Optimal SIL Configuration Selection: A graph-theoretic approach

Abdulqader Bin Sahl, Sidra Beg, Moreno Johan, Senithi Lorensuhewa, Cesare Baca, Maurizio Truscello, Francesco Perrone\*

Igeam Consulting S.r.l., Via Fara, 35 – 20124 Milano

\*Corresponding author E-Mail: f.perrone@igeam.it

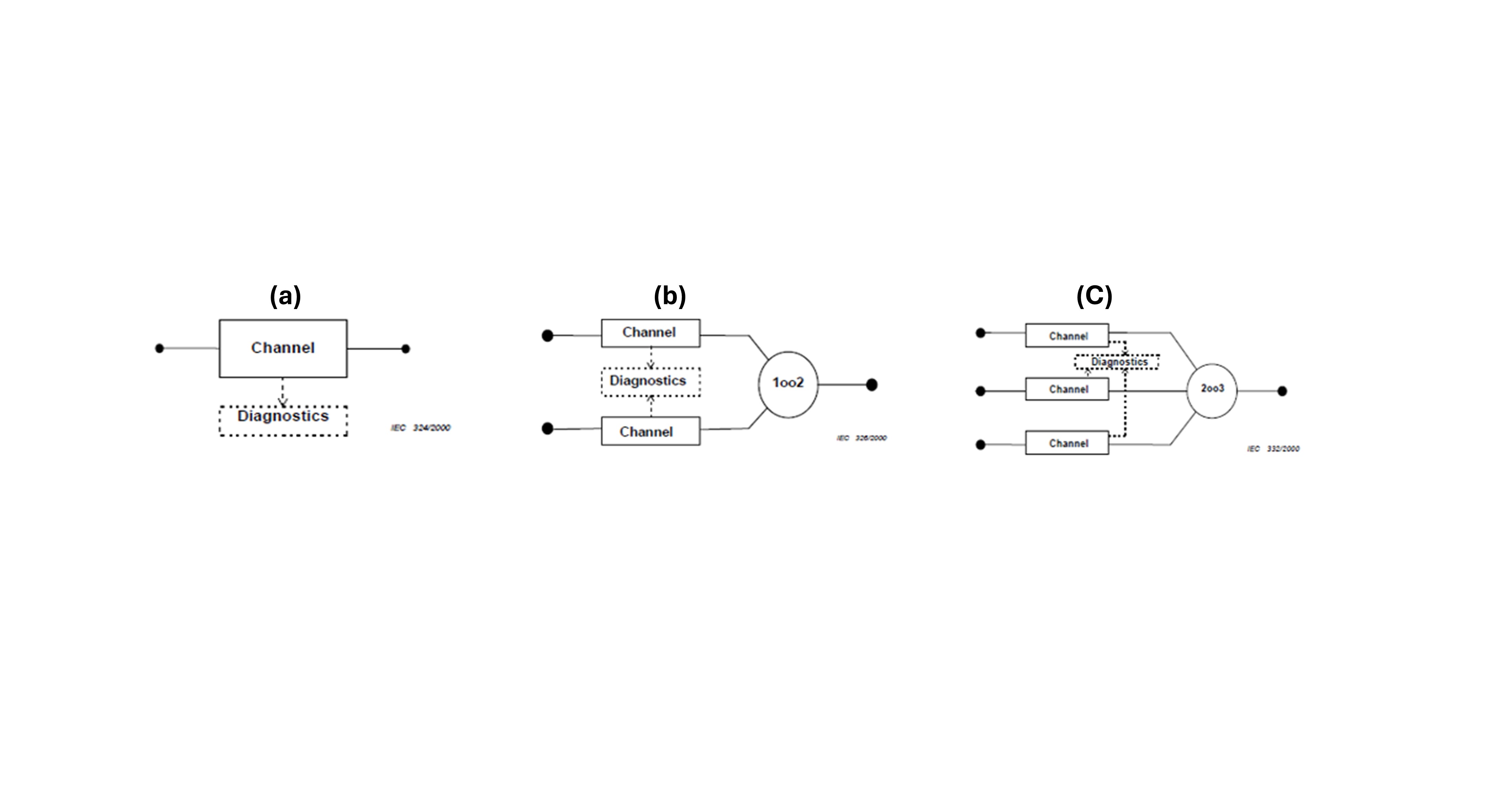
1. Introduction

The increasing awareness of industrial accidents, including property damage, injuries, and loss of life, has driven significant growth in functional process safety applications. Companies are legally and ethically obligated to mitigate operational risks, and the rising costs of mitigation have reinforced the importance of prioritizing reliability and safety. As a result, process industries are actively aligning with national and international safety standards, such as IEC 61508 and IEC 61511. To prevent accidents, industries implement multiple layers of protection, with Safety Instrumented Systems (SISs) being one of the most widely used. SISs are specifically designed to execute Safety Instrumented Functions (SIFs), to detect hazardous conditions and ensure the process remains in a safe state (Cheraghi & Taghipour, 2024). A SIS is composed of a combination of sensors, controllers, and final elements that work together to enhance process safety. Each SIF is designed to mitigate a specific process hazard or dangerous event, ensuring that the required Safety Integrity Level (SIL) is achieved. SIL defines the effectiveness and reliability of a SIF in reducing risks for a defined scenario, to an acceptable level. The appropriate SIL rating is determined by the Risk Reduction Factor (RRF), which quantifies the gap between the existing risk and the acceptable risk threshold. SIL are defined across four distinct levels of integrity. As the SIL level increases, the probability of failure on demand (PFD) decreases, reflecting enhanced system reliability and performance. However, higher SIL levels are generally accompanied by increased costs and complexity. SIL values are typically assigned within the range of 1 to 4, with Level 1 representing the lowest (least reliable) and Level 4 the highest (most reliable) level of safety. Table 1 presents the SIL ratings along with the corresponding ranges of RRF and Probability of Failure of Demand (PFD), where PFD is the inverse value of RRF, for a SIF functioning in demand mode (IEC 61511, 2016; IEC 61508a, 2010).

Table 1: SIL and the respective PFD and RRF (IEC 61511, 2016; IEC 61508a, 2010).

|  |  |  |
| --- | --- | --- |
| Safety Integrity Level (SIL) | Probability of Failure of Demand Avg (PFDAVG) | Risk Reduction Factor (RRF) |
| SIL 4 | ≥ 10-5 to < 10-4 | > 10 000 to ≤ 100 000 |
| SIL 3 | ≥ 10-4 to < 10-3 | > 1 000 to ≤ 10 000 |
| SIL 2 | ≥ 10-3 to < 10-2 | > 100 to ≤ 1000 |
| SIL 1 | ≥ 10-2 to < 10-1 | > 10 to ≤ 100 |

Achieving the desired SIL after the allocation of SIFs, such as through methods like Layers of Protection Analysis (LOPA) or Risk Graph, involves a thorough and strategic selection of system components. Furthermore, the integration of these components into a SIS must consider potential failure scenarios, response times, and the overall reliability of the system. In some cases, it may involve incorporating redundancy (e.g., multiple sensors or controllers) to ensure that a failure in one component does not compromise the system's ability to meet the required SIL. Selecting the optimal SIL configuration involves balancing cost, reliability, and operational feasibility, as compliance can be achieved through various system architectures. While industry standards and company policies often mandate fixed configurations, such as three SIL 2 transmitters, these may not always be the most cost-effective or efficient solutions. Redundant architectures, as opposed to the traditional one-out-of-one (1oo1), i.e., one-out-of-two (1oo2) or two-out-of-three (2oo3) (Figure 1), enhance system reliability but also lead to higher costs and increased complexity.



*Figure 1: Block Diagram for voting logics: (a) 1oo1, (b) 1oo2 and (c) 2oo3 (IEC 61508b, 2010)*

In SIL selection, Hardware Fault Tolerance (HFT) is a key parameter that defines the ability of a system to continue functioning despite hardware failures. It represents the number of failures a system can tolerate before losing its safety function, meaning an HFT of 0 implies a single component with no redundancy, while HFT = 1 means one redundant component is available, and so forth. Additionally, it is crucial to consider that each component of a SIS has a maximum achievable architectural SIL, constrained by HFT and Safe Failure Fraction (SFF). While redundancy improves system reliability, the maximum SIL that can be achieved is also dependent on the SFF of the individual components, meaning that even with increased HFT, certain components may still be limited in the SIL they can achieve due to their inherent failure characteristics. Table 2 and Table 3 present the required HFT and SFF for thresholds for achieving different SIL levels for Type A and Type B components route 1H approach, respectively. Type A components, being less complex with well-understood failure modes, generally require lower SFF values to achieve a given SIL. In contrast, Type B components, which include microprocessor-based or software-driven devices with more unpredictable failure characteristics, require higher SFF values to compensate for their increased uncertainty in failure behavior.

Table 3: Maximum allowable SIL for a safety function carried out by a type A element (IEC 61508c, 2010).

|  |  |  |  |
| --- | --- | --- | --- |
| Safe failure fraction of an Element | Hardware Fault Tolerance | | |
| 0 | 1 | 2 |
| < 60 % | SIL 1 | SIL 2 | SIL 3 |
| 60 % - < 90 % | SIL 2 | SIL 3 | SIL 4 |
| 90 % - < 99% | SIL3 | SIL 4 | SIL 4 |
| ≥ 99% | SIL 3 | SIL 4 | SIL 4 |

Table 4: Maximum allowable SIL for a safety function carried out by a type B element (IEC 61508c, 2010).

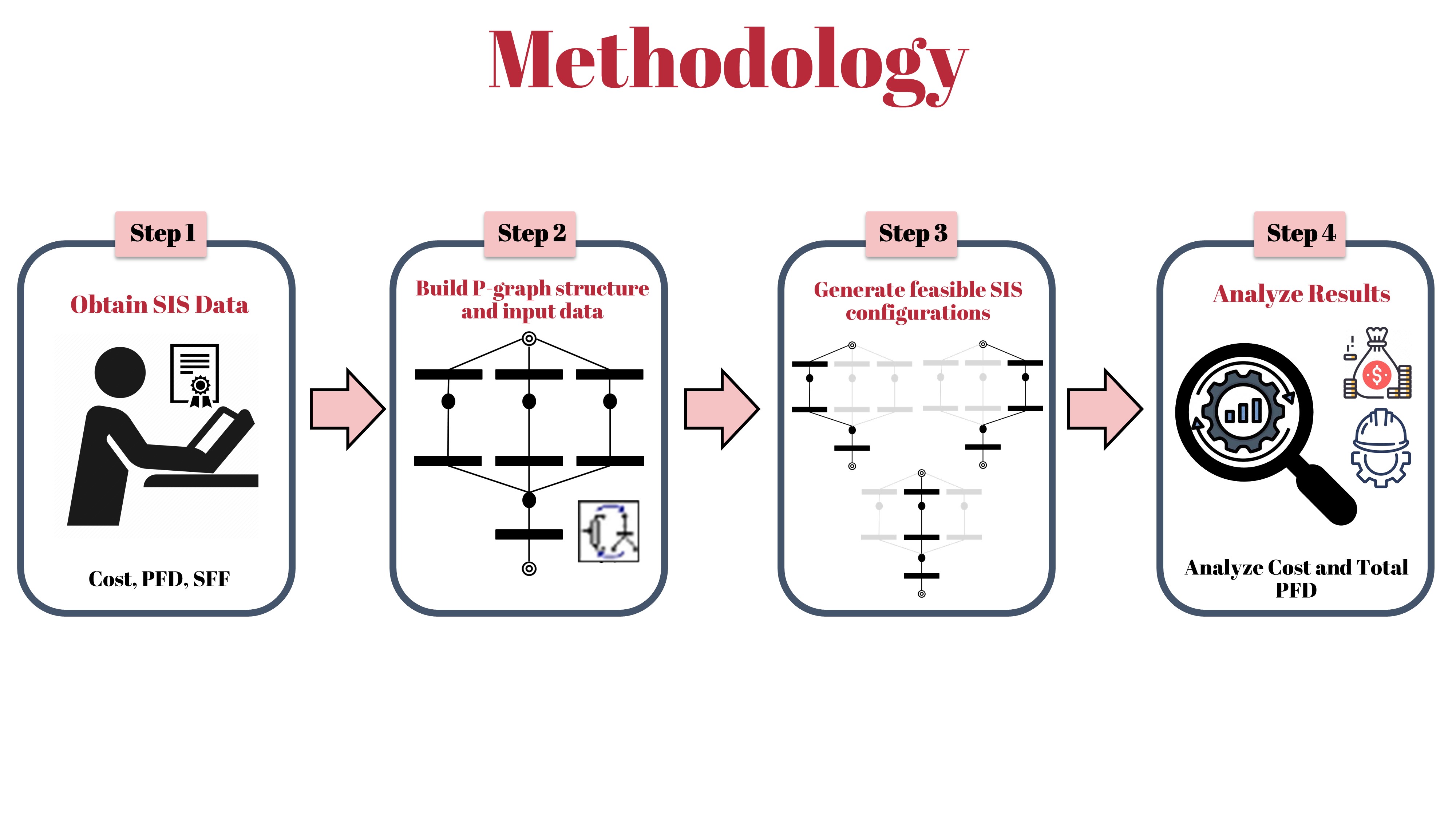
|  |  |  |  |
| --- | --- | --- | --- |
| Safe failure fraction of an Element | Hardware Fault Tolerance | | |
| 0 | 1 | 2 |
| < 60 % | Not Allowed | SIL 1 | SIL 2 |
| 60 % - < 90 % | SIL 1 | SIL 2 | SIL 3 |
| 90 % - < 99% | SIL 2 | SIL 3 | SIL 4 |
| ≥ 99% | SIL3 | SIL 4 | SIL 4 |

For optimal SIL configuration selection, decision-makers must carefully assess multiple feasible options, ensuring that safety requirements are met while optimizing compliance and economic viability. Conventional SIL configuration selection methods typically reply on engineering judgment or predefined standards and guidelines, which can sometimes overlook cost-effective or optimal solutions. Graph-theoretic approaches, such as P-graph, offer a structured and computational means to systematically evaluate all feasible solutions for a problem. P-graph, introduced by Friedler et al. (1979), has been a power tool to solve process network synthesis (PNS) problems given its capable mathematical algorithms, computational efficiency, and flexibility. As opposed to conventional mathematical programming (MP) methods, P-graph has a user-friendly interface which does not require prior programming knowledge (Friedler et al., 1998). Additionally, P-graph is capable of generating all optimal and near-optimal solutions, which provides decision-makers with the flexibility to choose the most optimal solution for their scenario. As such, P-graph has been implemented in several applications such as supply chain synthesis (How et al., 2016), resource conservation optimization (Sahl et al., 2023), multi-objective energy planning (Sahl et al., 2024), reliability and risk analysis (Süle et al., 2019), and non-engineering problems (Aviso et al., 2017).

However, to the best of the authors' knowledge, P-graph has not been previously applied to optimize SIL selection. Therefore, this work presents a novel P-graph approach to determine the optimal SIL configuration, leveraging its ability to systematically generate all optimal and near-optimal solutions. This capability ensures that decision-makers can evaluate multiple feasible configurations, allowing for flexibility in aligning with company guidelines, internal policies, and supplier restrictions. Since SIL compliance can often be achieved through different architectural setups, the ability to explore various alternatives while optimizing for cost, reliability, and operational feasibility makes P-graph a particularly valuable tool in SIS design and SIL allocation.

2. Methods

The methodology framework adopted for this work is shown in Figure 2. SIS data is collected in Step 1, which includes data for the transmitter, logic, and final element. All relevant data to calculate the PFD and is to be collected from manufacturer certificates. Similarly, SFF and cost data for the SIS is also collected. Following that, in Step 2, the P-graph structure is developed, and the collected data is used as input. Based on the desired SIL, the data constraints are entered in the model (e.g., Total PFD for SIL 2 ≤ 1 x 10-1). In Step 3, the P-graph model is used to generate all the feasible SIS configurations that meet the desired SIL requirement for the total PFD while also meeting the maximum allowable architectural SIL. Finally, in Step 4, the results are analyzed in terms of Cost and Total PFD.



*Figure 2. Methodology framework.*

* + 1. Mathematical Modelling

The mathematical formulations that are represented in the P-graph framework are discussed in this section, which consist of the objective function and model constraints based on a mixed integer linear programming (MILP) approach.

The objective function of this work is to minimize the total cost of the SIS (, which is c which is calculated as the sum of the costs of transmitter (), logic solver (), and final element () The objective function is expressed as:

Eq. (1)

where the cost of the transmitter varies based on the selected voting logic.

To satisfy the SIL requirement of the SIS, the total PFD () of the SIS must be determined, which is done by summing the PFD contributions from all system components, including the transmitter (, logic solver (, and final element (. The total PFD is calculated as:

Eq. (2)

The probability of failure of the transmitters differs based on the selected voting logic and is computed according to IEC 61508 standards. For a 1oo1 voting logic, the probability of failure is estimated by:

Eq. (3)

For a 1oo2 voting logic, the PFD is calculated as:

Eq. (4)

For a 2oo3 voting logic, the probability of failure is expressed as

Eq. (5)

where ​ represents the dangerous undetected failure rate of a channel in a subsystem, is the smallest of all dangerous undetected failure rates, is the fraction of undetected failures that have a common cause, and denotes the test period in years.

Once the total PFD is determined, the achievable RRF can be calculated also to facilitate the SIL selection process. The RRF is given by:

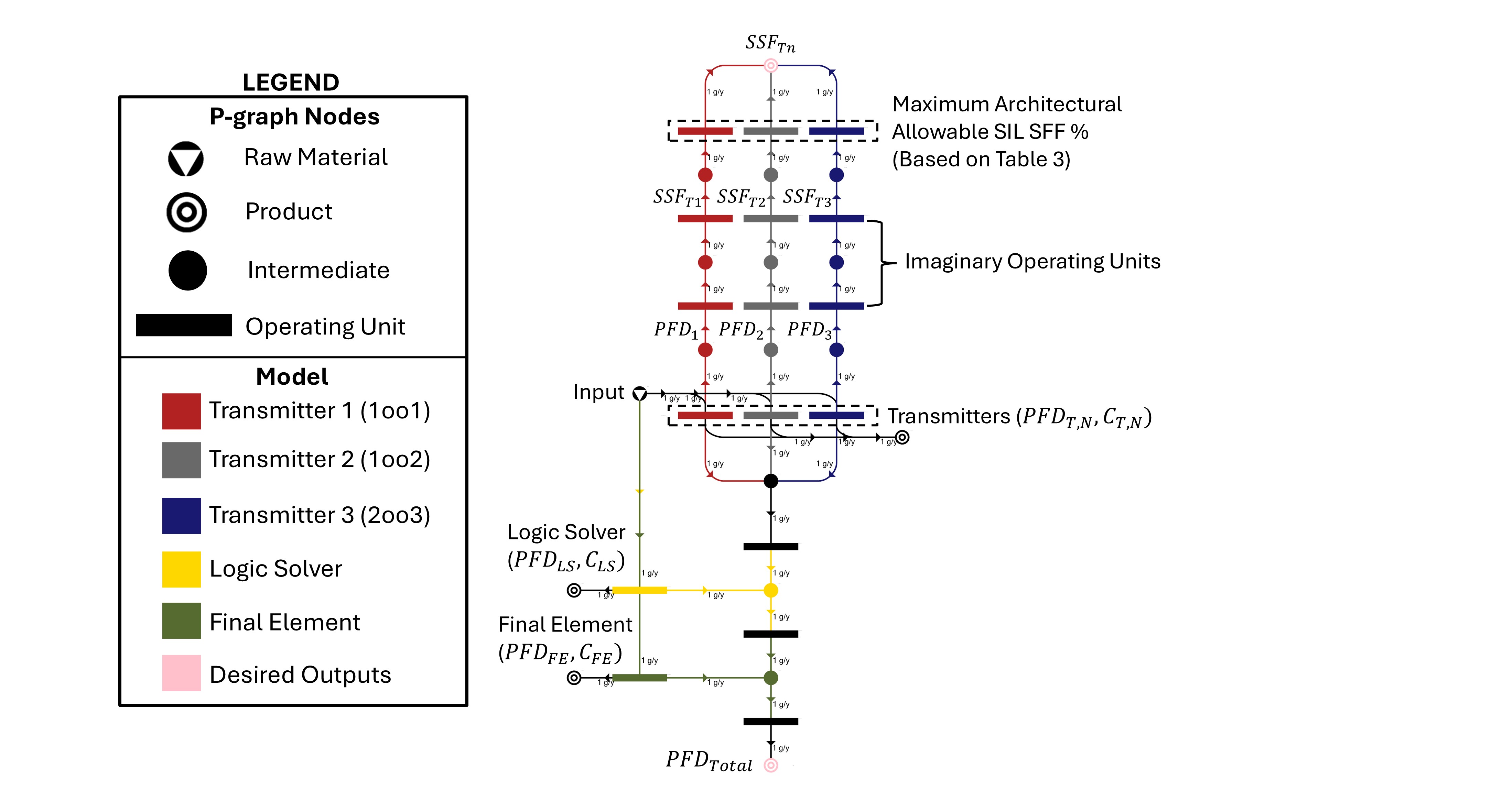
Eq. (6)

The maximum allowable SIL is constrained by the architectural limitations of the system component, which depend on the HFT and SFF. Thus, the system must satisfy the constraint:

Eq. (7)

* + 1. P-graph Model

A SIS that can adopt one of 3 transmitters with different voting logics (i.e., 1oo1, 1oo2, 2oo3), logic solver, and final element can be represented in P-graph as shown in Figure 3. P-graph nodes are classified to two classes, i.e., materials and operating units, where material nodes consist of raw material, intermediate, and product nodes. A detailed foundation of P-graph fundamentals is discussed in literature (Friedler et al., 1993; Friedler et al., 2022). The displayed P-graph model must follow the mathematical constrains outlined in Section 2.1. For Figure 3, the red colored nodes are for a transmitter of voting logic 1oo1, the grey color is for a transmitter of voting logic 1oo2, while the blue color represents the transmitter for a voting logic 2oo3. The respective and of each transmitter is inserted into the operating unit node. Similarly, the , , , are input into the operating unit nodes for the logic solver (represented in green) and final element (represented in yellow), respectively. The desired outputs of this model are the and , which are represented as product nodes in pink. The respective of the required SIL (based on Table 1) is to be inserted in the node. In addition, and must be added as a value on the connecting arcs of the intermediate material node and the operating unit, which are facilitated by imaginary operating units, as shown in Figure 3. Finally, the maximum architectural allowable SIL SFF range for each transmitter is inserted in a respective operating unit before being connected to the final product node.



*Figure 3. P-graph representation of a SIS with transmitters of different voting logic options.*

* 1. Results and discussion
     1. Case Study Description

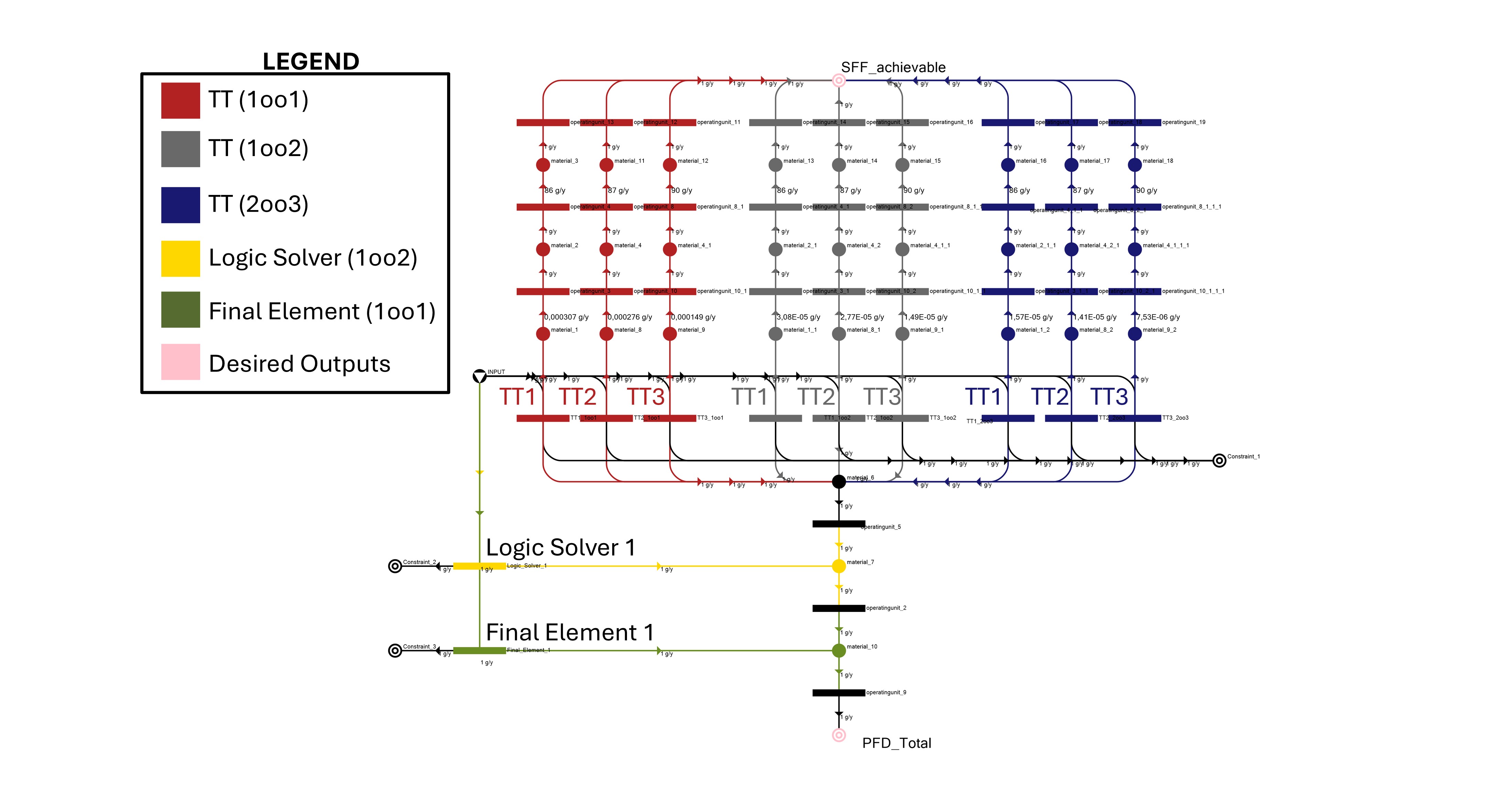
A case study of a generic SIS is adopted to demonstrate the proposed P-graph methodology. The SIS under consideration consists of temperature transmitters (TTs), a fixed logic solver, and a fixed final element. The system is designed to accommodate three different voting logics for the transmitters: 1oo1, 1oo2, and 2oo3. To evaluate different system configurations, three distinct temperature transmitter (TT) models are considered, denoted as TT1, TT2, and TT3. These models are based on industry data from available manufacturer safety certificates and specification sheets. Table 4 shows the data obtained for this case study, which consist of the PFD, SFF, and cost of each SIS component. It is worth noting that the test period for all the SIS components is taken as 1 year, which aligns with main industry best practices for safety system maintenance and inspection intervals. The objective of this SIS is to achieve a minimum requirement of SIL 2, which includes the verification in terms of maximum achievable architectural SIL. A SIL 2 verified (in terms of architectural constraints) logic solver and final element is used for this case study and thus they do not need to go through maximum achievable architectural SIL verification, unlike the TTs.

*Table 4: Case study data.*

|  |  |  |  |
| --- | --- | --- | --- |
| SIS Component | PFD | SFF (%) | Cost ($) |
| TT1 (1oo1) | 3.07 x 10-4 | 86 | 1195 |
| TT1 (1oo2) | 3.08 x 10-5 | 86 | 2390 |
| TT1 (2oo3) | 1.57 x 10-5 | 86 | 3585 |
| TT2 (1oo1) | 2.76 x 10-4 | 87 | 1935 |
| TT2 (1oo2) | 2.77 x 10-5 | 87 | 3870 |
| TT2 (2oo3) | 1.41 x 10-5 | 87 | 5805 |
| TT3 (1oo1) | 1.49 x 10-4 | 90 | 2200 |
| TT3 (1oo2) | 1.49 x 10-5 | 90 | 4400 |
| TT3 (2oo3) | 7.53 x 10-6 | 90 | 6600 |
| Logic Solver 1 (1oo2) | 4.69 x 10-4 | 80 | 3702 |
| Final Element 1 (1oo1) | 1.10 x 10-3 | 60 | 718 |

* + 1. P-graph Model

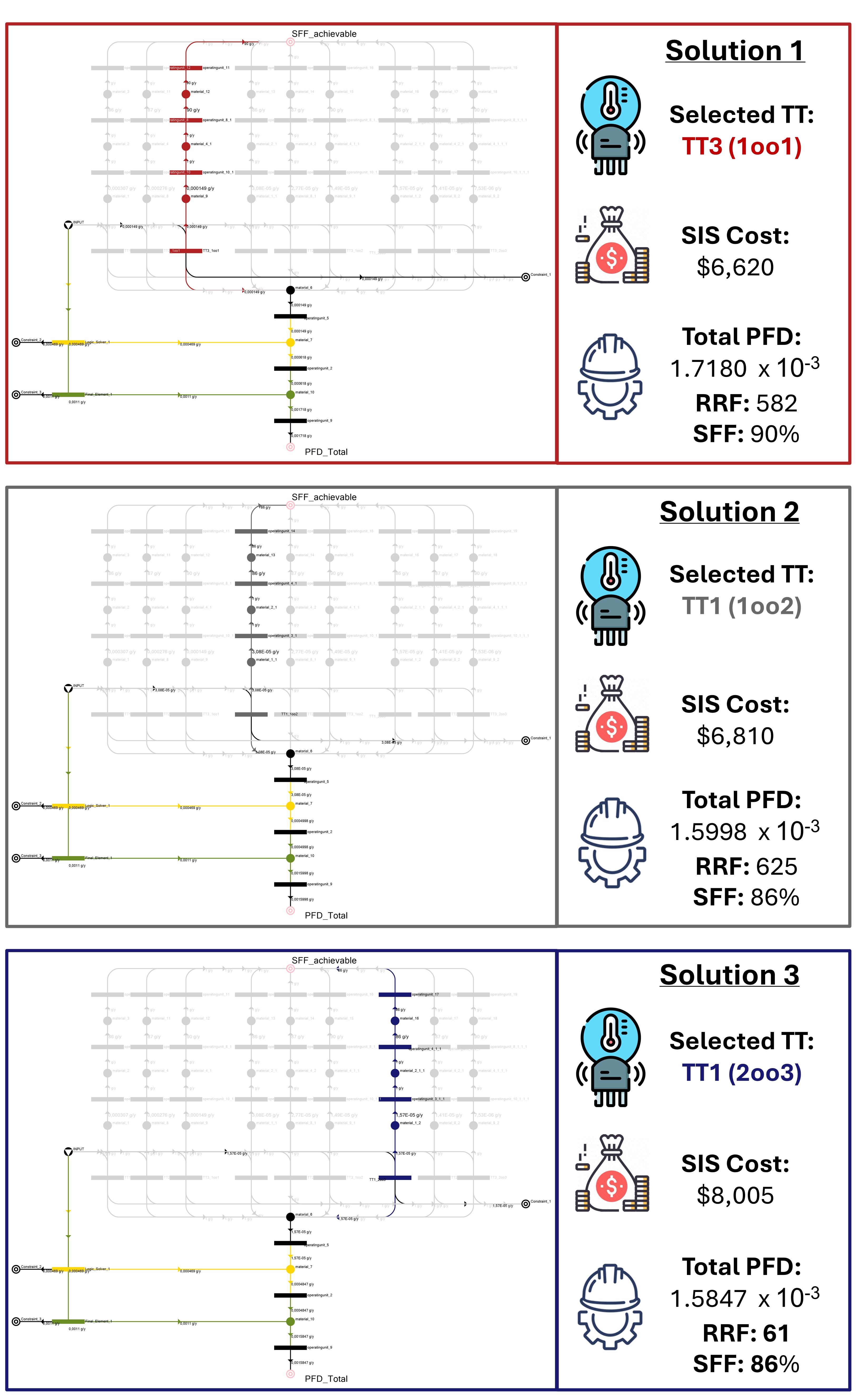
The P-graph model is developed based on the proposed case study as shown in Figure 4 with labels of each TT voting logic, logic solver, and final element. The P-graph model resulted in the generation of 7 total SIS configurations, and the solution details are shown in Table 4. In the proposed case study, 2 transmitters (i.e., TT1 (1oo1) and TT2 (1oo1)) were not selected as a possible configuration as their architectural requirements does not meet SIL 2 (SFF less than 90%). Among the seven solutions, the three most cost-effective configurations (refer to P-graph solution structure in Figure 5) are Solution 1 (TT3 (1oo1)) with a total cost of $6620, Solution 2 (TT1 (1oo2)) with a total cost of $6810, and Solution 3 (TT1 (2oo3)) with a total cost of $8005. The corresponding RRF values for these solutions are 582, 625, and 631, respectively, indicating an increasing level of reliability. Comparing Solution 1 and Solution 2, the latter is 2.87% more expensive but offers a 43-point increase in RRF, improving the system's fault tolerance. Similarly, Solution 3, which implements a 2oo3 voting logic, is 17.6% more expensive than Solution 2, with a minor RRF improvement of 6 points. Compared to the lowest-cost configuration (Solution 1), Solution 3 is 20.9% more expensive but provides a 49-point improvement in RRF, demonstrating enhanced system reliability. From a decision-making perspective, the selection of an optimal configuration depends on company policies and specific safety requirements. If a 2oo3 voting logic is required by company standards, Solution 3 (TT1 (2oo3)) would be a suitable choice, as it meets the redundancy requirement while maintaining a reasonable trade-off between cost and performance. However, if no strict voting logic constraints are imposed, Solution 1 (TT3 (1oo1)) offers the most cost-effective option while still achieving SIL 2 compliance. The results highlight the flexibility of the P-graph optimization model, enabling users to evaluate multiple configurations based on their respective cost, reliability, and safety performance. This flexibility will become even more apparent when additional transmitter options are introduced, as the model would be able to identify the most cost-effective choices from a broader set of alternatives. The P-graph framework thus serves as a powerful decision-support tool, enabling structured evaluation of safety instrumented system configurations while ensuring compliance with SIL requirements and minimizing costs.



*Figure 4. P-graph model for the case study’s SIS.*

*Table 4: P-graph solution results.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Solution No. | Selected TT | Total PFD (x 10-3) | RRF | Total Cost ($) | SFF (%) |
| 1 | TT3 (1oo1) | 1.7180 | 582 | 6620 | 90 |
| 2 | TT1 (1oo2) | 1.5998 | 625 | 6810 | 86 |
| 3 | TT1 (2oo3) | 1.5847 | 631 | 8005 | 86 |
| 4 | TT2 (1oo2) | 1.5967 | 626 | 8290 | 87 |
| 5 | TT3 (1oo2) | 1.5839 | 631 | 8820 | 90 |
| 6 | TT2 (2oo3) | 1.5831 | 632 | 10225 | 87 |
| 7 | TT3 (2oo3) | 1.5765 | 634 | 11020 | 90 |



*Figure 5. Top 3 SIS configuration solutions from P-graph.*

4. Conclusions

This study presented a novel P-graph approach for optimizing SIL configuration selection, addressing the challenge of balancing cost, reliability, and compliance in SISs. The proposed model systematically generates all optimal and near-optimal solutions, allowing decision-makers to evaluate feasible configurations while considering architectural constraints, redundancy levels, and economic feasibility. The case study demonstrated that among the seven feasible solutions, the three most cost-effective configurations were Solution 1 (TT3 (1oo1)) at $6620, Solution 2 (TT1 (1oo2)) at $6810, and Solution 3 (TT1 (2oo3)) at $8005, with corresponding RRF of 582, 625, and 631, respectively. The results highlighted the trade-off between cost and reliability, where Solution 3 (2oo3 configuration) offers the highest reliability but at a 20.9% higher cost compared to the cheapest option (Solution 1, TT3 1oo1). By integrating SFF and HFT constraints, the model ensures that selected configurations are both technically feasible and compliant with SIL architectural limitations. The P-graph methodology proved to be a computationally efficient and scalable tool, enabling users to systematically explore different SIS configurations and select an optimal or near-optimal solution based on budget, safety requirements, and regulatory constraints. This flexibility will become even more apparent as additional transmitter options, logic solvers, and final elements are introduced, allowing for broader optimization in future applications. A natural extension of this work would be to incorporate a wider selection of SIS components (i.e., transmitters, logic solvers, and final elements), enabling more complex configurations while maintaining optimal SIL configuration selection. The proposed P-graph approach serves as a structured decision-support tool, allowing SIS engineers and process safety practitioners to achieve cost-effective and compliant SIL configuration selection while enhancing industrial safety and reliability.

Acknowledgments

The authors would like to acknowledge the support provided by Igeam Consulting in conducting this work. Their valuable insights and resources greatly contributed to the development of this study.

References

Cheraghi, M., Taghipour, S., 2024. A mathematical optimization model for determining safety integrity levels in process facilities. Reliab. Eng. Syst. Saf. 109896.

Friedler, F., Blicket, T., Gyenis, J., Tarján, K., 1979. Computerized generation of technological structures. Comput. Chem. Eng. 3 (1–4), 241–249. https://doi.org/10.1016/0098-1354(79)80042-3.

Friedler, F., Fan, L., Imreh, B., 1998. Process network synthesis: problem definition. Networks Int. J. 31 (2), 119–124.

Friedler, F., Tarjan, K., Huang, Y., Fan, L., 1993. Graph-theoretic approach to process synthesis: polynomial algorithm for maximal structure generation.

Friedler, F., Orosz, A., Losada, J.P., 2022. P-Graphs for Process Systems Engineering. Springer.

How, B.S., Lam, H.L., 2017. Novel evaluation approach for biomass supply chain: an extended application of PCA. Chem. Eng. Trans. 61, 1591–1596. https://doi.org/10.3303/CET1761263.

IEC 61508a, 2010. IEC 61508 Functional Safety of electrical, electronic and programmable electronic (E/E/PE) safety-related system - Part 1: General requirements. International Electrotechnical Commission.

IEC 61508b, 2010. IEC 61508 Functional Safety of electrical, electronic and programmable electronic (E/E/PE) safety-related systems - Part 6: Guidelines on the application of parts 2 and 3. International Electrotechnical Commission.

IEC 61508c, 2010. IEC 61508 Functional Safety of electrical, electronic and programmable electronic (E/E/PE) safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission.

IEC 61511, 2016. IEC 61511 Functional Safety - Safety Instrumented Systems for the Process Industry Sector - Part 1: Framework, definitions, system, hardware and application programming requirements. International Electrotechnical Commission.

Sahl, A.B., Loy, A.C.M., Lim, J.Y., Orosz, A., Friedler, F., How, B.S., 2023. Exploring N-best solution space for heat integrated hydrogen regeneration network using sequential graph-theoretic approach. Int. J. Hydrogen Energy 48 (13), 4943–4959. https://doi.org/10.1016/j.ijhydene.2022.10.196.

Sahl, A.B., Orosz, Á., How, B.S., Friedler, F., Teng, S.Y., 2024. Electrification of oil refineries through multi-objective multi-period graph-theoretical planning: A crude distillation unit case study. J. Clean. Prod. 434, 140179. https://doi.org/10.1016/j.jclepro.2023.140179.

Süle, Z., Baumgartner, J., Dörgő, G., Abonyi, J., 2019. P-graph-based multi-objective risk analysis and redundancy allocation in safety-critical energy systems. Energy 179, 989–1003. https://doi.org/10.1016/j.energy.2019.05.043.

Aviso, K.B., Cayamanda, C.D., Mayol, A.P., Tan, R.R., 2017. P-graph approach to human resource reallocation in industrial plants under crisis conditions. In: 2017 6th International Symposium on Advanced Control of Industrial Processes (AdCONIP), pp. 131–136. IEEE.