



Review

Lifecycle costs of safety instrumented systems in process industries: a systematic literature review

Mehran Farzadmehr^a, Philippe Nimmegeers^{a,b,c,*}

^a Department of Engineering Management, Faculty of Business and Economics, University of Antwerp, Prinsstraat 13, 2000 Antwerp, Belgium

^b Flanders Make@UAntwerp, Prinsstraat 13, 2000 Antwerp, Belgium

^c NANOLight Centre of Excellence, Prinsstraat 13, 2000 Antwerp, Belgium

ARTICLE INFO

Keywords:

Safety instrumented systems
Lifecycle cost
Process industries
Systematic literature review
Functional safety

ABSTRACT

A safety instrumented system (SIS) is an automated system designed to detect and mitigate potential risk of hazardous conditions in industrial processes by taking actions to prevent or mitigate incidents. It is essential because it helps protect people, equipment, and the environment by reducing the risk of accidents in hazardous operations, such as in chemical plants, oil refineries, or power stations. While the primary objective of SIS design is safety, economic considerations, particularly lifecycle cost, play a pivotal role in decision-making during the design phase. Although research efforts exist to incorporate lifecycle cost with safety, the literature is fragmented and lacks a comprehensive lifecycle cost framework. Therefore, a systematic literature review is conducted to uncover safety instrumented systems' lifecycle cost elements and the decision variables that impact them. The review results lead to a comprehensive and structured cost calculation framework to assess SIS designed to protect a process unit economically. Finally, this study provides perspectives on potential research directions relevant to SIS lifecycle cost, including the impact of systematic failures, cybersecurity integration, the relative weighting of different cost elements, inclusion of risk costs, and various SIS application types.

1. Introduction

A Safety Instrumented System (SIS) is a layer of protection in process industries, designed to prevent hazardous events and mitigate risk to people, the environment, and assets. Such safety barriers constitute an important element of hazard prevention and mitigation in chemical process industries, with their performance and management being essential to maintaining plant safety (Yuan et al., 2022). As defined by the International Electrotechnical Commission (IEC) standard 61511 (which applies specifically to the process industry sector), an SIS is composed of one or more Safety Instrumented Functions (SIFs) (International Electrotechnical Commission, 2017). Each SIF is designed and engineered to bring a process to a safe state in response to specific abnormal conditions.

An SIS typically includes sensors (for detecting abnormal conditions), logic solvers (to process the signal and decide on action), and final elements (such as valves or actuators that bring the process to a safe state) (Cai et al., 2021; Innal et al., 2015; Julsereewong et al., 2017). Unlike basic process control systems (BPCS), an SIS is designed and

implemented according to strict functional safety requirements to meet predetermined risk reduction levels (Jahanian, 2017; Redutskiy, 2017b; Yasser et al., 2025). In this context, safety-related control design in process industries is closely linked to hazard identification, risk analysis, and the prevention and mitigation of critical faults in accordance with functional safety requirements (Squillante Jr. et al., 2021).

The IEC 61508 standard provides a framework for designing, implementing, operating, and maintaining functional safety of electrical/electronic/programmable electronic safety-related systems (International Electrotechnical Commission, 2010), while IEC 61511 tailors the requirements specifically for the process industry. According to these standards, the need for an SIS is determined through risk analysis, and each SIF within the SIS must meet a specified Safety Integrity Level (SIL), ranging from SIL 1 (lowest) to SIL 4 (highest), based on the required risk reduction. Fig. 1 depicts an example of an SIS that contains n SIFs, each of which includes one sensor and final element subsystems connected to a main Safety-PLC. Each SIF is designed to safeguard a process from a hazardous event concerning the required SIL.

In the high-risk environment of process industries (e.g., oil and gas, chemicals, petrochemicals, and pharmaceuticals), failure to manage

* Corresponding author at: Department of Engineering Management, Faculty of Business and Economics, University of Antwerp, Prinsstraat 13, 2000 Antwerp, Belgium.

E-mail address: Philippe.Nimmegeers@uantwerpen.be (P. Nimmegeers).

<https://doi.org/10.1016/j.ssci.2026.107495>

Received 6 October 2025; Received in revised form 23 August 2026; Accepted 28 September 2026

Available online 1 October 2026

0925-7535/© 2026 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

Nomenclature			
Notation	Description		
SIS	Safety instrumented system	PTC_j^D	Coefficient that impacted the proof test duration of device j due to test coverage (Percentage)
LCC	Lifecycle cost	$PTTI_{ij}$	Proof test interval for device j assigned to component i (month)
SIF	Safety instrumented function	PTP_{ij}	Equals 1, if the decision on proof test policy and operation condition leads to downtime during the proof test of device j assigned to component i; 0, otherwise
SIL	Safety integrity level	DT	Downtime cost (monetary unit/hour)
IEC	International Electrotechnical Commission	C_{Maint}^t	Total maintenance cost (monetary unit/year)
PFD	Probability of failure on demand	C_j^{PM}	Cost of performing preventive maintenance (repair cost) for device j (monetary unit/hour)
RRF	Risk reduction factor	C_j^{CM}	Cost of performing corrective maintenance (spare part cost) for device j (monetary unit/hour)
RAMS	Reliability, availability, maintainability, and safety	PMd_{ij}	Duration of preventive maintenance for device j assigned to component i (hour)
RAMS + C	Reliability, availability, maintainability, and safety + cost	CMd_{ij}	Duration of corrective maintenance for device j assigned to component i (hour)
CapEx	Capital expenditure	PM_{ij}	Probability of preventive maintenance occurrence for device j assigned to component i during proof test/spurious trip (percentage)
OpEx	Operational expenditure	CM_{ij}	Probability of corrective maintenance occurrence for device j assigned to component i during proof test/spurious trip (percentage)
i	Index running over set of SIS components (sensor, Safety-PLC, final element)	C_{Risk}^t	Total risk cost (monetary unit/year)
j	Index running over set of devices distinguished by model and types to be used for SIS components	C_{SPT}^t	Total spurious trip cost (monetary unit/year)
N_{ij}	Number of device j used in SIS component i. This notation represents both device type/model and redundancy decision variables.	C_j^{Insp}	Inspection cost during spurious trip for device j (monetary unit/hour)
C_{Cap}	Capital cost (monetary unit)	$Inspd_{ij}$	Duration of inspection for device j assigned to component i (hour)
C_{des}	Total design cost for each SIF (monetary unit)	$SPTR$	Spurious trip rate (percentage/year)
$C_{ins/com}$	Total installation and commissioning cost (monetary unit)	C_{Inc}^t	Total incident cost (monetary unit/year)
$C_j^{ins/com}$	Installation and commissioning cost of device j (monetary unit)	R	Residual risk after implementing the SIF in an SIS (percentage/year)
C_{Purch}	Total component purchase cost (monetary unit)	C_{Hazard}	Catastrophic consequences of an incident (monetary unit)
C_j^{Purch}	Purchase cost of device j (monetary unit)	C_{EndL}	Total end-of-life cost (monetary unit)
C_{Oper}^t	Operating cost (monetary unit/year)	C_j^{Decom}	Decommissioning cost of device j (monetary unit)
C_{Econs}^t	Total energy consumption cost (monetary unit/year)	$C_{lifecycle}$	Lifecycle cost of one SIF
C_j^{ECons}	Annual energy consumption cost of device j (monetary unit)	t	Time (year)
C_{Ptest}^t	Total proof test cost (monetary unit/year)	LC	Lifecycle (year)
C_j^{Ptest}	Cost of performing proof test for device j (monetary unit/hour)	δ	Annual discount rate (percentage)
PTC_j^P	Coefficient that impacted the proof test performing cost of device j due to test coverage (Percentage)		
PTd_{ij}	Duration of proof test for device j assigned to component i (hour).		

risks can result in severe consequences, including explosions, toxic releases, and significant economic loss (Rabah et al., 2024; Redutskiy, 2017b, 2017a, 2018; Yasser et al., 2025). SIS plays a vital role in preventing such events by automatically initiating protective actions when unsafe conditions are detected. Moreover, increasing digitalization introduces additional cyber-physical risks, as malicious manipulation of industrial control and safety systems can contribute to major accident scenarios, reinforcing the need to consider the interaction between process safety and cybersecurity (Carreras Guzman et al., 2021; Iaiani et al., 2021b; Ylönen et al., 2022). Key reasons for designing SIS are risk reduction, operational continuity, and protection of life and the environment. IEC 61511 emphasizes a lifecycle approach to SIS design, encompassing phases from conceptual design through operation and maintenance to eventual decommissioning (International Electrotechnical Commission, 2017). Besides, safety instrumented systems' effectiveness is impacted by factors that alter throughout their lifecycle, including operational and maintenance conditions. For instance, Ouache et al., (2015); Ouache & Kabir, (2016) have shown that SIS component degradation pattern and environmental situations extremely influence the probability of failure on demand of SIS in

different periods, emphasizing the importance of lifecycle-based SIS performance assessment. More broadly, the adequacy of safety barriers depends on their availability, probability of failure on demand, and ability to provide the required safety integrity for the prevailing level of risk (Sobral & Guedes Soares, 2019). This ensures that safety is not only designed into the system but maintained throughout its operational life.

While the primary objective of SIS design is functional safety and compliance with SIL requirements, economic considerations, particularly Lifecycle Cost (LCC), play a pivotal role in decision-making during the design phase (Chebila, 2023; Wacker et al., 2013; Julsereewong et al., 2017; Torres-Echeverría et al., 2009a; Yasser et al., 2025). LCC refers to the total cost of ownership of the SIS throughout its entire lifespan (Cai et al., 2021; Machleidt & Litz, 2011; Redutskiy, 2017a; Torres-Echeverría et al., 2009a). The SIS lifecycle commences from initial concept and capital investment and continues through operations and eventually ends with decommissioning. Integrating LCC analysis into SIS design allows engineers and decision-makers to evaluate trade-offs between cost, performance, reliability, and safety. This approach considers both over-designed and under-designed protection levels for process units, leading to cost-effective safety solutions that comply with

IEC 61511 and align with business and operational goals.

By scientifically investigating the SIS LCC topic, this study contributes to the academic research domain and practice in various vital ways. First, it provides a thorough overview of SIS LCC elements, filling the gap in existing literature where cost elements are treated inconsistently. Second, this review identifies the main decision variables considered throughout the SIS lifecycle, together with the modeling assumptions associated with these variables, and examines how they influence SIS life-cycle costs. Lastly, the study proposes a structured and comprehensive SIS LCC calculation framework that combines technical and economic factors in a model. This framework is novel in its ability to be used for comparative evaluations of SIF design alternatives across the full SIS lifecycle. Overall, this paper expands current understanding about the SIS LCC topic by providing a more comprehensive, decision-oriented approach to SIS cost evaluation, which can improve both safety performance and cost efficiency of SIS applications in process industries.

The remainder of this paper is structured as follows. In Section 2, this study carries out a systematic literature review on SIS LCC to extract existing knowledge in scientific literature about cost elements and how they are impacted. Section 3 exhibits the thematic structure of the literature on SIS LCC based on keyword co-occurrence networks. Subsequently, Section 4 presents the results of the literature review that includes a proposed comprehensive SIS LCC calculation framework by synthesizing the existing knowledge in the literature. Furthermore, in Section 5, perspectives about potential research directions are provided. These potential future research directions are about the SIL and SIS LCC, impact of incorporating risk costs, cybersecurity, weight of downtime cost, systematic failure, and protected process unit through different safety functions into the SIS lifecycle cost framework. To conclude, the key takeaways and main contributions of this research are summarized in Section 6.

2. Methodology

This study follows the PRISMA framework to conduct a systematic literature review on SIS LCC in process industries. The search query for this literature review contains two parts: keywords related to SIS/SIF (“safety instrumented system” OR “safety instrumented systems” OR “safety

instrumented system (SIS)” OR “Safety instrumented function” OR “safety instrumented function (SIF)”) and used keywords for extracting publications in relevant topics to SIS cost (“Design” OR “Optimization” OR “Lifecycle cost” OR “SIL verification” OR “SIL assessment” OR “SIL determination” OR “RAMS” OR “reliability, availability, maintainability, and safety” OR “RAMS + C”). This study employs the PRISMA framework and predefined inclusion/exclusion criteria to ensure a precise and transparent process for retrieving the most relevant publications regarding SIS LCC.

Fig. 2 illustrates the PRISMA flow diagram demonstrating the steps of this systematic literature review concerning the identification, screening, and checking eligibility of publications. First, the query was searched concerning the inclusion and exclusion criteria mentioned in Table 1, yielding a total of 935 publications split between Scopus (n = 679) and Web of Science (WoS) (n = 256). Following the criteria mentioned in Table 1, the review only includes journal and conference papers written in English and published up to the second quarter of 2025 in the relevant subject areas such as engineering, chemistry, energy, environmental science, and decision science.

After removing 315 duplicate papers, the remaining 620 publications were considered for initial screening. In the screening step, titles and abstracts were checked for relevance, excluding 535 papers that did not meet the inclusion criteria. The eligibility of studies was decided based on inclusion and exclusion criteria, presented in Table 1. Publications to be included in the review must address the cost aspects of SIS/SIF design, optimization, or lifecycle management in alignment with the IEC 61511 standard. Hence, studies that did not explicitly address SIS/SIF lifecycle costs were not considered.

Eventually, 85 papers were selected for full-text retrieval, of which 35 could not be accessed due to availability limitations. As this represents a substantial proportion of the papers selected for full-text assessment, the inability to retrieve these studies may have limited the completeness of the review and may have resulted in the exclusion of potentially relevant evidence. The full text of the remaining 50 papers underwent a detailed eligibility check concerning the inclusion and exclusion criteria stated in the last row of Table 1. Accordingly, 28 of the remaining papers were excluded because they lacked sufficient details on the SIS LCC model, including SIS lifecycle cost elements and decision variables impacting them. Eventually, 22 studies were included in the

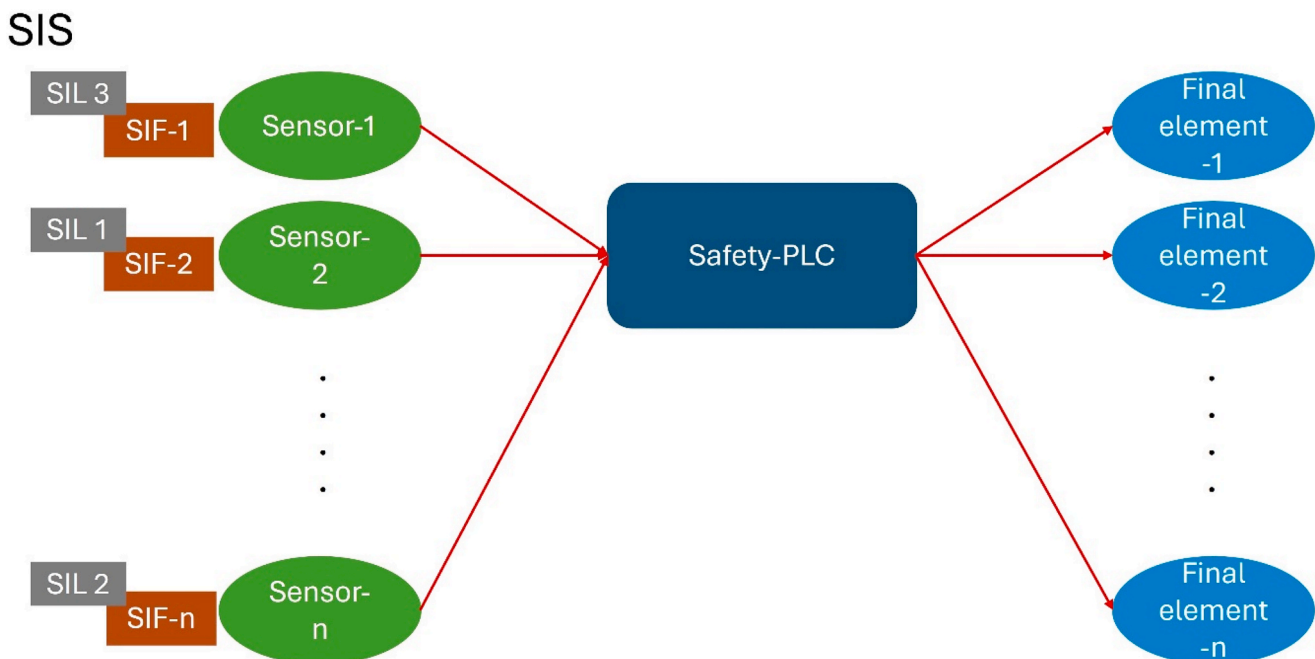


Fig. 1. Relation between SIS, SIF, and SIL and the connection to sensors, safety-PLC and final elements.

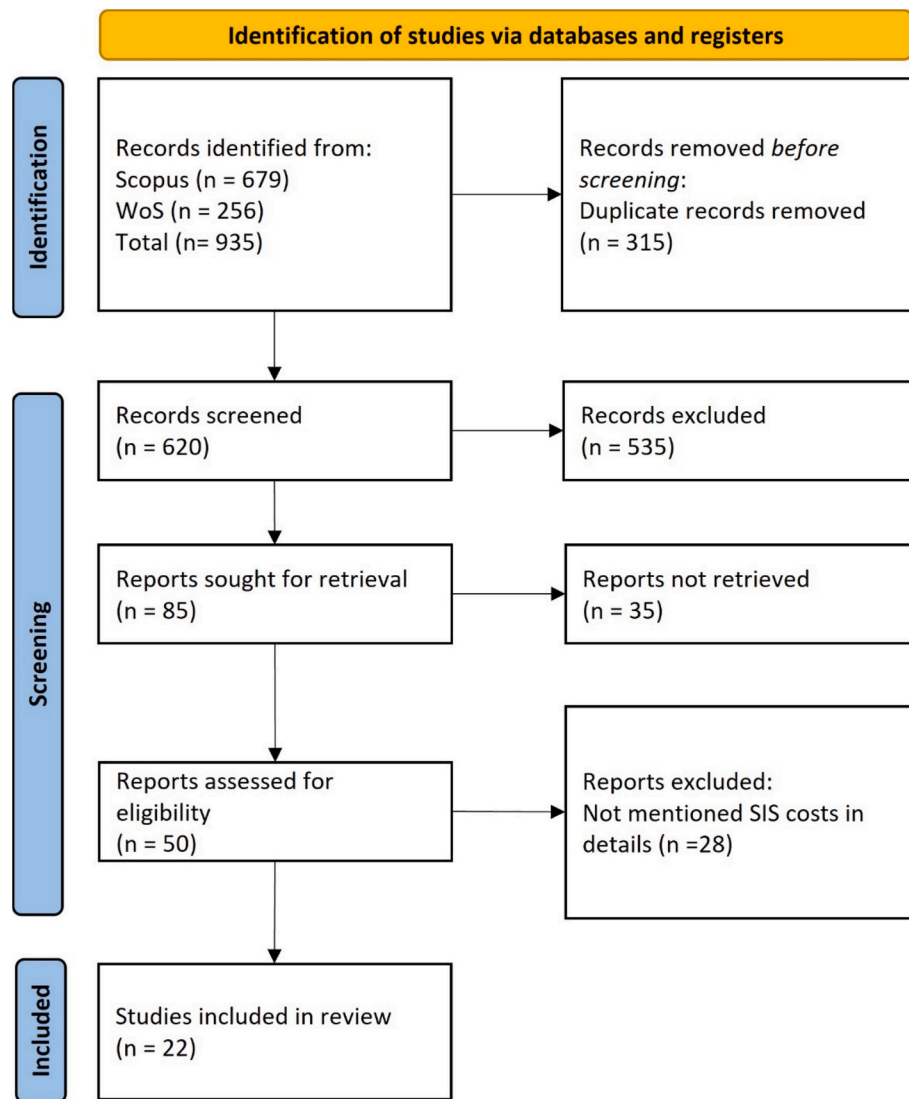


Fig. 2. PRISMA flow diagram for systematic literature review process.

Table 1

Inclusion and exclusion criteria for systematic literature review.

	Inclusion criteria	Exclusion criteria
Document type	Journal paper, Conference paper, early access	Book chapter, Editorial material, etc.
Document language	English	Non English
Published year	Up to the second quarter of 2025	After the second quarter of 2025
Subject area	All topics like Engineering, chemistry, energy, environmental science, decision science	None
Content	Publications focusing on the cost of SIS/SIF design, optimization through its lifecycle with respect to IEC 61511.	Any publication that does not cover the SIS/SIF lifecycle cost

final database for conducting the literature review on SIS lifecycle costs.

The final set of 22 included studies was analyzed using a structured data extraction and synthesis process. For each publication, key information related to SIS lifecycle cost modeling was systematically extracted. The extracted information includes the process unit protected by the SIS, the types of costs incorporated into the SIS life-cycle cost model, the decision variables considered, and the modeling assumptions

associated with these variables in each study. A qualitative synthesis was then conducted to identify common SIS cost-modeling approaches and differences in cost structures, decision variables, and associated modeling assumptions across the literature. These synthesized insights were utilized to develop and structure the proposed SIS LCC framework, reflecting the various methodologies in SIS cost modeling practices articulated in the existing SIS LCC literature.

Fig. 3 below presents a keyword co-occurrence network generated using VOSviewer to further investigate the thematic structure of the literature on SIS LCC. Prior to conducting the analysis, some keywords were merged due to either conveying similar terms or appearing in different spelling. For instance, “Testing” and “Proof testing” or “Safety system” and “Safety instrumented system” were merged due to conveying the same terms. Besides, abbreviations of “Safety instrumented system”, “Safety integrity level”, “Genetic algorithm”, “Probability of failure on demand” were merged with their complete version. After keywords merging process, a total of 101 distinct keywords remained for the analysis. During the analysis, the minimum number of occurrences of a keyword is set to 2 and only 17 different keywords met this threshold.

The network shows “safety instrumented systems” as a dominant and significantly connected theme, directly related to risk management and multi-objective optimization, highlighting its role as a central domain.

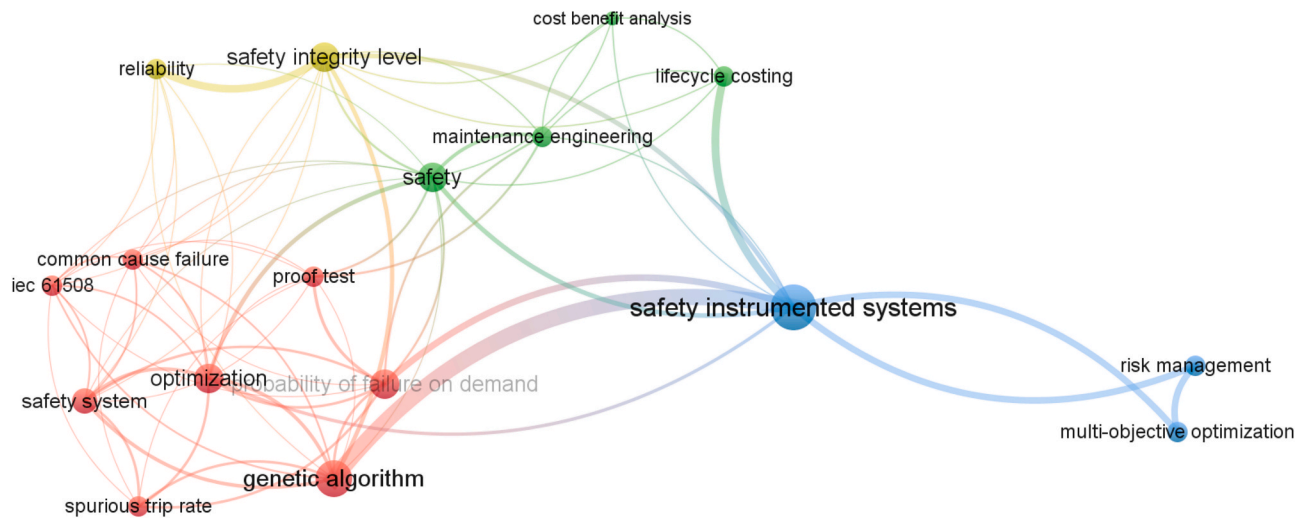


Fig. 3. Keywords co-occurrence network of SIS LCC literature review.

Around this main core, there exists a reliability and safety assessment cluster that contains keywords such as safety integrity level, reliability, and common cause failure. This cluster also connects to the foundational analytical frameworks guided by international standards such as IEC 61508. Another important cluster focuses on optimization and SIS design evaluation, comprising genetic algorithm, optimization, proof test, probability of failure on demand, and spurious trip rate, which together emphasize model-based methodologies for SIS design assessment. In parallel, a maintenance and cost-oriented cluster links maintenance engineering, testing, cost-benefit analysis, and lifecycle costing, emphasizing the increase in attention to lifecycle and economic considerations among researchers active in the SIS design topic. The interconnected nature of these clusters illustrates an increasing convergence between safety standards, optimization techniques, and lifecycle-based decision-making in the design and operation of safety instrumented systems.

3. Results

Systematic literature review results are presented in four different themes. First, SIS applications referring to various processes, which are safeguarded by SIS, are discussed. The second theme entails SIS LCCs referring to cost elements for having an SIS in place. Subsequently, decision variables influencing SIS LCCs are provided in the third subsection of results. Finally, an SIS LCC calculation framework is presented based on the insights from the systematic literature review. The detailed literature review table is presented in Table 2.

3.1. SIS applications

SISs are applied to a wide variety of industrial applications to reduce specific risks and take processes to a safe situation upon facing hazardous events. This subsection provides an overview of the types of process units safeguarded by SIS throughout selected studies in the literature. In addition, it describes how diverse safety functions are designed for specific operational risks.

Many publications are focused on SIS applications in the oil and gas industry, specifically for overpressure protection and emergency shutdown systems (ESD). Cai et al. (2021) and Zhang et al. (2021) explore the design of High-Integrity Pressure Protection Systems (HIPPS). These systems are employed to prevent overpressure situations, with Cai et al. (2021) particularly targeting wellhead offshore production platforms. Similarly, Zhang et al. (2021) focus on the HIPPS in a regular process unit in the oil and gas industry, but they do not provide exact

information regarding the intended process unit. Within the same industry, Redutskiy (2017b), (2017a), (2018), and Redutskiy et al. (2021) investigate SIS design in an oil and gas company with a storage tank, where the SIS safeguards operation from high liquid level and fire by stopping the feed pump and shutting valves. Moreover, John Satur et al. (2016) depict the SIS implementation to protect the flare knock-out drum in an oil and gas or petrochemical plant from high-pressure risk. The SIS operates using high liquid level sensors and shuts the inlet valves to avoid overfill and flare risks.

Zhang et al. (2020) study an ESD system employed to stop flow under overpressure conditions, even though they do not indicate the studied process unit. They mainly investigate the generic role of SISs in keeping the equipment under control (EUC) in a safe mode. Furthermore, Innal et al. (2015) and Cheraghi & Taghipour (2024) also do not develop an SIS for a real case study. They focus on a hypothetical SIS application for a facility with six process units: two gasoline tanks, two sour natural gas pipelines, and two sweet natural gas pipelines. This SIS application includes various SIFs for avoiding gasoline spills via level sensors, isolating sour gas lines by leak detection, and protecting jet fires from sweet gas releases. Although no information about a particular process unit is provided, the SIS design is relevant to processes within the chemical or refining industry where overpressure risk is frequent. Berrah et al. (2023) and Chebila (2023) follow the same model for SIS design using altered parameters. Moreover, Torres-Echeverría et al. (2009a), (2009b), and (2012) study SIS design for a chemical reactor, which should be protected from high pressure and temperature. This research effort presents a systematic analysis of risk reduction in typical high-risk chemical processes.

Rabah et al. (2024) also consider a flared gases recovery unit in which an ESD is executed as an SIS. This system is created to bring the compression section of the recovery unit to a safe state when parameters such as temperature, pressure, or level exceed safety constraints. The objective is to guarantee safe gas-lift injection into oil wells, highlighting a regular theme of SISs supporting pressure control in upstream oil operations. Yasser et al. (2025) examine an SIS designing model for a separation process, particularly in a reflux drum. The designed SIS is activated by a high-high level sensor and immediately closes the overhead line valve to avoid overpressure and overfilling. In this specific SIS application, the risk of liquid overflow and vapor containment is mitigated. Moreover, Julsereewong et al. (2017) recommend a thorough SIS design model for the tail gas treating process, including three different SIFs protecting various process units: reactor effluent, reactor, and contact condenser. The SIFs separately react to low liquid level, high temperature, and pump suction loss. This research is one of the more

Table 2

Overview literature review results. Abbreviations: PT = Proof Test; PM = Preventive Maintenance; Prod loss = Production loss; Temp = Temperature; Maint = Maintenance; Spurious = Spurious trip-related costs; Incident = Incident or risk-related costs; Energy = SIS energy consumption; Catastrophic = Catastrophic loss; Staggering = Test-staggering factor; Separation = Electrical/physical separation; Location = Plant location-dependent maintenance cost factors.

Code	Reference	Cost Elements	Decision Variables	Application
P1	Julsereewong & Thepmanee (2017)	Purchase; maint; energy; spurious	Redundancy	Low level; high temp; pump suction
P2	Wacker et al. (2013)	PT	PT coverage	None
P3	Cheraghi & Taghipour (2024)	Purchase; PT; maint; spurious; incident	SIL selection	High level; gas leak
P4	Redutskiy (2017b)	Purchase; PT; shutdown; repair; maint; spurious; incident	Device type; redundancy; separation; PT interval	High level; fire
P5	Torres-Echeverría et al. (2009b)	Purchase; maint; PT; repair; spare; prod loss; start-up; catastrophic	PT interval; staggering	High pressure; temp
P6	Torres-Echeverría et al. (2009a)	Same as P5	Device type; redundancy	High pressure; temp
P7	Torres-Echeverría et al. (2012)	Same as P5	Device type; redundancy; PT interval; staggering	High pressure; temp
P8	Innal et al. (2015)	Purchase; PT	Device type; redundancy; PT interval	High level; gas leak
P9	Zhang et al. (2020)	PT; maint; incident	PM degradation thresholds	High pressure
P10	Zhang et al. (2021)	PT; maint	PT coverage	High pressure
P11	Redutskiy et al. (2021)	Maint; workforce	—	High level; fire
P12	Jahanian (2017)	PT	PT interval	Turbine fuel valve
P13	Chebila (2023)	Purchase; maint; PT; energy; spurious; incident	Device type; redundancy; PT interval	High pressure
P14	Rabah et al. (2024)	PT	PT interval; coverage	High temp; pressure; level
P15	Redutskiy (2017a)	Purchase; PT	Device type; redundancy; PT interval; separation	High level; fire
P16	Machleidt & Litz (2011)	Purchase; maint; PT; spurious; shutdown	Device type; redundancy; PT interval	None
P17	Yasser et al. (2025)	Purchase; PT	Device type; redundancy; PT interval	High pressure; high level
P18	Berrah et al. (2023)	Purchase; prod loss; start-up; energy; maint; PT; spurious; decommission	Device type; redundancy; PT interval	High pressure
P19	Redutskiy (2018)	Purchase; maint; incident	Device type; redundancy; separation; PT interval;	High level; fire

Table 2 (continued)

Code	Reference	Cost Elements	Decision Variables	Application
P20	Zhang et al. (2023)	Maint	location; crew scheduling PM threshold; PM imperfection; inspection policy	None
P21	Longhi et al. (2015)	Spurious; unavailability; maint; PT	First test; staggering; test interval	None
P22	Cai et al. (2021)	Purchase; energy; maint; incident	Device type; redundancy; PT interval	High pressure

complete SIS applications in terms of process unit coverage.

Among publications in the literature, Jahanian (2017) represents the only research in the power generation context, studying SIS for gas turbines. This paper studies an SIS containing a single SIF that is designed to avoid turbine overspeed by initiating an emergency shutdown of the fuel control valve.

Throughout the reviewed literature, safety functions associated with overpressure states appear as the most frequently considered SIS application. Whether applied in offshore platforms, reactors, or storage tanks, SISs are regularly implemented to react to high pressure by initiating shutdowns. Another widely addressed hazard is high liquid level (e.g., in knock-out drums, reflux drums, and storage tanks), mostly avoided through automated valve closures.

3.2. SIS lifecycle cost elements

The LCC analysis of SIS has been discussed among publications existing in the literature, often sharing common cost elements but illustrating diverse categorization methods with different degrees of detail. The overview of SIS LCC structures developed in the literature is thoroughly argued in the following paragraphs. A comparative review of this literature uncovers both convergence and divergence in how researchers distinguish and group these costs.

Julsereewong et al. (2017) classify SIS LCC into two main categories: procurement costs and operating costs. Procurement costs comprise the SIS components' purchase, design, installation, and commissioning. SIS design costs include configuration and safety validation, while installation and commissioning cover physical setup, wiring, debugging, and verification. Operating costs encompass modification costs, fixed maintenance (e.g., inspections, proof testing, spare parts, maintenance staff training, and wages), SIS energy consumption, and failure-related costs. Notably, SIS failure costs are split into required maintenance and production loss due to downtime, both incurred because of spurious trips.

Berrah et al. (2023) agree with the same LCC categorization (procurement and operational) but with a wider range. In this study, procurement costs also include SIS design and installation, and SIS components purchase (including delivery, taxes, and handling). Besides, the procurement cost here covers staff training to work with SIS. Operational costs comprise SIS energy consumption, preventive and corrective maintenance, periodic proof testing, and production losses from SIS failures. The model also includes SIS decommissioning costs as a standalone category. Although Berrah et al. (2023) employs another terminology, their SIS LCC categorization significantly resembles the SIS LCC model presented by Julsereewong et al. (2017), mainly in terms of procurement and operations costs.

Cai et al. (2021) establish a similar SIS LCC model, grouping costs within fixed and operating categories. They indicate that fixed costs comprise SIS design, component purchase, and installation, while operating costs cover modifications, SIS energy consumption,

maintenance, and spurious trip costs. Compared to Julsereewong et al. (2017) or Berrah et al. (2023), Cai et al. (2021) extend their SIS LCC model to introduce risk cost, defined as the catastrophic consequence of SIS failing to prevent dangerous events.

Unlike the abovementioned studies, Chebila (2023) recommends a different SIS LCC model, classifying costs in capital, recurring, and side effect groups. Similar to fixed and procurement costs, capital costs include SIS design, commissioning, components purchase, installation, and staff training, but also extend to SIS design modification. Same as operating costs, recurring costs focus meticulously on operational expenses and contain maintenance, proof testing, SIS's energy consumption, and other recurring costs (e.g., auditing, supervision, insurance). The new category, so-called "side effect," encompasses spurious trip and risk costs, including downtime, repair, and hazard consequences costs.

Although Cheraghi & Taghipour (2024) introduce almost the same costs in the SIS lifecycle, they outline four cost categories: fixed costs, operating costs, spurious trip cost, and risk cost. The fixed costs entirely overlap with Cai et al. (2021) while operating costs consist of proof testing, preventive, and corrective maintenance. Spurious trip and risk costs are introduced separately, even though they repeat Chebila (2023)'s "side effect" cost category. The incorporation of spurious trip and risk costs into SIS LCC models shows a growing consensus among scholars on the importance of accounting for accidental event-related costs in the SIS lifecycle.

A series of papers in the literature, carried out by the same leading author, also utilize three cost categories to demonstrate SIS LCC: procurement, operations, and risk (Redutskiy, 2017b, 2017a, 2018; Redutskiy et al., 2021). Besides the familiar categorization, the demonstrated SIS LCC model by the abovementioned author completely overlaps with previous SIS LCC models. However, these papers expand the SIS LCC model in a way that dives deeper in terms of maintenance staff costs, such as establishing a local engineering department and related organizational expenses. Moreover, Torres-Echeverría et al. (2009b), (2009a), (2012) also present a three-party SIS LCC model, including procurement, operating, and risk costs. In these publications, risk costs encompass hazard consequences, such as asset loss and production loss. This perspective significantly matches that of Redutskiy and previous authors, demonstrating that a robust SIS LCC model must consider residual risk impact.

Unlike publications presented so far, other papers introduce incomplete or only investigate certain parts of the presented SIS LCC models. For instance, Machleidt & Litz (2011) argue procurement, maintenance, and downtime costs within a fragmented framework. Similarly, Zhang et al. (2020), (2021) do not provide any clear framework for SIS LCC while they underline the importance of downtime cost caused by maintenance and proof testing. Longhi et al. (2015) only investigate maintenance, proof testing, spurious trip costs, including production loss caused by performing maintenance/proof testing. Furthermore, Innal et al. (2015) and Yasser et al. (2025) only concentrate on the SIS components purchase and proof test costs. Despite the fact that these publications are less comprehensive, they emphasize the critical importance of procurement (SIS components purchase), maintenance/proof test-related costs in SIS LCC.

Most publications offer an SIS LCC model, sharing numerous common cost elements such as SIS design, component purchasing, installation, proof testing, preventive and corrective maintenance, energy consumption, and failure-related costs. However, terminology varies with "fixed", "capital", and "procurement" costs often referring to capital expenditures, while "operational", "recurring", or "operations" costs typically cover similar operational expenditures. More advanced models separately introduce an extra cost category, focusing on spurious trips and hazardous consequences due to SIS failing to prevent dangerous events, while emphasizing more precise SIS lifecycle evaluations. Moreover, this section also presents the appearance of SIS LCC elements among publications in literature. Fig. 4 illustrates that the most frequently mentioned cost element is proof test cost, appearing in

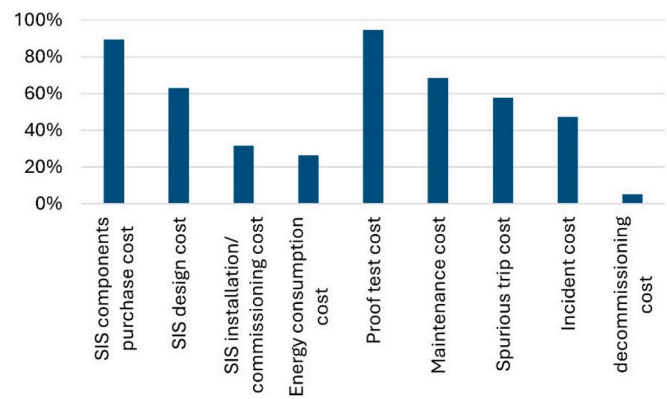


Fig. 4. Frequency of cost element occurrence in SIS LCC literature.

approximately 95% of papers. SIS components' purchase cost is also commonly considered by almost 85% of the literature. Maintenance cost and SIS design cost follow, with about 65% and 60% occurrence, respectively. Regarding the risk costs, spurious trip cost and incident cost are mentioned in around 55% and 45% of the reviewed publications in the literature. SIS installation/commissioning cost, along with energy consumption cost, appear less frequently, both under 35%. The least mentioned cost is the decommissioning cost, which is included in less than 5% of the publications.

3.3. Decision variables in SIS design

Many of the reviewed publications investigate how specific decision variables, together with the modeling assumptions associated with them, affect the total SIS life-cycle cost. These factors range from the selection of device models and architectural configurations during SIS design to the choice of proof-testing strategies during operation and maintenance. This section summarizes the principal decision variables identified in the literature and discusses the relevant modeling assumptions associated with them, where applicable. Almost 60% of covered studies within this systematic review investigate how the type/model of device (i.e., specific hardware or technology) chosen for SIS components affects the SIS reliability and LCC. Berrah et al. (2023), Chebila (2023), Innal et al. (2015), and Yasser et al. (2025) all focus on device type as an imperative decision variable, and they all came to the same conclusions, stating various device models/types have varying failure rates and maintenance requirements, causing considerable alterations in SIS LCC.

Opting for appropriate redundancy architecture design for SIS components, particularly the "KooN" (K-out-of-N) voting configurations, is repeatedly mentioned as a decision variable, impacting SIS LCC. Julsereewong et al. (2017) discuss how various redundancy architectures in SIS components, which are used to protect a process unit from hazardous events, lead to varying LCC. Similarly, Berrah et al. (2023) and Yasser et al. (2025) provide results of different SIS design configurations, which are distinguished by device types and redundancy architecture used for their components, illustrating the influential role of these variables.

The same results are reinforced by Cai et al. (2021) and Torres-Echeverría et al. (2009a), who investigate diverse or heterogeneous redundancy architecture, where various device models/types are utilized for redundancy to reduce common-cause failures. However, both papers find that such diversity may mitigate failures, while it increases SIS LCC due to higher procurement and maintenance expenditures. Torres-Echeverría et al. (2012) expand this analysis by studying how redundancy architecture, together with proof testing policies, impacts SIS LCC, further highlighting the importance of SIS redundancy architectural choices.

Regarding the proof test policy, the interval between proof tests is a

key decision variable referred to by 80% publications in the literature. Berrah et al. (2023), Chebila (2023), and Yasser et al. (2025) combine proof test intervals with optimization models to reveal how shorter proof test intervals increase SIS reliability but may increase LCC due to higher test performance and process downtime costs.

In addition to the interval, several publications make a distinction between existing proof testing strategies, which also influence cost fluctuations. Torres-Echeverría et al. (2009b) present proof testing strategies within four main groups: simultaneous, sequential, staggered, and independent. The abovementioned research aligns with the latter one (Torres-Echeverría et al., 2012), examine how proof testing strategies and redundancy architecture impact SIS availability and LCC. Furthermore, Zhang et al. (2021) only compare two proof testing strategies (simultaneous and staggered) in the context of SIS final elements and demonstrate that testing strategies alter SIS LCC and timing of maintenance. Additionally, Longhi et al. (2015) consider different operational modes during proof testing as modeling assumptions associated with the proof-testing strategy. These include whether production is interrupted during testing and whether components under test remain available to vote for activation of the SIF. The study shows that these assumptions can substantially affect process downtime and, consequently, the SIS LCC.

The effectiveness of proof testing, often quantified by the proof test coverage rate, is a vital assumption altering both SIS LCC and reliability. Wacker et al. (2013) discuss that complete detection of hidden dangerous failures by conducting proof testing is hardly reachable, especially in complex SIS design. They state that proof test coverage rate must be realistically indicated to prevent overestimating SIS reliability and underestimating its LCC. Rabah et al. (2024) also investigate the effects of proof-test interval and proof-test coverage on SIS LCC. In this context, assumptions regarding proof-test effectiveness are incorporated when defining feasible values of the proof-test interval and coverage, thereby reflecting operationally realistic proof-testing conditions.

Finally, to mitigate common-cause failures, a few publications mention another imperative decision variable. Redutskiy (2017b) incorporates physical/electrical separation of SIS components as a decision variable to address such failures in the SIS LCC model. This is a huge contribution as it addresses systemic risks that traditional redundancy may not mitigate. The same author further introduces the assignment of maintenance personnel to different maintenance duties as a decision variable, with which organizational common-cause failures could be decreased (Redutskiy, 2018; Redutskiy et al., 2021).

To recap, Fig. 5 depicts that the literature converges on several core decision variables impacting SIS LCC, such as device type/model, redundancy architecture, and proof test interval. Among these, proof

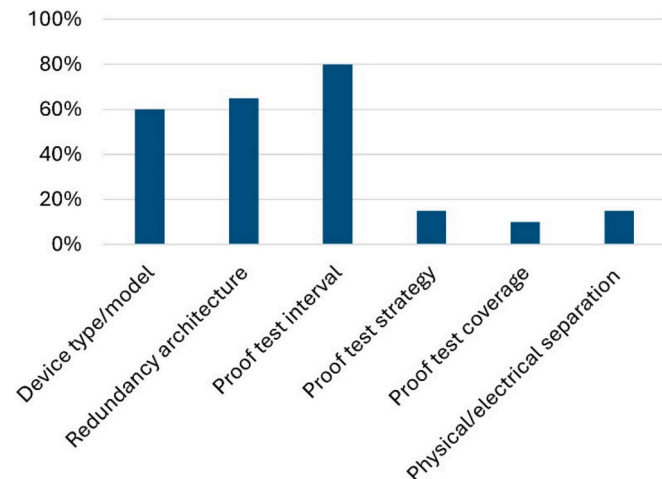


Fig. 5. Frequency of decision variables in SIS LCC literature.

test interval receives the most comprehensive treatment. Moreover, other decision variables related to proof testing, such as proof-testing strategy and coverage, together with their associated modeling assumptions, have also received attention in the reviewed literature. Eventually, the decision variable associated with physical/electrical separation of SIS components is exploited in 15% of reviewed publications in this study.

3.4. Proposed SIS lifecycle cost framework

The SIS LCC calculation framework's primary purpose is to compute and compare the total LCC of one SIF aimed at preventing a particular hazardous event. Given that multiple SIFs may be applicable within a specific SIS design, this framework also supports decision-making by helping identify the most cost-effective option for each SIF. To do so, the LCC of all existing SIFs in an SIS must be calculated individually using the framework. Thus, the total LCC of the entire SIS consists of all SIFs' LCC.

In this paper, the SIS LCC calculation framework is structured around four main categories: capital cost (C_{Cap}), annual operating cost (C_{Oper}^t), annual risk cost (C_{Risk}^t), and end-of-life cost (C_{EndL}). Table 3 illustrates all cost elements within each category. This framework is designed to calculate the total LCC of various SIFs within an SIS tailored to protect a specific process unit. Equation (1) presents the SIS LCC calculation formula containing all four cost categories. Since operating and risk cost categories are considered on an annual basis, their net present value (NPV) is calculated using the annual discount rate during the SIS lifecycle (δ). Besides, the NPV of the end-of-life cost is also calculated using the same discount rate.

$$C_{lifecycle} = C_{Cap} + \sum_{t=1}^{LC} (C_{Oper}^t + C_{Risk}^t) \times \frac{1}{(1 + \delta)^{t-1}} + C_{EndL} \times \frac{1}{(1 + \delta)^{LC-1}} \quad (1)$$

3.4.1. Capital cost

In the literature, many publications refer to capital expenditures in SIS LCC by various terms such as fixed, capital, and procurement costs. Although procurement is the most used term in the literature, according to IEC 61511, procurement is only a part of the engineering and design phase of the SIS. Therefore, this study assigns "Capital" term to present capital expenditures in the SIS lifecycle. Equation (2) illustrates that capital costs (C_{Cap}) contain all the incurred expenses in the phase of SIS design/engineering (C_{des}) and SIS installation/commissioning ($C_{ins/com}$) with respect to the IEC 61511 standard. Besides, it shows that expenses associated with SIS components purchasing (C_{Purch}) are considered in this category.

$$C_{Cap} = C_{des} + C_{ins/com} + C_{Purch} \quad (2)$$

3.4.1.1. SIS design cost. SIS design/engineering covers activities such as SIS configuration, SIS validation, factory acceptance test, and any other activity falling under the SIS design and engineering phase with respect to the IEC61511 standard. SIS design cost contains all the expenses associated with this phase to reach to the SIS installation/commissioning phase. Therefore, all these expenses are spent for one SIS that consists of one (or multiple) SIF(s). Since this phase occurs once and the result will be the SIS that will be taken into operation, the SIS design cost should be considered as a fixed cost that is independent of any presented decision variables.

3.4.1.2. SIS installation/commissioning cost. According to IEC 61511, the SIS installation and commissioning phase encompasses physical setup, wiring, debugging, and verification of the designed SIS within the field. Unlike SIS design cost, this cost depends on SIS architecture complexity, including the type/model of devices and the redundancy proposed for the designed SIS. Therefore, this variable cost is influenced

Table 3
Developed SIS LCC framework.

Cost category	Cost element	Impactful Decision variables	Cited publications (see Table 2)
Capital costs	SIS design cost	–	P1, P3, P4, P5, P6, P7, P22
	SIS installation/commissioning cost	Device type/model, Redundancy architecture	P1, P3, P4, P5, P6, P7, P13, P18, P22
	SIS component purchase cost	Device type/model, Redundancy architecture	P1, P3, P4, P5, P6, P7, P8, P13, P15, P16, P17, P18, P19, P22
Operating costs	Energy consumption cost	Device type/model, Redundancy architecture	P4, P13, P18, P22
	Proof test cost (including test and downtime costs)	Device type/model, Redundancy architecture, Proof test interval, Proof test strategy, Proof test coverage	P1, P2, P3, P4, P8, P9, P10, P12, P13, P14, P15, P16, P17, P18, P21
	Maintenance cost (including repair/spart part and downtime costs)	Device type/model, Redundancy architecture,	P1, P3, P4, P5, P6, P7, P9, P10, P11, P13, P16, P18, P19, P20, P21, P22
Risk costs	Spurious trip cost (including repair/spart part and downtime costs)	Device type/model, Redundancy architecture, Proof test interval, Proof test strategy, Proof test coverage	P1, P3, P4, P13, P16, P18, P19, P21
	Incident cost (including catastrophic event consequences)	Device type/model, Redundancy architecture, Proof test interval, Proof test strategy, Proof test coverage	P4, P5, P6, P7, P9, P13, P19, P22
End of life costs	SIS decommissioning cost	Device type/model, Redundancy architecture	P18

by the specification of devices to be used as SIS components and the redundancy architecture proposed for all SIS components, denoted by i . Since there are three SIS components (sensor, Safety-PLC, final element), $i=\{1,2,3\}$. However, there could be an unlimited number of device models/types to be used for each SIS component. Therefore, this study sets $j = \{1, 2, 3, \dots, n\}$ and use N_{ij} as a combined decision variable for both device type/model and redundancy assigned to each SIS component. This way, N_{ij} represents the number of device j considered to be used for the SIS component i . Here, Equation (3) displays the total installation/commissioning cost ($C_{ins/com}$), which is calculated by multiplying the installation/commissioning cost of each device ($C_j^{ins/com}$) with the number of corresponding devices used for each SIS component (N_{ij}).

$$C_{ins/com} = \sum_{i=1}^3 \sum_{j=1}^n C_j^{ins/com} \times N_{ij} \quad (3)$$

3.4.1.3. SIS components purchase cost. Purchasing devices for SIS components incurs expenses before putting SIS into operation. Since the literature presents this cost as a standalone cost element, this study also refers to it outside of the SIS installation/commissioning cost element denoted by C_{Purch} . The SIS components purchase cost for each device type/model (C_j^{Purch}) includes the actual purchasing price, taxes, delivery, and any handling fee associated with procurement. This variable cost is also impacted by the decision variable N_{ij} , representing the used device type/model and redundancy architecture for each SIS component.

$$C_{Purch} = \sum_{i=1}^3 \sum_{j=1}^n C_j^{Purch} \times N_{ij} \quad (4)$$

3.4.2. Operating cost

Although various terms are used in the literature to present operational expenditures in the SIS lifecycle, all refer to the same concept of SIS LCC. Since operating is the commonly used term among most publications in the literature of SIS LCC, this research also assigns it to illustrate operational expenditures in the SIS lifecycle. Operating costs encompass all the expenses occurring within the operation and maintenance phase in the safety lifecycle concerning the IEC61511 standard. Equation (5) shows that annual operating cost (C_{Oper}^t) includes annual energy consumption cost (C_{Econs}^t), annual proof test cost (C_{Ptest}^t), and annual maintenance cost (C_{Maint}^t).

$$C_{Oper}^t = C_{Econs}^t + C_{Ptest}^t + C_{Maint}^t \quad (5)$$

Energy consumption cost

Like any other set of digital/mechanical equipment, SIS components, including sensors, Safety-PLCs, and final elements, require energy to operate. Therefore, the cost of energy consumed by SIS components to safeguard the process falls under operational expenses. This variable cost is impacted by the decided device type/model and redundancy architecture for each component during the SIS design phase, represented by N_{ij} . This way, Equation (6) demonstrates that the total annual energy consumption cost (C_{Econs}^t) is calculated by multiplying the annual energy consumption cost of devices (C_j^{Econs}) with the number of devices used for each SIS component (N_{ij}).

$$C_{Econs}^t = \sum_{i=1}^3 \sum_{j=1}^n C_j^{Econs} \times N_{ij} \quad (6)$$

3.4.2.1. Proof test costs. Next to costs incurred for performing proof tests for each SIS component (C_j^{Ptest}), the downtime cost (DT) associated with proof tests is considered under this cost element. Besides device model/type and the redundancy used for each SIS component, which is denoted by N_{ij} , the cost of performing the proof test for SIS components is influenced by test coverage, test interval, and test policy.

This study assumes that as the coverage increases, the cost of performing a proof test for devices (C_j^{Ptest}) and proof test duration for devices (PTd_{ij}) should increase. Equation (7) shows this relation using two variables PTC_j^P and PTC_j^D as coefficients impacting proof test cost and duration, while test coverage varies. However, there might be cases in which proof test cost and duration act independently from proof test coverage. Moreover, the downtime cost associated with the proof test is also impacted by test coverage and interval. As the test coverage increases, the duration of the test becomes longer, leading to higher downtime costs. Regarding the test interval variable, it is apparent that more frequent proof test means more downtime during the SIS lifecycle and higher proof test cost in total. Equation (7) shows that as the proof

test interval ($PTTI_{ij}$) increases, total proof test cost decreases.

Moreover, the proof test policy (e.g., simultaneous, staggered) can also influence the associated downtime cost throughout the lifecycle. In a simultaneous proof test, all devices under a component (sensor, Safety-PLC, or final element) are tested at the same time. In contrast, a staggered proof test involves scheduling and testing each device individually over the proof test interval. The second one can reduce or avoid the incurred downtime costs associated with proof tests if the SIS is kept in operation during the test without the device being tested. This way, if the decision on proof test policy leads to downtime during the proof test of devices used for each SIS component, PTP_{ij} equals 1 in Equation (7)

$$C_{Prest}^t = \sum_{i=1}^3 \sum_{j=1}^n (PTC_j^p \times C_j^{Ptest} + DT \times PTP_{ij}) \times N_{ij} \times PTC_j^D \times PTd_{ij} \times \frac{12}{PTTI_{ij}} \quad (7)$$

3.4.2.2. Maintenance costs. This section focuses on scheduled maintenance due to the results of the proof test performed for each SIS component. The result of the proof test can lead to either preventive or corrective maintenance for any devices under each SIS component. Preventive maintenance is about repairing the device associated with SIS components to make it as good as new, while corrective maintenance refers to replacing the entire device or part(s) in the device. Therefore, in addition to downtime cost during the maintenance, the maintenance cost includes repair and spare parts expenses for SIS component devices throughout the lifecycle. Although this cost is an operational expenditure, its amount firstly depends on the probability of failure and degradation of SIS components, and secondly, it depends on device specification, redundancy architecture, and proof test interval. Moreover, more frequent proof tests can increase the chance of diagnosing a device before it becomes useless, replacing preventive maintenance with corrective maintenance, which might incur higher costs.

This way, Equation (8) present the total annual maintenance cost, containing both preventive and corrective maintenance costs. The first part of the formula relates to preventive maintenance, while the second part calculates corrective maintenance costs. Since it is probable that a device requires either preventive maintenance or corrective maintenance, Equation (8) considers the occurrence of preventive and corrective maintenance for devices used for SIS components during a proof test by PM_{ij} and CM_{ij} , respectively. The remaining part of the formula follows the same structure for both maintenance costs. During each proof test, if either preventive maintenance or corrective maintenance is required for devices used for each SIS component, the cost of performing maintenance (C_j^{PM} or C_j^{CM}) plus downtime cost (DT) are considered with respect to the number of devices used for each SIS component (N_{ij}) and duration of a specific type of maintenance (PMd_{ij} or CMd_{ij}).

$$C_{Maint}^t = \sum_{i=1}^3 \sum_{j=1}^n \left(\left((C_j^{PM} + DT) \times N_{ij} \times PMd_{ij} \times \frac{12}{PTTI_{ij}} \right) \times PM_{ij} + \left((C_j^{CM} + DT) \times N_{ij} \times CMd_{ij} \times \frac{12}{PTTI_{ij}} \right) \times CM_{ij} \right) \quad (8)$$

3.4.3. Risk cost

Many publications in the literature (almost 60%) introduced another category of SIS LCC, next to capital and operational expenditures. According to IEC 61511, risk cost does not explicitly refer to any phase in the SIS lifecycle framework. Although it is incurred throughout the SIS lifecycle after the commissioning phase, it does not represent an operational expenditure. This study classifies spurious trip and incident costs under the risk cost category. Despite a few publications in the literature presenting the spurious trip cost under operating costs, the remaining papers introduce the consequences of spurious trips as a standalone or risk/failure-related cost category. Those studies in literature that

comprise risk/failure-related cost mostly present the catastrophic consequences of the SIS failing to respond to hazardous events. In this research, the incident cost represents costs associated with the catastrophic consequences of SIS failure throughout the safety lifecycle.

$$C_{Risk}^t = C_{SPT}^t + C_{Inc}^t \quad (9)$$

3.4.3.1. Spurious trip cost. This cost belongs to the situation in which SIS trips the process while no demand. This way, this false error causes expenses within the SIS lifecycle, including downtime and maintenance. Once a spurious trip occurs in the operation, the SIS shuts down the process, and it is required to inspect and fix the issue to take the SIS to the operational mode again. However, the total annual spurious trip cost, which is denoted by C_{SPT}^t , depends on spurious trip rate. Meaning, this cost only incurs based on the probability of spurious trip occurrence, which is denoted by $SPTR$. Nonetheless, every time a spurious trip happens, it is required to inspect all devices used in SIS components. This way, the first part of Equation (10) represents incurred expenses for inspection of devices used in each SIS component. The inspection cost includes the cost of performing the inspection for each device C_j^{Insp} and downtime cost (DT) subject to the duration of inspection ($Inspd_{ij}$). Followed by inspecting all devices used for SIS components, it may be necessary to perform maintenance. Therefore, the second and third parts of Equation (10) represent preventive and corrective maintenance costs, respectively. The formula for calculating both maintenance costs is similar to that of maintenance cost under operating cost categories. The only difference here is that maintenance costs are not tied to the proof test interval.

$$C_{SPT}^t = \sum_{i=1}^3 \sum_{j=1}^n \left(\left((C_j^{Insp} + DT) \times N_{ij} \times Inspd_{ij} \right) + \left((C_j^{PM} + DT) \times N_{ij} \times PMd_{ij} \right) \times PM_{ij} + \left((C_j^{CM} + DT) \times N_{ij} \times CMd_{ij} \right) \times CM_{ij} \right) \times SPTR \quad (10)$$

3.4.3.2. Incident cost. Like any other system, an SIS also operates with a certain level of reliability, availability, and performance. Despite the risk reduction factor for an SIS is considered in the SIS design, there is always a certain amount of remaining risk after putting an SIS into operation. The residual risk accounts for potential expenses due to the probability of its catastrophic consequences, even though this residual risk is acceptable by the field and industry standards. In another words, catastrophic consequences of the SIS failing to respond to hazardous events can be monetized with expected value of those outcomes accumulated over the SIS operational life. Therefore, half of the studies in literature (47%) include this cost in the economic analysis of decision-making about SIS design and implementation. Since this cost occurs once an incident happens due to SIS's failure to respond, this research effort refers to this expense as incident cost. Like spurious trip cost, incident cost also might incur over the SIS life cycle based on the amount of residual risk (R). Therefore, Equation (11) shows that the annual incident cost is calculated by multiplying the cost of catastrophic consequences of an incident (C_{Hazard}) by residual risk (R). Considering this cost element in the SIS LCC framework enables an economic comparison among different SIS design that all fall under same SIL with different residual risk.

$$C_{Inc}^t = R \times C_{Hazard} \quad (11)$$

3.4.4. End-of-life cost

Only a few publications in the literature refer to decommissioning an SIS at the end of its lifecycle. The end of the SIS lifecycle cost category includes the decommissioning cost for each SIS component category (sensor, Safety-PLC, Final element) at the end of the SIS lifecycle. This study assumes that decommissioning occurs once per SIS component, upon completion of the SIS lifecycle. This cost is influenced by device

type and the redundancy architecture of each SIS component. Hence, Equation (12) calculates this cost by multiplying the decommissioning cost per device (C_j^{Decom}) by the number of each particular device used for each SIS component (N_{ij}).

$$C_{Decom} = \sum_{i=1}^3 \sum_{j=1}^n C_j^{Decom} \times N_{ij} \quad (12)$$

4. Discussion

Based on the result of the systematic literature review, several perspectives relevant to the SIS LCC modeling topic have been identified. These perspectives are concerned with the impact of risk costs, downtime cost weight, cyber-attack threats, SIS applications, impact of SIL and system complexity on SIS LCC, and systematic failures on SIS LCC. Each specific perspective is further discussed in the following subsections individually.

4.1. Incorporating risk costs in the SIS LCC model

The inclusion of risk costs in the SIS LCC analysis is still a matter of discussion amongst researchers. While many researchers recommend SIS LCC models that include capital and operational costs, there exist publications in the literature that consider risk costs as an extra cost category in cost-effectiveness assessments of SIS. The differences observed in the literature stem from contrasting interpretations of the scope and purpose of SIS LCC analysis, rather than from cost modelling preferences.

From an economics perspective, ignoring risk costs leads to a more straightforward SIS LCC model, but it cannot account for the economic implications of less-frequent events with catastrophic impact that SIS is primarily implemented to avoid. As underscored by researchers such as Redutskiy (2017b) and Torres-Echeverría et al. (2009b), risk costs can be significant, containing consequences of asset and environmental damage, and even loss of human life. Hence, extending the SIS lifecycle cost framework to include risk-related costs allows for quantification of the expected economic impact of the accepted residual risk and spurious trip accumulated over SIS lifecycle.

Within the risk costs category, spurious trip cost represents relatively frequently incurred costs with non-hazardous implications, causing only downtime and maintenance. Although half of the publications in the literature consider process downtime as an objective besides lifecycle cost, calculating the economic implications of spurious trips as part of the lifecycle cost is also considered by them. On the other hand, incident cost shows the economic impact of the remaining risk after implementing SIS to safeguard a particular process unit. Hence, including incident cost allows selection of economically preferable SIS design solutions within the region of acceptable risk and supports aggregation of expected losses across multiple SIFs at the plant level.

Here, all researchers consider either the probability of failure on demand (PFD) or the risk reduction factor (RRF) as objectives in their studies. However, incorporating incident cost requires agreement on an acceptable PFD/RRF for a specific hazardous event, depending on the conducted HAZOP. This way, conservative PFD/RRF calculation leads to higher SIS capital and operating costs and less incident cost, significantly influencing SIS LCC calculation outcomes. Moreover, incident cost often corresponds to the estimated catastrophic consequences in case the SIS does not react when demanded. If the economic impact of these consequences is overestimated, the calculated incident cost may dominate the total SIS LCC, leading to unnecessarily costly SIS designs.

To sum up, including risk costs in SIS LCC allows decision makers to step beyond basic CapEx/OpEx consideration and acknowledge the impact of SIS failure. Besides, adding risk costs to SIS LCC provides a more thorough and practical economic basis for decision-making, while part of the literature considers this non-compulsory. Nevertheless, it is

worth noting that quantifying both spurious and incident costs must be supported by uncertainty analysis.

4.2. Impact of different cost elements on SIS LCC

As mentioned earlier in this research, the total SIS LCC comprises various cost elements: SIS design cost, SIS commissioning/installation cost, SIS components purchase cost, SIS energy consumption cost, SIS proof test and maintenance costs (including downtime cost), spurious trip cost (including downtime cost), and incident cost (including catastrophic consequences of residual risk). However, these cost elements vary greatly in magnitude and financial weight. While costs such as SIS components purchase are moderately predictable and often marginal in scale, planned and unplanned downtime costs, which are incurred due to maintenance/proof test and spurious trips, they can be disproportionately huge and unpredictable.

In particular, the cost of taking a process offline for scheduled maintenance or proof testing can exceed the value of the SIS components themselves, even for short-term durations. This consequence is even more noticeable in the case of unscheduled downtime resulting from spurious trips. Such events can lead to unexpected production losses, equipment resets, and broader operational disruption, such as contractual penalties for supply delay. For instance, in many different contexts within process industries, a single hour of unplanned shutdown may incur a cost several times greater than the full purchase price of an individual SIS component.

For future research, this demonstrates the requirement of distinguishing cost components not only by category but also by their potential economic impact. A more nuanced understanding of how (planned or accidental) downtime dominates LCC will be essential in developing SIS designs that are both technically robust and economically optimized.

4.3. Incorporating cybersecurity impact on SIS LCC

Like any other digital systems, an SIS, including its sensors, Safety-PLC, communication interfaces and final elements, which might be integrated with an existing network, is vulnerable to cyber-attacks. This vulnerability increases concerns because cyber-attacks can affect the SIS's reliability and integrity. More specifically, malicious manipulation may falsify sensor information, modify or inhibit Safety-PLC logic, alter actuator commands, or prevent a final element from executing the required safety action. Such effects may result either in a dangerous impairment of the SIF, in which the SIS fails to respond correctly to a genuine process demand, or in spurious activation, which may cause an unnecessary process shutdown and associated production losses. Historical analyses of cybersecurity-related incidents in the process industry confirm that cyber-attacks have affected operational technology systems and, in some cases, have contributed to production outages or physical events with potentially severe consequences (Iaiani et al., 2021a; Ylönen et al., 2022). Moreover, malicious manipulation of both BPCS and SIS may contribute to major accident scenarios, indicating that cyber threats can challenge assumptions concerning the availability and independence of protection layers (Iaiani et al., 2021b; Iaiani et al., 2023).

In practice, safety and cybersecurity are usually addressed independently, each treated by its own standards, respectively, IEC 61511 and IEC 62443. These standards utilize separate terminologies, which are not aligned in terms of risk models and assessment methods, causing complexity in SIS designs. This separation is particularly relevant for SIS lifecycle assessment because conventional functional-safety analyses primarily address random hardware failures, systematic failures, and human errors, whereas intentional cyber manipulation may create combinations of failures or process states that are not sufficiently captured by conventional safety analyses (Ylönen et al., 2022). To inject SISs' vulnerability to cyber-attacks into SISs' lifecycle, an approach must

be employed to examine how cybersecurity risks may affect the effective risk reduction delivered by the SIS and the assumptions underlying SIL verification (Deconinck et al., 2025). In particular, cybersecurity-induced unavailability or inhibition of a SIF may increase the likelihood that the protection function is unavailable when demanded, whereas malicious or unintended activation may introduce an additional source of spurious trips. These effects provide a direct link between cybersecurity scenarios, SIS performance, and lifecycle economic consequences.

The literature review also demonstrates a huge gap in explicitly addressing the integration of cyber-attack consequences into the SIS LCC modeling. Although the reviewed literature focuses on modeling LCC for SIS to optimize the design and implementation, there are few publications measuring the economic implications of SIS vulnerability to cyber-attacks throughout its lifecycle. Nevertheless, Redutskiy (2017b) offers a decision variable, so-called physical/electrical separation, to mitigate common-cause failures. This decision variable could be used to decrease the likelihood of simultaneous failure while an SIS is designed in a redundant architecture, a principle that also applies in the context of cybersecurity threats. Although originally considered from a functional-safety perspective, physical/electrical separation may also support cybersecurity by limiting connectivity and increasing independence between redundant SIS components or between the SIS and BPCS, thereby reducing the possibility that a single malicious action compromises multiple protection functions.

Within the proposed SIS LCC framework, cybersecurity-related scenarios can be incorporated through several cost pathways. First, a cyber scenario that impairs or bypasses a SIF and thereby increases the likelihood of an unmitigated hazardous event can be represented in the risk cost through the scenario likelihood and its associated accident consequences. Second, a cyber-induced false activation or manipulated trip of the SIS can contribute to operating cost through production downtime, restart activities, and spurious-trip consequences. Third, costs associated with recovery after a cybersecurity incident, such as investigation, system restoration, revalidation, additional proof testing, software updates, or component replacement, can also be represented as operating costs. Finally, investment in preventive cybersecurity safeguards, including network segmentation, restricted communication paths, physical or electrical separation, secure architecture, and additional security-related hardware or engineering activities, can be considered as additional capital or operating costs in the LCC framework (Iaiani et al., 2023).

From the above-mentioned research, it can be suggested that similar decision variables (e.g., network separation, isolating SIS from BPCS, etc.) and capital/operating cybersecurity countermeasures cost could be used while modeling SIS LCC to incorporate cybersecurity in SIS design strategies. Accordingly, a cybersecurity scenario can be mapped to (i) the affected SIS component or function, (ii) its consequence for SIS performance, such as dangerous unavailability or spurious activation, (iii) the resulting process consequence, such as loss of protection, production shutdown, or a major accident, and (iv) the corresponding capital, operating, or risk cost in the LCC model.

Thus far, these potential decision variables and cost elements have not been included within the presented SIS LCC models in this research. Therefore, further research is required to identify and validate relevant decision variables and cost elements to effectively map the impact of cybersecurity on the economic evaluation of SISs throughout their lifecycle. Further work should also quantify cyber-induced changes in SIS performance, estimate the likelihood and economic consequences of relevant cyber scenarios, and validate how cybersecurity investments and residual cyber risks can be represented within SIS lifecycle economic evaluation.

4.4. Impact of different SIS applications on SIS LCC

According to IEC 61511, all SIS applications have to go through

particular phases (design and engineering, installation and commissioning, operation and maintenance, modification, decommissioning) throughout the SIS lifecycle. Besides, SIS fundamentally includes three components (sensor, Safety-PLC, and final elements), no matter what application is assigned to it. Therefore, the application of SIS does not alter the lifecycle phases and its fundamental structure. Accordingly, the SIS LCC model is not altered across the SIS applications existing in the industry. Meaning, the structure of the SIS LCC model remains the same while evaluating various SIS applications to avoid a risky situation. Nevertheless, the amount of each cost element might differ from one SIS application to another.

The type of safety function designed within an SIS application to safeguard a process unit from a hazardous event fundamentally influences identified decision variables, especially the choice of device type/model for SIS components. Different device types/models have diverse specifications, which can directly influence purchasing cost in the capital cost category. The device specifications can also indirectly differ from other SIS LCCs, such as proof testing and maintenance costs. In addition to safety function alteration from one SIS application to another, the change in process unit protected by a SIF can also impact SIS LCC. For instance, downtime costs involved in proof testing, maintenance, and spurious trip costs might fluctuate from one process unit to another.

Consequently, the SIS LCC can be altered directly by changes in decision variables due to variations in the designed safety functions in an SIS application. Moreover, process units protected by a specific SIF from hazardous events might directly influence existing cost elements within the SIS LCC model. To thoroughly understand the impact of various SIS applications (safety function and process unit) on SIS LCC, extensive research is required.

4.5. Impact of systematic failures on SIS LCC

Within the functional safety topic, two types of failure can happen in the SIS lifecycle: systematic failures and random failures. Random failures occur unpredictably due to hardware degradation or aging and can be analyzed statistically, while systematic failures are caused by flaws in design, specification, configuration, software, or human error. Systematic failures are repeatable and often triggered under specific conditions. They are not inherent to physical components but are instead embedded in the way SIS is designed, built, or operated. Hence, they require process discipline, rigorous validation, and competent engineering practices to prevent.

In case systematic failures are overlooked in the design and implementation of an SIS, the consequences often appear during the entire lifecycle. Problems such as selecting an improper device for an SIS component, a fault in logic programming, and incomplete verification may not cause immediate failure, but they can lead to rework, delays, increased maintenance demands, and operational inefficiencies. These failures can also raise the frequency of spurious trips and reduce SIS reliability, increasing incident and downtime costs. Moreover, ignoring systematic failures drastically leads to overestimated risk reduction factors, increasing the likelihood of hazardous events with severe financial and catastrophic consequences.

From SIS design to decommissioning, ignoring systematic failures can increase LCCs in ways that are often unknown until they cause a problem. Hence, it is crucial to incorporate them, not only to increase SIS reliability but also to have more accurate SIS LCC estimation. As current available research focuses on multi-objective decision making about SIS implementation, future research should consider the quantitative evaluation of how the incorporation of systematic failure management influences SIS LCC and reliability. Proposing methods to clearly predict these impacts could provide valuable insights for improving SIS design in process industries.

4.6. Impact of SIL and system complexity on SIS LCC

Publications focusing on optimization of SIS design, presented in the literature of SIS LCC, consistently prove that there exists a relationship between SIL and lifecycle cost. The uncovered relationship is depicted as a non-linear and stepwise pattern rather than proportional. Although satisfying higher SIL generally leads to higher SIS lifecycle cost, the magnitude of the cost increase is not uniform across SIL levels. In a process unit with a low SIL requirement, moderate improvements in PFD can be obtained using relatively low-cost measures such as slightly more sophisticated SIS component, minor redundancy in SIS component design, or adjustment of proof test intervals, resulting in a gradual surge in LCC. However, when targeting a higher SIL, it might be needed to have additional redundancy, diversity, and enhanced diagnostics. These requirements introduce lifecycle cost escalations, significantly increasing in LCC for incremental SIL improvements. The SIS design optimization papers in the literature of SIS LCC often jointly minimize PFD and LCC, presenting that after a certain PFD level, improvements in safety integrity show diminishing returns with respect to cost. Meaning, significant surges in SIS lifecycle cost are needed to obtain relatively small reductions in PFD and accordingly satisfying the targeted SIL. Therefore, the Pareto-optimal relationship between LCC and SIL always depicts a convex curve, where higher SIL is reachable only at disproportionately higher lifecycle costs. This pattern illustrates the impact of SIL on SIS LCC, emphasizing the importance of lifecycle cost consideration when selecting target SIL levels in SIS design.

5. Conclusion

A detailed and structured understanding and analysis of SIS lifecycle costs is essential for ensuring both safety compliance and cost-effective operation in process industries. This study lays an important foundation for a more coherent and comprehensive approach to SIS LCC analysis, with significant implications for both academic inquiry and industry practice. By systematically reviewing the relevant literature, the study provided a comprehensive and structured examination of SIS LCC within process industries. The contributions of this study improve the understanding of SIS LCC calculation by framing SIS cost evaluation as a lifecycle-driven, decision-oriented process.

The paper conducted a systematic literature review on the SIS LCC topic both in process industries and other industries. The results of this literature review are manifold. Firstly, it is uncovered that hazardous events caused by overpressure and high liquid level are the most frequently addressed SIS applications in the literature related to SIS LCC. Secondly, most SIS LCC models in the literature share a common categorization of CapEx and OpEx, while their terminology varies. Besides, almost half of the publications include an extra category containing spurious trip and incident costs. Thirdly, among all identified decision variables impacting SIS LCC, SIS component redundancy architecture and proof testing policy (including test interval and strategy) are the most frequently and deeply discussed decision variables in the literature. Finally, this paper proposed a comprehensive SIS LCC calculation framework to be used for individually calculating SIF LCC in an SIS. This framework encompasses four cost categories, namely capital, operating, risk, and end-of-life costs, which appear in approximately 90%, 95%, 60%, and 5% of publications, respectively. A limitation of this review is that the full texts of 35 potentially relevant records could not be accessed, which may have affected the completeness of the literature coverage and should be considered when interpreting these findings.

Furthermore, this review paper also provides perspectives on the SIS LCC topic, demonstrating potential directions for future research. These topics span from incorporating the impact of risk costs, cybersecurity, weight of downtime cost, systematic failure, and SIS applications into the SIS LCC framework. It is recommended that further research be conducted to quantitatively assess these factors and integrate them into a more dynamic and adaptive SIS LCC framework. Such research could

enhance the precision and applicability of LCC models, support more informed decision-making, and better reflect the evolving complexity of SIS design and operation in modern process industries.

CRedit authorship contribution statement

Mehran Farzadmehr: Writing – review & editing, Writing – original draft, Visualization, Validation, Methodology, Investigation, Data curation, Conceptualization. **Philippe Nimmegeers:** Writing – review & editing, Supervision, Methodology, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research was supported by the VLAIO (Flanders Innovation and Entrepreneurship)-CATALISTI FUNCTIONARY-I CSBO project (grant number: HBC.2024.0786). Philippe Nimmegeers holds an FWO senior postdoctoral fellowship (grant number: 1215523 N) granted by FWO Vlaanderen/Research Foundation Flanders.

Data availability

Data will be made available on request.

References

- Berrah, F., Chebila, M., Innal, F., Got, A., 2023. Cost effective analysis of the design of safety instrumented systems using manta-ray foraging optimization algorithm. *International Journal of Safety & Security Engineering* 13 (6).
- Cai, B., Li, W., Liu, Y., Shao, X., Zhang, Y., Zhao, Y., Liu, Z., Ji, R., Liu, Y., 2021. Modeling for evaluation of safety instrumented systems with heterogeneous components. *Reliab. Eng. Syst. Saf.* 215, 107823. <https://doi.org/10.1016/j.res.2021.107823>.
- Carreras Guzman, N.H., Kozine, I., Lundteigen, M.A., 2021. An integrated safety and security analysis for cyber-physical harm scenarios. *Saf. Sci.* 144, 105458. <https://doi.org/10.1016/j.ssci.2021.105458>.
- Chebila, M., 2023. Many-objective robust decision making for efficient designs of safety instrumented systems. *Process Saf. Environ. Prot.* 172, 869–881. <https://doi.org/10.1016/j.psep.2023.02.059>.
- Cheraghi, M., Taghipour, S., 2024. A mathematical optimization model for determining safety integrity levels in process facilities. *Reliab. Eng. Syst. Saf.* 243, 109896. <https://doi.org/10.1016/j.res.2023.109896>.
- Deconinck, G., Luyts, J., Boogaerts, G., 2025. Exploring complementarity between functional safety and cybersecurity in the chemical process industry. 20th European Dependable Computing Conference Companion Proceedings. IEEE.
- Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021a. Analysis of cybersecurity-related incidents in the process industry. *Reliab. Eng. Syst. Saf.* 209, 107485. <https://doi.org/10.1016/j.res.2021.107485>.
- Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V., 2021b. Major accidents triggered by malicious manipulations of the control system in process facilities. *Saf. Sci.* 134, 105043. <https://doi.org/10.1016/j.ssci.2020.105043>.
- Iaiani, M., Tugnoli, A., Cozzani, V., 2023. Process hazard and operability analysis of BPCS and SIS malicious manipulations by POROS 2.0. *Process Saf. Environ. Prot.* 176, 226–237. <https://doi.org/10.1016/j.psep.2023.06.024>.
- Innal, F., Dutuit, Y., Chebila, M., 2015. Safety and operational integrity evaluation and design optimization of safety instrumented systems. *Reliab. Eng. Syst. Saf.* 134, 32–50. <https://doi.org/10.1016/j.res.2014.10.001>.
- International Electrotechnical Commission, P. 2010. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems. *IEC Standards Online*.
- International Electrotechnical Commission. 2017. IEC 61511-1: Functional safety-Safety Instrumented Systems for the Process Industry Sector-Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements.
- Jahanian, H., 2017. Optimization, a rational approach to SIL determination. *Process Saf. Environ. Prot.* 109, 452–464. <https://doi.org/10.1016/j.psep.2017.04.015>.
- John Satur, D., Kim, J., Bae, M., Kim, S.-Y., Lee, Y., 2016. Cost effective alternative in meeting the required Safety Integrity Level (SIL). *J. Loss Prev. Process Ind.* 40, 406–418. <https://doi.org/10.1016/j.jlp.2015.12.023>.
- Julsereewong, A., Thepmanee, T., 2017. Safety instrumented system design in consideration of cost-benefit analysis: a case study of tail gas treating process. In:

- 2017 17th International Conference on Control, Automation and Systems (ICCAS), pp. 637–642. <https://doi.org/10.23919/ICCAS.2017.8204307>.
- Longhi, A.E.B., Pessoa, A.A., de Almada Garcia, P.A., 2015. Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees. *Reliab. Eng. Syst. Saf.* 142, 525–538. <https://doi.org/10.1016/j.res.2015.06.010>.
- Machleidt, K., Litz, L., 2011. An optimization approach for safety instrumented system design. *Proceedings - Annual Reliability and Maintainability Symposium 2011*, 1–6. <https://doi.org/10.1109/RAMS.2011.5754503>.
- Ouache, R., Kabir, M.N., 2016. Models of probability of failure on demand for safety instrumented system using atmospheric elements. In *Safety Science* (vol. 87, 38–46. <https://doi.org/10.1016/j.ssci.2016.03.015>.
- Ouache, R., Kabir, M.N., Adham, A.A.J., 2015. A reliability model for safety instrumented system. *Saf. Sci.* 80, 264–273. <https://doi.org/10.1016/j.ssci.2015.08.004>.
- Rabah, B., Younes, R., Djeddi, C., Laouar, L., 2024. Optimization of safety instrumented system performance and maintenance costs in Algerian oil and gas facilities. *Process Saf. Environ. Prot.* 182, 371–386. <https://doi.org/10.1016/j.psep.2023.11.081>.
- Redutskiy, Y., 2017. Optimization of safety instrumented system design and maintenance frequency for oil and gas industry processes. *Management and Production Engineering Review* 8, 46–59. <https://doi.org/10.1515/mper-2017-0006>.
- Redutskiy, Y. (2017a). Modelling and Design of Safety Instrumented Systems for Upstream Processes of Petroleum Sector. *7th International Conference on Engineering, Project, and Production Management*, 182, 611–618. doi: 10.1016/j.proeng.2017.03.165.
- Redutskiy, Y. (2018). Pilot Study on the Application of Employee Scheduling for the Problem of Safety Instrumented System Design and Maintenance Planning for Remotely Located Oil and Gas Facilities. 10, 55–64. doi: 10.2478/emj-2018-0022.
- Redutskiy, Y., Camitz-Leidland, C.M., Vysochyna, A., Anderson, K.T., Balycheva, M., 2021. Safety systems for the oil and gas industrial facilities: design, maintenance policy choice, and crew scheduling. *Reliab. Eng. Syst. Saf.* 210, 107545. <https://doi.org/10.1016/j.res.2021.107545>.
- Sobral, J., Guedes Soares, C., 2019. Assessment of the adequacy of safety barriers to hazards. *Saf. Sci.* 114, 40–48. <https://doi.org/10.1016/j.ssci.2018.12.021>.
- Squillante Jr., R., Dias, J.C., Moscato, L.A., Junqueira, F., Miyagi, P.E., dos Santos Filho, D.J., 2021. A framework for synthesis of safety-related control design to avoid critical faults and pathogenic accidents in the process industries. *Saf. Sci.* 139, 105168. <https://doi.org/10.1016/j.ssci.2021.105168>.
- Torres-Echeverría, A.C., Martorell, S., Thompson, H.A., 2009a. Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy. *Reliab. Eng. Syst. Saf.* 94 (2), 162–179. <https://doi.org/10.1016/j.res.2008.02.010>.
- Torres-Echeverría, A.C., Martorell, S., Thompson, H.A., 2009b. Modelling and optimization of proof testing policies for safety instrumented systems. *Reliab. Eng. Syst. Saf.* 94 (4), 838–854. <https://doi.org/10.1016/j.res.2008.09.006>.
- Torres-Echeverría, A.C., Martorell, S., Thompson, H.A., 2012. Multi-objective optimization of design and testing of safety instrumented systems with MooN voting architectures using a genetic algorithm. *Reliab. Eng. Syst. Saf.* 106, 45–60. <https://doi.org/10.1016/j.res.2012.03.010>.
- Wacker, H.D., Holub, P., Börcsök, J., 2013. Optimization of diagnostics with respect to the diagnostic coverage and the cost function. In: *2013 XXIV International Conference on Information, Communication and Automation Technologies (ICAT)*, pp. 1–7. <https://doi.org/10.1109/ICAT.2013.6684064>.
- Yasser, R., Youcef, Z., Noureddine, T., 2025. An integrated approach to safety instrumented system lifecycle management: risk evaluation and optimization in the petrochemical industry using genetic algorithms. *Instrumentation Measure Metrologie* 24. <https://doi.org/10.18280/im.240103>.
- Ylönen, M., Tugnoli, A., Oliva, G., Heikkilä, J., Nissilä, M., Iaiani, M., Cozzani, V., Setola, R., Assenza, G., van der Beek, D., Steijn, W., Gotcheva, N., Del Prete, E., 2022. Integrated management of safety and security in Seveso sites – sociotechnical perspectives. *Saf. Sci.* 151, 105741. <https://doi.org/10.1016/j.ssci.2022.105741>.
- Yuan, S., Yang, M., Reniers, G., Chen, C., Wu, J., 2022. Safety barriers in the chemical process industries: a state-of-the-art review on their classification, assessment, and management. *Saf. Sci.* 148, 105647. <https://doi.org/10.1016/j.ssci.2021.105647>.
- Zhang, A., Zhang, T., Barros, A., Liu, Y., 2020. Optimization of maintenances following proof tests for the final element of a safety-instrumented system. *Reliab. Eng. Syst. Saf.* 196, 106779. <https://doi.org/10.1016/j.res.2019.106779>.
- Zhang, A., Srivastav, H., Barros, A., Liu, Y., 2021. Study of testing and maintenance strategies for redundant final elements in SIS with imperfect detection of degraded state. *Reliab. Eng. Syst. Saf.* 209, 107393. <https://doi.org/10.1016/j.res.2020.107393>.
- Zhang, A., Hao, S., Xie, M., Liu, Y., Yu, H., 2023. Inspection and maintenance optimization for heterogeneity units in redundant structure with Non-dominated sorting Genetic Algorithm III. *ISA Trans.* 135, 299–308. <https://doi.org/10.1016/j.isatra.2022.09.029>.