resulting in events with “Catastrophic” or “Disastrous” consequences as per TotalEnergies referential. In these circumstances, TotalEnergies internal rule specifies that a “permanent SIL3” (SIL = Safety Integrity Level, as per IEC 61508/511) shall be achieved for the HIPS, i.e. PFD(t) < 10^{-3} all over the calculation period (PFD = Probability of Failure upon Demand).

This objective being not met for the particular system under study here, the conventional options to reach the SIL target induce either an OPerational EXpenditures (OPEX) increase and production shortfalls (frequency test increase) or a CAPital EXpenditures (CAPEX) increase (addition of a third valve).

The operating conditions and systems configuration led us to use Petri nets for modelling of the system (according to ISO/TR 12489 Figure 2). This allowed to assessing a third option designated as “adapted test frequency”. It consists in increasing the test frequency only when certain degraded modes of the system are reached further to the detection of one or several failures (sensors or valves).

The “adapted test frequency” appeared to be an efficient solution to reach the required SIL level and to reduce impact on availability compared to a fixed increased test frequency.

Regarding the approach it-self, modifying the testing strategy of a safety system under given conditions during/inside the simulation is something that can be modelled only through dynamic modelling techniques. Petri nets being one the most flexible and powerful one, it was quite easy to address that specificity properly.

Keywords — Petri nets, PFD, Availability, HIPS, Test, SIL, Safety

II. INTRODUCTION

TotalEnergies, a leading global energy company, operates across various segments of the petroleum industry. With a presence in over 130 countries and nearly 100,000 employees, TotalEnergies is a major player in the energy landscape.

- Exploration, Development, and Production
  In the upstream sector (commonly referred to as “amont”), TotalEnergies engages in exploration, development, and production of hydrocarbons. This includes oil and natural gas exploration, as well as activities related to coal, gas, and emerging energy sources. Operationally, TotalEnergies covers:
  1. Oil Exploration and Production: Prospecting, exploration, and extraction of oil.
  2. Natural Gas Exploration and Production: Exploration, production, liquefaction (for liquefied natural gas), transportation, and commercialization.
  3. Alternative Energy Cycles: TotalEnergies participates in solar equipment manufacturing, coal-steam production for thermal power plants, nuclear projects, and renewable energy generation.
- Downstream Operations
  In the downstream sector (“aval”), TotalEnergies focuses on petroleum products. Key operational areas include:
  1. Maritime Transport: Ensuring safe transportation of petroleum products by sea.
  2. Pipeline Transport: Efficient movement of products through pipelines.
  3. Refining: Processing crude oil into refined products.
  4. Distribution: Supplying refined products to end-users.
  5. Market Activities: Trading and market-related operations.
- Chemistry and Sustainability
  TotalEnergies is not limited to fossil fuels. It is a significant player in the chemical industry. Operationally, it covers:
  1. Basic Chemistry: This includes petrochemicals (such as olefins and aromatics) and their derivatives (polyethylene, polypropylene, and polystyrene). Additionally, TotalEnergies manufactures fertilizers.
  2. Renewable Energy: The company actively supports the growth of renewable energies, including solar and biomass.

Regarding Exploration and Production activities, offshore exploration expands and the installation of Safety Instrumented Systems (SIS) on subsea units becomes increasingly common. These systems monitor critical parameters (pressure, flow, temperature…), detect anomalies, and ensure the safety of personnel and assets onshore and of the environment. TotalEnergies remains committed to advancing safety practices in its offshore operations.

LGM has been qualified by TotalEenergies for achieving Reliability studies of Safety Instrumented Function (SIF) and Production Availability Studies (PAS). Accordingly, both companies collaborate regularly and for many years on projects of all kinds.

The purpose of this communication paper is to present the results of one of these collaborations on an advanced reliability study performed on a subsea SIF. This study was carried out in the frame of the Absheron project located in the Caspian Sea. Indeed, TotalEnergies and SOCAR, the national oil company of Azerbaijan, have signed an agreement establishing the contractual and commercial terms for a gas and condensate field named Absheron discovered by TotalEnergies in 2011.

SIFs require periodic testing to ensure their proper functioning regarding response at the selected threshold at the sensor level, response time of the safety function and effectiveness of the barrier (leak test of the shutdown valve). These test operations are themselves dangerous operations (shutdown/restarts of the production system) and generate production shortfalls and loss of revenue. The test frequency shall as a consequence be optimized to ensure people and asset safety while limiting impact on production availability. The case presented here is a typical example where the use of Petri Nets has allowed to investigate alternative ways to conventional approaches to reach the reliability target, with the ambition to minimize the impact on production.

III. CONTEXT AND METHODOLOGY

A. Context

1) System description

High Integrity Protection Systems (HIPS) or High Integrity Pressure Protection Systems (HIPPS) act as sole and ultimate barriers to protect Oil & Gas installations. The aim is to protect equipment against hazardous scenarios resulting in events with "Catastrophic" or "Disastrous" consequences as per TotalEnergies referential. In most of the cases, the event under study is an overpressure scenario resulting from well shut-in pressure being largely higher than the design pressure of downstream equipment or flowline. In these circumstances, TotalEnergies internal rule specifies that a "permanent SIL3" (SIL = Safety Integrity Level, as per IEC 61508/511) shall be achieved for the HIPS, i.e. PFD(t) < 10^{-3} all over the calculation period (PFD = Probability of Failure upon Demand).

In the system under study presented here, the blocked outlet scenario necessitates 3 identical parallel subsea HIPSs to react to prevent overpressure within the 18-inch downstream flowline (each HIPS having then PFD(t) $\leqslant$ 3.3 x 10^{-4}).

The figure blow shows how the different wells are connected to the main flowline through Flow Line End Terminations (FLETs) and the location of the HIPPSs.

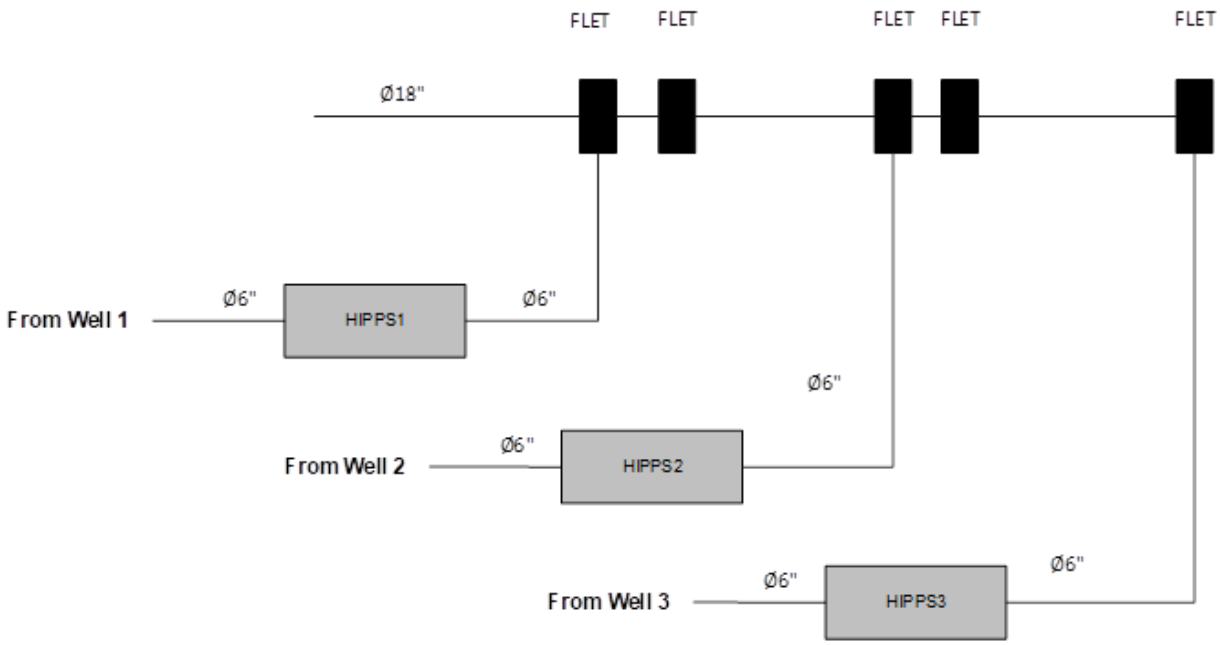

Fig. 1. System under study.

A FLET is a rigid structure made up of pipping and isolation valves that are normally open. These valves are not part of the SIFs under study.

The analysis was based on a HIPS configuration that was proven successful in meeting the objective over 2 years of operation, with a single HIPS composed of 6 pressure sensors, a logic solver and 2 emergency shutdown valves.

The figure below provides a detailed description of the HIPPSs to analyze that are installed on the 6-inch flowlines coming from the production wells and connected to the main flowline.

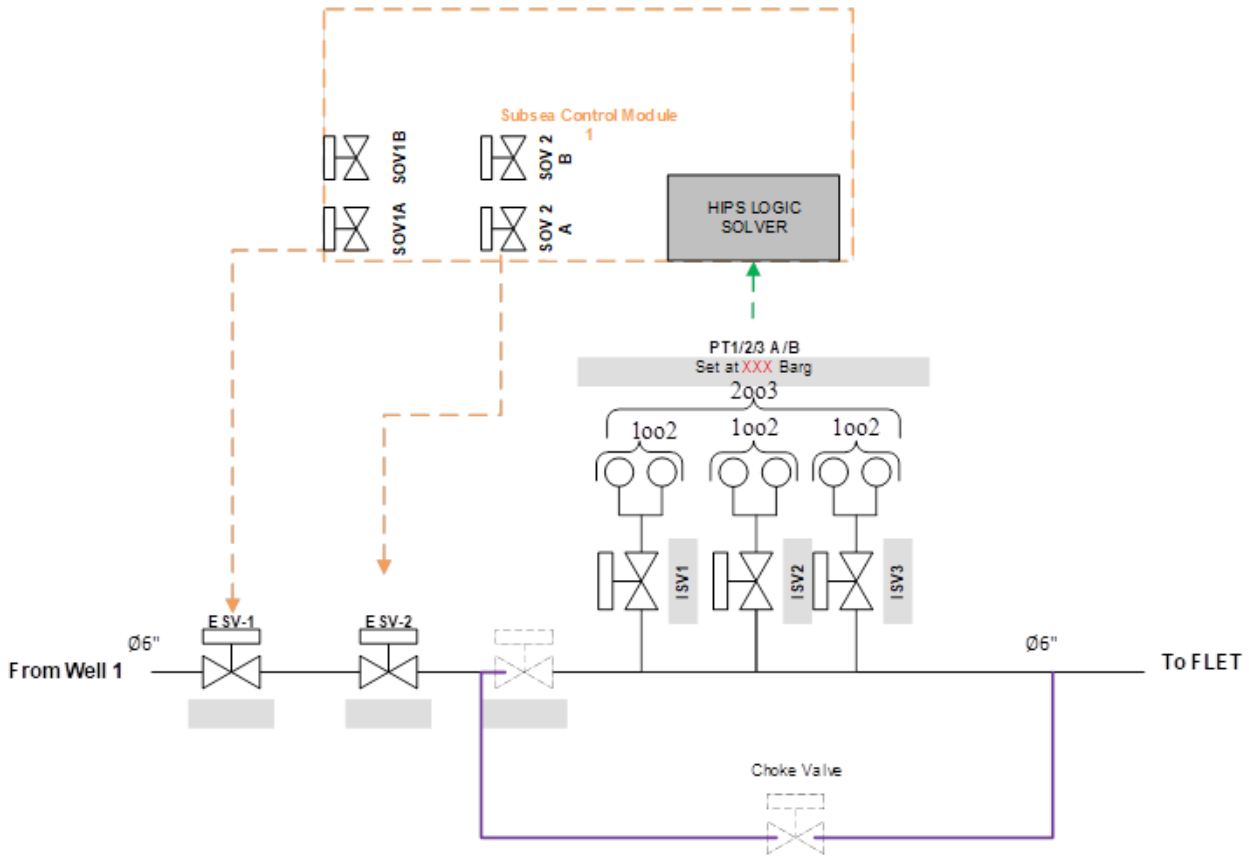

Fig. 2. High Integrity Protection System.

Upon confirmed detection of a high pressure by 2 of the 3 sets of sensors (2oo3 logic among the three sets, each set being composed of 2 sensors in 1oo2 logic), the HIPS logic solver closes the redundant Emergency Shutdown Valves (ESV) via deenergized to trip SOlenoid Valves (SOV).

2) Test policy

This system is fully tested once a year (including valve leak test after closure) with an intermediate function test every 6 months. During the tests of one pressure sensor set (function test), the remaining pressure sensor sets are reconfigured in 2oo2 logic. These tests allow to detect a portion of the Dangerous Undetected (DU) failures as defined in IEC 61508/511.

3) Detected failures reonfiguration and repair policy

Diagnostics on PT (Pressure Transmitter) is achieved by constantly comparing the readings between transmitter pairs and transmitter banks. In case of failure diagnosed on a PT for a given set of PTs, the failed set is inhibited and the top voting migrates from 2oo3 to 2oo2.
In case of PT's failure detection, its signal is ignored and voting is reconfigured until one set only is available. In that case production is stopped, the module for PT's and ESV will be replaced, (production will be stopped during approximately 52 weeks, time to bring the spares and the intervention vessel to the site).
If 1 of the 2 ESVs is tested and diagnosed as failed open, the second ESV must be fully tested. If it works, the system can continue on producing in degraded mode with only 1 operating ESV.

B. Choice of modelling technique

The use of Petri net modelling of the system in order to calculate PFD(t) was selected according to Figure 2 of ISO/TR 12489 (Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems) due to:

- The repair of the equipment being done under certain conditions (e.g. when 2 sensors out of 3 have failed);
- The replacement and intervention having a longer duration for subsea systems compared to standard onshore systems, implying the modelling of both dangerous detected and dangerous undetected failures;
- The system containing 39 components with 10 states per component, leading to a very large number of states of the system.

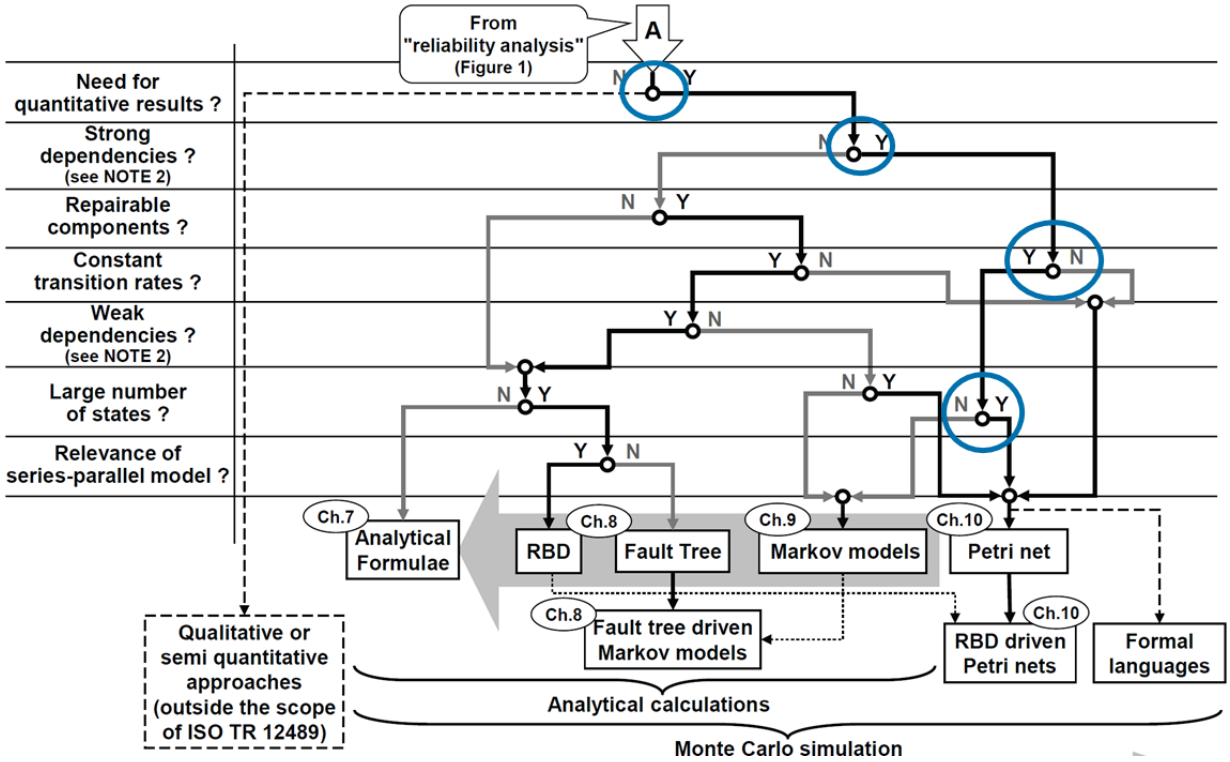

Fig. 3. ISO/TR 12489 Figure 2 – Overview of reliability modelling and calculation apporaches currently used.

IV. MODELLING AND CHALLENGES

A. Modelling

The Petri net model was structured in 4 layers built with the Petri module of GRIF (GRaphical Interface for reliability Forecasting), a technology of TotalEnergies:

1. State/failure mode of equipment;
2. State per equipment/sub-function with voting combinations;
3. 1 HIPPS – Combination of dangerous state;
4. Combination of the 3 HIPPS dangerous state.

Others Petri nets were built for mobilization of vessels and spare part management for replacement of failed components.

GRIF is a software suite developed by TotalEnergies for almost 40 years. It proposes more than 10 modules dedicated to reliability, availability and production availability calculations (fault trees, bowties, event trees, reliability block diagrams, Petri nets, etc.).

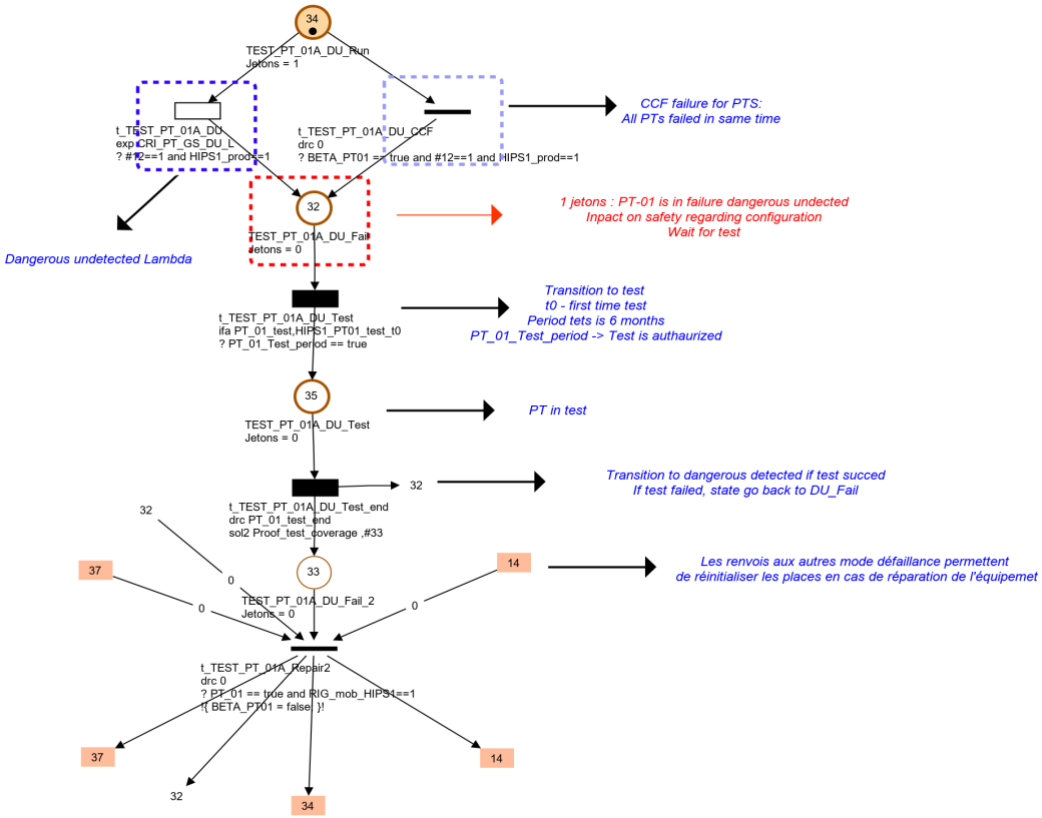

Fig. 4. Typical Petri net for modelling the Dangerous Undetected (DU) failures of a pressure sensor.

The transitions to test for all components (Pressure, sensors, logic solver, SOV's and ESV's) are modelled using a periodic test law, with a fixed parameter for the time of first test fire and a fixed parameter for the test period (respectively "HIPS1_PT01_test_t0" and "PT_01_test_HIPS1" in the example in Fig. 5).

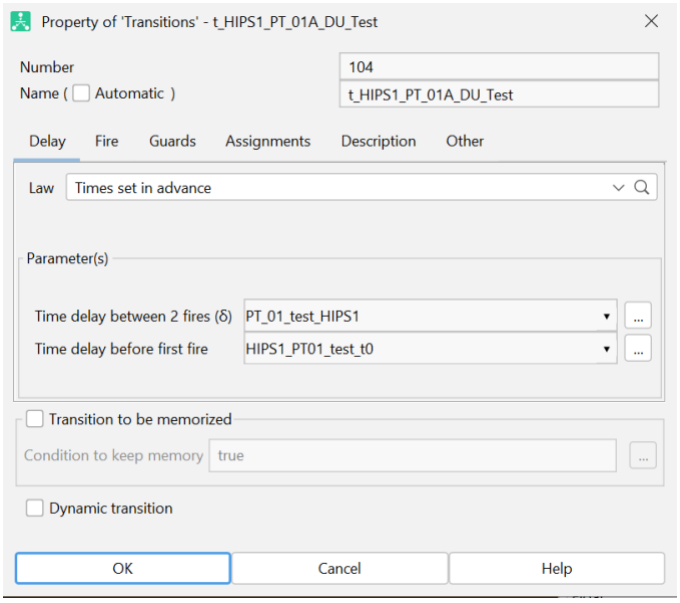

Fig. 5. Periodic test law used for a pressure sensor.

B. *First results*

The first run of calculations showed that the permanent SIL3 target was not met starting from Year 3 (compared to a potential operation of the system of 6 to 10 years). The "conventional" PFD_{avg} as defined in ISO 61508/511 target was not reached either due to the need for the 3 HIPS in parallel being successful and the long operation period (the system is designed for operation over 12 years, but its requirement to act as a safety system is not expected to remain after year 10 maximum).

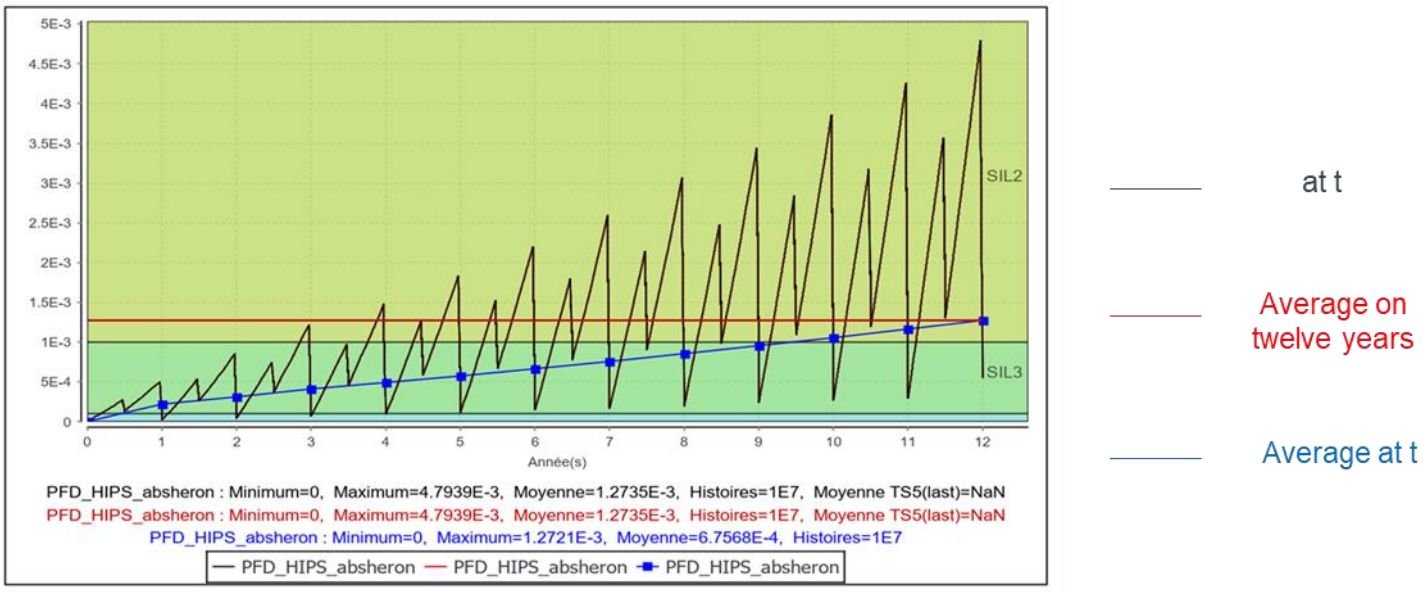

Fig. 6. Results with fixed 6 months function test and 1 year full test.

The effects of intermediate and annual function tests can be easily observed on the black curve above. The blue one ($PFD_{avg}(t)$) shows that the system remains SIL3 up to Year 9. At Year 10, PFD_{avg} is in the SIL2 zone (red line).

It is important to mention that the global increase of PFD(t) is due to the possibility to operate in degraded mode i.e. with 1 SOV or 1 ESV failed detected.

The options usually used to solve these issues and reach the SIL target are:

- Increasing the test frequency for valves and sensors, which increases Operational Expenditures (OPEX) and production shortfalls; or
- Adding a third emergency shutdown valve, which increases Capital Expenditures (CAPEX).

The flexibility of the dynamic simulation proposed by Petri nets under GRIF allowed to assess the efficiency of a third alternative designated as “adapted test frequency”. It consists in increasing the test frequency only when certain degraded modes of the system are reached further to the detection of one or several failures (Solenoid Valves or Emergency Shutdown Valves).

For the Emergency Shutdown Valves, the fixed parameter for the test period is replaced by a variable which allows to divide the frequency by 2 when the system has been detected as being under degraded mode.

This variable is a simple logical formula looking at the state of the system:

$$ite(HIPS1\_ESVSOV\_degraded\_mode==1,(4380./2.),4380.0) \quad (1)$$

meaning: if one ESV/SOV assembly of HIPS1 is in a degraded mode, then the test frequency is of 3 months (4,380 hours divided by 2), else the test frequency is of 6 months (4,380 hours).

V. OPTIONS COMPARISON

The adapted test frequency scenario was assessed as well as the third valve addition in order to provide to the project team the different results as a help for decision making.

A. Addition of a third valve

The SOV and ESVs being the most contributing element to safety function unavailability, the addition of a third valve has an immediate and substantial effect on the results.

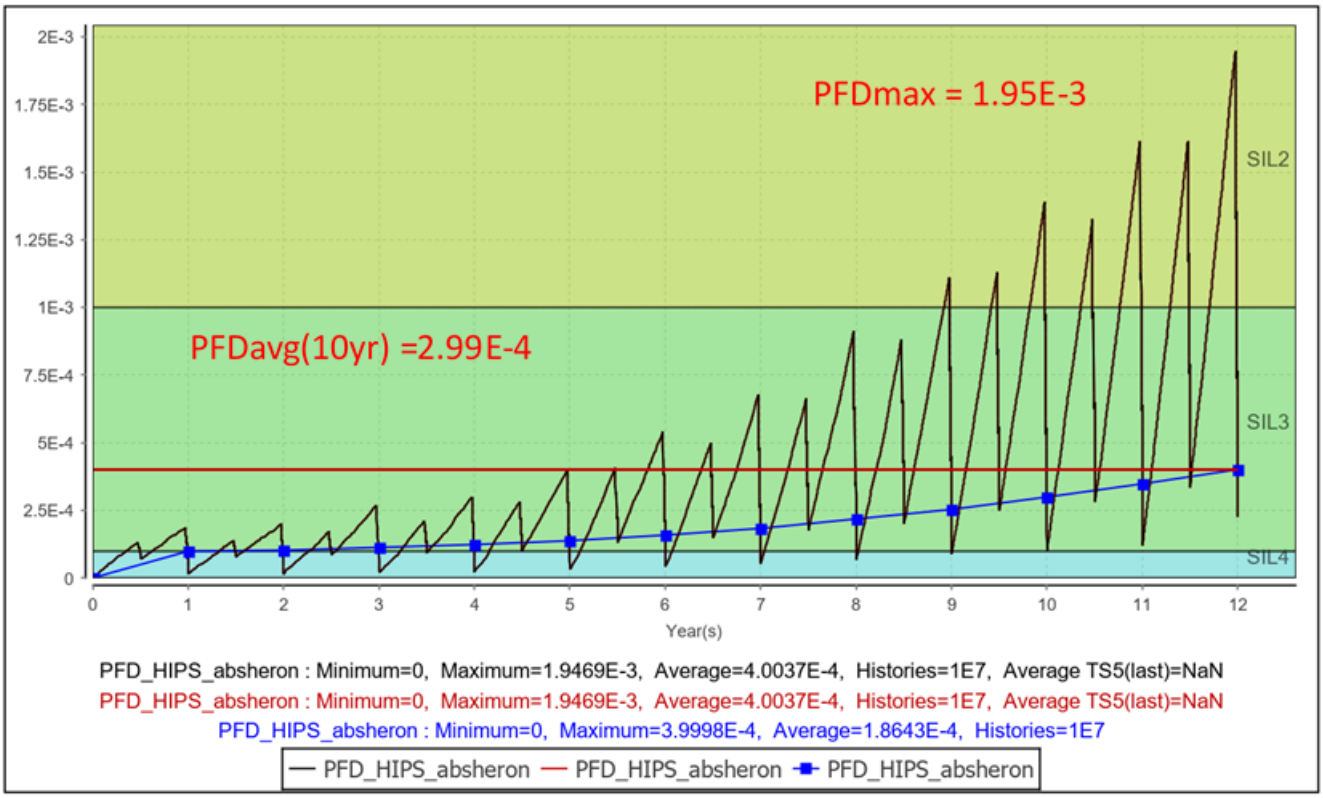

Fig. 7. Results with a third ESV.

B. Increase of test frequency when in degraded mode

In addition to the PFD curves, the Petri net modelling allows to calculate the probability of being in degraded mode and then to have to adjust the test frequency in order to meet the SIL target, increasing the project OPEX.

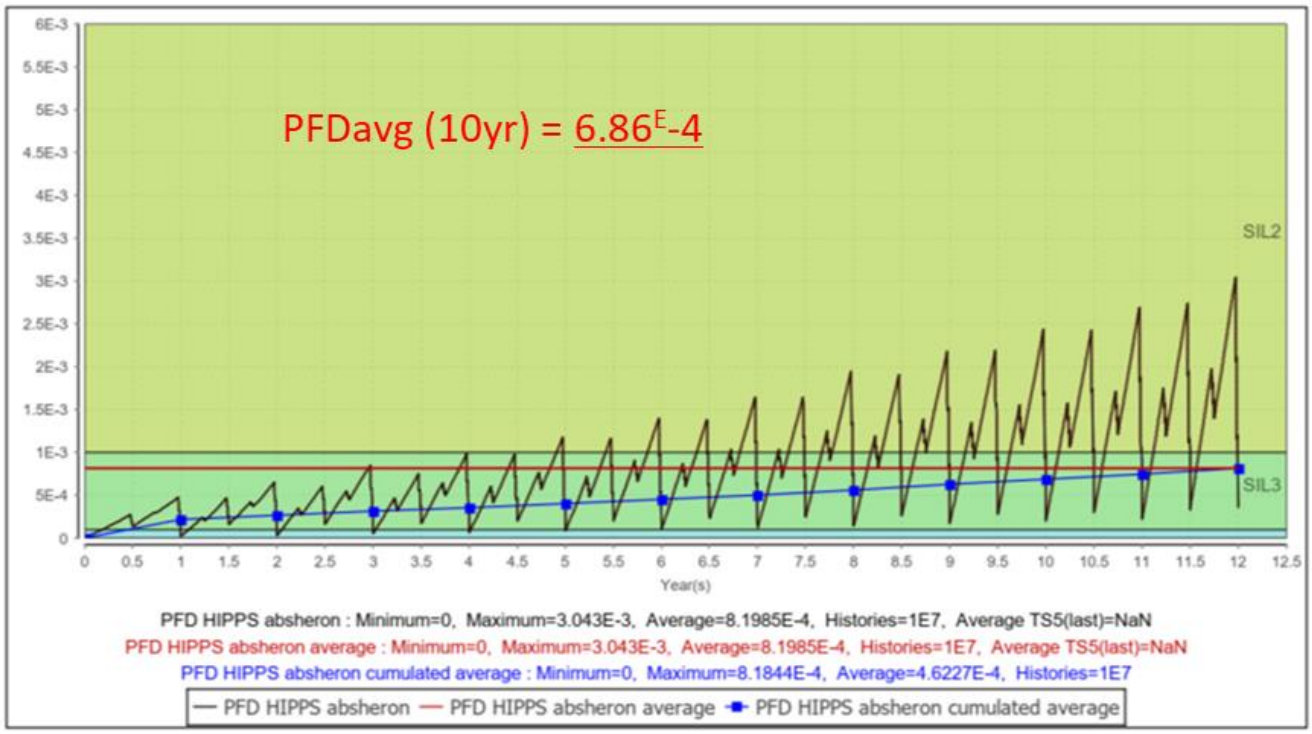

Fig. 8. Increase of test frequency in degraded mode.

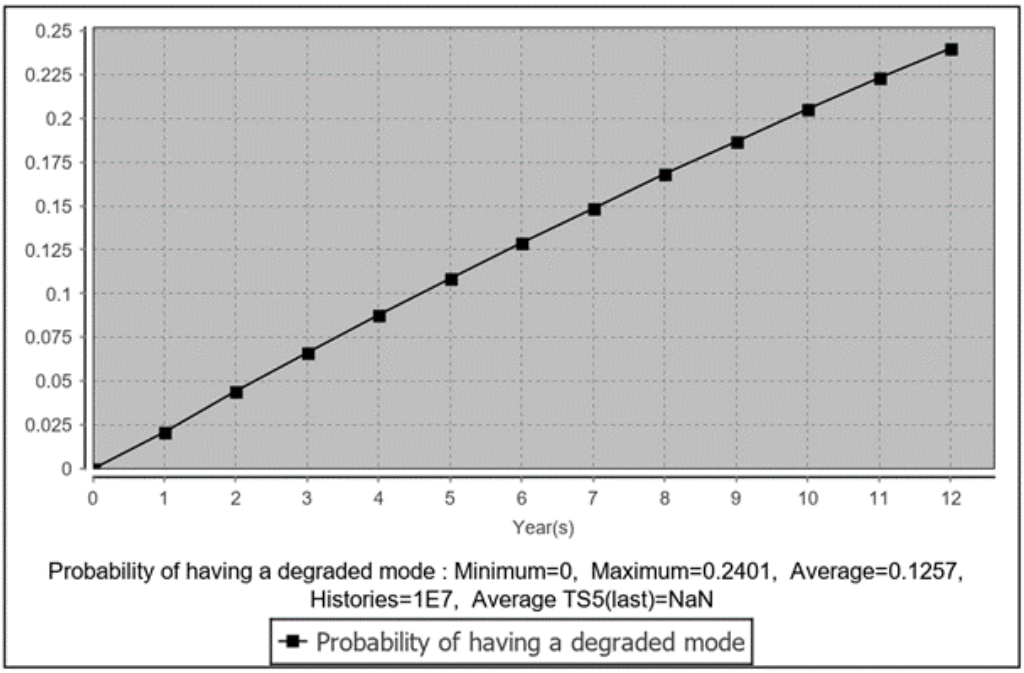

Fig. 9. Probability of being in degraded mode over 12 years.

This option allows reaching an acceptable SIL over 6 years (not permanent SIL 3 but time in SIL 2 area remaining acceptable) and to meet the IEC 61508/61511 criteria regarding the PFD average over 10 years. The duration for which the HIPS is required being under review, this provide valuable input to project decision process, having the possibility to assign a probability to the OPEX increase.

VI. CONCLUSION

Reaching a permanent SIL 3 as per TotalEnergies rule for 3 HIPS in parallel appears as a very challenging objective, which may not be met with conventional HIPS assemblies and test policies.

The “adapted test frequency” appeared to be an efficient solution to reach the required SIL level and to reduce the impact on availability compared to a fixed increased test frequency or adding a third Emergency Shutdown Valve. This solution and the results provided also allowed the project management to challenge the different options considering their relative impacts on OPEX and CAPEX.

Regarding the approach itself, modifying the testing strategy of a safety system under given conditions during/inside the simulation is something that can be modelled only through dynamic modelling techniques. Petri nets being one the most flexible and powerful one, it was quite easy to address that specificity properly.

The Petri nets model can as well be easily enriched with a system availability calculation, as all the states of the system are already modelled, which will provide additional input for options costs comparison by the project team.

References

[1] ISO/TR 12489, *Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems*, 2013

[2] IEC 61508:2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES). IEC. Geneva: Switzerland.

[3] IEC 61511:2023 SER. Functional safety - Safety instrumented systems for the process industry sector. All parts. IEC. Geneva: Switzerland.

[4] IEC 62551:2012. Analysis techniques for dependability — Petri nets techniques. IEC. Geneva: Switzerland.

[5] TotalEnergies. About GRIF. 2023. In: https://grif.totalenergies.com/en/about-grif/about-grif.

[6] Brissaud, F. Review of the calculation methods of ISO/TR 12489 for the probability of failure of safety-related systems. Presentation at the ISO Seminar on International Standardization in the Reliability Technology and Cost Area – presentations. Paris, 1 December 2022. https://standard.no/nyheter/nyhetsarkiv/petroleum/2022-news/iso-seminar-on-international-standardization-in-the-reliability-technology-and-cost-area---presentations/#.Y9y0oXbMJaS

[7] Brissaud, F., Oliveira, L.F. Average probability of a dangerous failure on demand: Different modelling methods, similar results. In proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference, Helsinki, Finland, June 25-29, 2012.

[8] Clavé, N., & Signoret, J.-P. ISO/TR 12489 – Reliability modeling and calculation of safety systems: Business application by TOTAL. Presentation at the ISO Seminar on International Standardization in the Reliability Technology and Cost Area – presentations. Stavanger, 26 April 2016. https://www.standard.no/rel-tech-cost#.Y9zSvXbMJaS

[9] Dutuit, Y. & Signoret, J-P. (2003) Tutorial on dynamic system modelling by using stochastic Petri nets and Monte Carlo simulation. Konbin 2003, Gdansk, Poland.

[10] Signoret, J-P. (1998) Modeling the behavior of complex industrial systems with stochastic Petri nets. ESREL 1998, Trondheim, Norway.

[11] Signoret, J-P. & al. (2002). Hiding a stochastic Petri net behind a reliability block diagram. ESREL 2002, Lyon, France.

[12] Signoret, J-P. & al. (2013) Make your Petri nets understandable: Reliability block diagrams driven Petri nets. Reliability Engineering and System Safety 113: 61-75, http://dx.doi.org/10.1016/j.ress.2012.12.008

[13] Signoret, J-P, Leroy, A. (2001) Reliability Assessment of Safety and Production Systems: Analysis, Modelling, Calculations and Case Studies, Mars 2021, Springer