Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P2922-cd

Optimal SIL Allocation to the Safety Functions Implemented over Layers of Protection – Design Sensitivity due to Dependent Failures

Edin Alijagic, PhD

Plant Safety, TÜV SÜD AG, Basel, Switzerland. E-mail: edin.alijagic@tuvsud.com

Abstracts: Safety Instrumented Systems (SIS) based on E/E/PE technology have nowadays become a standard for managing risks in complex technical enterprises. These systems typically use multiple layers of protection to mitigate risks to acceptable levels while ensuring high system availability. Compliance with functional safety standards like IEC 61508/61511 or ANSI ISA-84.01 requires assigning risk reduction factors (RRF) to each safety function and protection layer. IEC 61511 offers guidance on failure detection and prevention but lacks provisions for automatic mitigation systems, such as fire & gas systems. This gap, acknowledged in IEC 61511-4:2020, can lead to unnecessary design costs.

In this paper we address this gap by providing cost-effective SIS design for mitigation layers without compromising the safety. By introducing RRFs as proxies for implementation costs, we use Lagrange optimization to calculate these factors while adhering to the risk equation. Cost-optimal RRFs are calculated for each protection layer, considering an overall risk reduction target, and given loss distribution profile associated to single hazardous category. The model accounts for dependent failures across two successive layers. We demonstrate the algorithm's effectiveness through practical examples involving various loss distribution profiles.

Keywords: IEC61508, *Functional Safety, safety function, PFD&RRF, SIL, Layers of Protection, E/E/PE, SIS, ESD & Fire&Gas System, Lagrange optimization*

1. Introduction

Safety Instrumented Systems (SIS) are widely used in industries for loss prevention and limitation (CCPS 2007, Gruhn & Cheddie 2006). Triggered by accident precursors, these systems implement safety functions (SFs) through various topologies. Designing an SF requires understanding initiating events and consequences, followed by determining the Risk Reduction Factor (RRF) or Safety Integrity Level (SIL) as per Safety Requirement Specifications (SRS) (IEC61508, IEC61511, CCPS 2007, Cornelliusen 2002). These targets guide design decisions, including diagnostic coverage and redundancy to manage systematic and Common-Cause Failures (CCF), though high costs are inherent. Component costs often depend on allocated SIL targets, and redundancy is introduced later to address these costs.

While IEC61508 is widely recognized as the foundational standard for functional safety, its guidance on SIL allocation primarily focuses on frequency (F) of a hazardous event aspect of risk, without explicitly addressing losses (L). The standard frames risk reduction R=F×L but emphasizes risk prevention by reducing frequency to achieve this. As a result, its scope is largely confined to the left side of the bowtie risk model, up to the top event. After the top event is triggered, safety depends on the subsequent layers of protection. The safety measures are applied across Independent Protection Layers (ILPs) to gradually mitigate these losses.

The limitation of IEC61508 in allocating SIL to the safety functions implemented in protection layers has been acknowledged in the recent (IEC61511-4 2020) update, which states that while the methodologies from IEC61508 are still valid, they do not provide guidance for designing mitigation layers.

Allocating SIL to ILPs involves balancing risk tolerance, the number of layers, and risk reduction per layer. Tools like Layers of Protection Analysis (LOPA) (CCPS 2001, Dowell 1998) provide quantitative rigor compared to Risk Graph or Risk Matrix methods (De Salis 2001). LOPA analyzes single cause-consequence pairs identified during HAZOP but

may overlook certain scenarios, risking insufficient RRF allocation (Marszal & Scharpf 2002).

This paper extends the author's earlier paper (Alijagic 2014) to analytically solve the SIL allocation problem for protection layers whose dependent failures, caused by shared components cannot be neglected. This quantitative methodology is designed to assist SIS designers in evaluating the robustness of the layers and promotes cost-efficient design choices for the system architectures.

The proposed approach ensures that the safety targets are met, maintaining alignment with IEC 61508. By avoiding the assignment of unnecessarily high RRF targets, the methodology mitigates the cost implications of added redundancy, diversification, and separation required to address dependent failures arising from shared components across layers.

2. The Structure of the Paper

The introduction provides an overview of the fundamental concepts of protection layers and presents LOPA as a preferred tool for risk analysts to evaluate and quantify residual risks within protection systems. It also highlights a key limitation of the LOPA methodology, for which the author proposes a solution in the form of a one-pass algorithm. The next chapter establishes a formal framework for analytically solving the SIL-allocation problem for a typical Fire & Gas (F&G) SIS. This is followed by a demonstration of the procedure using two protection layers. Subsequently, the sensitivity of the calculated RRFs is analyzed and a four-step design flow is established. Following this, a sketch of the proof is provided, demonstrating that the obtained RRFs are indeed minimal. Finally, chapter Conclusions summarizes the findings and outlines potential future steps.

3. The Main Matter

The conceptual design of the layers of protection for mitigating F&G scenarios in the oil&gas industry are based on the technical guidance from (NORSOK 2008). It introduces two distinct protection layers. The first layer focuses on managing gas releases in process areas caused by loss of containment. The corresponding F&G SIS responds by shutting down and isolating the process node, restricting access and alerting workers in the area with sounders and light beacons, and switches off electrical equipment from the safe areas to prevent ignition and escalation to more severe fire scenarios.

If the first layer fails to execute its safety function, fire scenarios of varying severity may arise as the released gas disperses and ignites—either on hot surfaces of nearby process equipment or through sparks within the enclosures of electrical equipment. To mitigate these events while maintaining high availability, the second protection layer is required. This layer performs controlled depressurization, activates firewater pumps, sprinkler systems, and foam release mechanisms. In electrical equipment rooms, firefighting is performed using neutral gases to effectively suppress flames.

3.1 *Problem setting*

For the two layers of protection as shown in Fig. 1 let L_1, L_2 $(L_1 \le L_2)$ be the severities of the consequences of the hazardous events involved. Let SF1 and SF2 represent the safety functions each implemented within its respective protective layer, while jointly contributing to risk mitigation against a single hazard category.

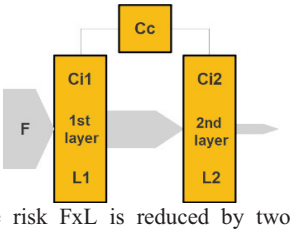

Fig. 1. The risk FxL is reduced by two protective layers that share a component.

As the use of single SIL-certified logic solver is presumed, there will inevitably be shared components C_c involved in executing the safety functions implemented within the layers. In addition to these shared components each protection layer will also include its own independent components $C_{ik}, k = 1, 2$, whose failure does not affect the functioning of the other layer.

Let $P_c = PFD(C_c)$ represent the probability of failure on demand due to dangerous undetected

failures for the shared components C_c, and $P_{ik} = PFD(C_{ik}), k = 1,2$, likewise, represent those for the protective layers' independent components $C_{ik}, k = 1,2$. As Fig. 2 suggests, the PFDs for each individual layer are found as

$$P_k := PFD\left(C_{ik} \,\&\, C_c\right) = P_{ik} + P_c, \quad k = 1,2. \tag{1}$$

The goal of this section is to calculate these PFDs or their respective inverses, RRFs; $\alpha_i := \left(P_k\right)^{-1}, k = 1,2$.

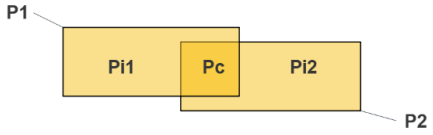

Fig. 2. PFDs of the components used in the implementation of two protective layers.

As the frequency of the hazardous event is F, the risk (R) of the unprotected system is $R = FL_2$. Since this risk is assumed intolerable, we introduce an overall risk reduction factor (RRF); α (≥ 1) to reduce the initial risk to a tolerable level $R^{tol.} = FL_2/\alpha$ which is achieved jointly by the protective layers. The risk equation for the system, once the protection measures are in place, becomes

$$\begin{aligned} R^{tol.} &= FP_cL_2 \\ &+ F\left(1-P_c\right)\left[P_{i1}\left(1-P_{i2}\right)L_1 + P_{i1}P_{i2}L_2\right]. \end{aligned} \tag{2}$$

The impact of parameter P_c is critical here as dangerous undetectable failures in the common component render both the layers unavailable. This puts an upper bound on the overall RRF α, limiting the amount of the risk reduction that can be realized by this component. For example, when $P_c = 0.001$, then the maximal SIL achieved through single architecture is SIL2.

Let $\alpha_{ik} := P_{ik}^{-1}, k = 1,2$ denote the RRFs corresponding to the independent components $C_{ik}, k = 1,2$. Then, equation Eq.(2), after dividing by F and L_2, reduces to the normalized risk equation

$$\frac{\alpha^{-1} - P_c}{1 - P_c} = \frac{l_1}{\alpha_{i1}} + \frac{1 - l_1}{\alpha_{i1}\alpha_{i2}} \tag{3}$$

where $l_1 := L_1/L_2 \ (\leq 1)$.

The problem of finding PFDs $P_k, k = 1,2$ through PFDs $P_{ik}, k = 1,2$ is now replaced by first finding minimal RRFs $\alpha_{ik}, k = 1,2$ for independent components from each protection layer. As Eq.(3) has two unknowns $\alpha_{ik}, k = 1,2$, the minimal RRFs for the independent components can only be found by introducing an additional equation. The additional equation can be obtained by solving the optimization task

$$\begin{aligned} &\min\left\{\alpha_{i1} + \alpha_{i2} + 1/\alpha_{i2} + 1/\alpha_{i2}\right\} \\ &\text{such that } \frac{\alpha^{-1} - P_c}{1 - P_c} = \frac{l_1}{\alpha_{i1}} + \frac{1 - l_1}{\alpha_{i1}\alpha_{i2}} \end{aligned} \tag{4}$$

The minimization objective is chosen such that the optimization task is feasible. That is, it ensures that $\alpha_{i2} = 1$ when $l_1 = 1$ and that $\alpha_{i2} = \sqrt{\alpha}$ when $l_1 = 0$ as well as that $1 \leq \alpha_{i2} \leq \alpha_{i1} \leq \alpha$. However, there are new insights; the task specified by Eq.(4) implies that $\alpha_k = \alpha_{ik} = P_{ik}^{-1}, k = 1,2$ when the layers are independent ($P_c = 0$) (see Fig. 3). We denote these RRFs as $\alpha_k^{IND} := \alpha_{ik}(P_c = 0), k = 1,2$ to distinguish them from the case when $P_c \neq 0$.

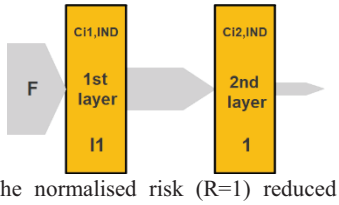

Fig. 3 The normalised risk (R=1) reduced by two independent protection layers ($P_c = 0$).

It is clear now that we first set out to find $\alpha_k^{IND}, k = 1,2$, then increase these RRFs by P_c^{-1} to determine $\alpha_{ik}, k = 1,2$ for the purely independent component parts.

The optimization task for $P_c = 0$ becomes

$$\begin{aligned} &\min\left\{\alpha_1^{IND} + \alpha_2^{IND} + 1/\alpha_1^{IND} + 1/\alpha_2^{IND}\right\} \\ &\text{such that } 1/\alpha = l_1/\alpha_1^{IND} + (1 - l_1)/\alpha_1^{IND}\alpha_2^{IND} \\ &\text{and } 1 \leq \alpha_2^{IND} \leq \alpha_1^{IND} \leq \alpha. \end{aligned} \tag{5}$$

The optimal values α_k^{IND}, $k=1,2$ for Eq.(5) are calculated in Chapter 4. The values amount at

$$\alpha_1^{IND} = \alpha\left(l_1 + \frac{1-l_1}{\alpha_2^{IND}}\right), \qquad (6)$$
$$\alpha_2^{IND} = 1 + (\sqrt{\alpha} - 1)\sqrt{1-l_1}$$

Building on the previous insights, we can calculate the optimal RRFs α_k, $k=1,2$ as

$$\alpha_k = \frac{\alpha_k^{IND}}{1 - P_c\alpha_k^{IND}},\ k=1,2. \qquad (7)$$

The RRFs α_{ik}, $k=1,2$ for the independent components C_{ik}, $k=1,2$ of the protection layers follow from Eq.(1) and previously calculated α_k, $k=1,2$ as

$$\alpha_{ik} = \frac{\alpha_k}{1 - P_c\alpha_k},\ k=1,2 \qquad (8)$$

Finally, we use the β-factor model from IEC61508 to quantify CCFs. In this case one obtains

$$\beta = \frac{P_c}{P_c + \alpha_{i1}^{-1} + \alpha_{i2}^{-1}} \qquad (9)$$

Although traditionally applied to redundant systems, β-factor remains relevant for analyzing CCF in non-redundant configurations such as multiple protection layers implemented on a single safety PLC.

3.2 *Examples*

The formulas given by Eq.(6), Eq.(7) and Eq.(9) are demonstrated and verified on example of a hypothetical SIL3-certified safety instrumented system (SIS) with $PFD(C_c) = P_c = 1.0E-4$ accommodating two layers of protection and several values for loss l_1. The upper bound for the overall RRF α for this system is set to $\alpha_{\max} := P_c^{-1} = 1.0E+4$, and the following four cases are discussed over the range $[1, \alpha_{\max}]$ of overall RRFs.

Case A; The optimal RRFs α_k^{IND}, $k=1,2$ for independent protection layers ($P_c = 0$) and very small l_1 ($l_1 = 0.1\%$) are shown in the top subplot of Fig. 4. When l_1 approaches 0 - meaning the first layer provides no risk reduction - both RRFs α_k^{IND}, $k=1,2$ become equal to $\sqrt{\alpha}$. In this scenario, the system behaves as a single protection layer with two safety functions operating redundantly against a single hazardous scenario.

The middle subplot ($P_c = 0.0001$) illustrates how the minimal RRFs increase compared to the top subplot ($P_c = 0$) – see the values indicated by the arrows on the dashed vertical lines. This increase is expected, as the criticality of the common component starts influencing the minimal RRFs. The bottom subplot shows how the β-factor changes along α for this l_1. When the overall RRF α is set to be smaller than the threshold $1.0E+4$ (for example 8000), both SFs have their minimal RRFs equal 100 (corresponding to SIL2). Any other SIL3-rated SIS in this case, with β smaller than approximately 0.0047, provides a sufficient safety margin.

Case B & Case C: Shown in Fig. 5 ($l_1 = 25\%$) and Fig. 6 ($l_1 = 50\%$) these cases represent more realistic scenarios of RRF-allocations across two protection layers. They convey a message similar to that of Case A. As expected, with increasing l_1, the first layer must cover even greater risks than in Case A. Therefore, α_1 in the middle subplot increases faster along with increasing allocated loss l_1, while α_2 decreases but remains higher than its value in Case A for the same α.

Case D: This extreme case ($l_1 = 99\%$) exhibits an interesting behaviour for large l_1. The upper bound on the overall RRF; $\alpha_{\max}$ is no longer P_c^{-1} but is significantly affected by l_1. In this scenario, the maximal achievable overall RRF that can be realized by this SIL3 system is no longer 10E+4 but has been reduced to approximately half that value - see the range of the greyed-shaded area in Fig. 7. This indicates that the capability of single PLC in the protection layers depends heavily on the accepted risk per layer, providing a crucial insight for the designers of safety instrumented systems.

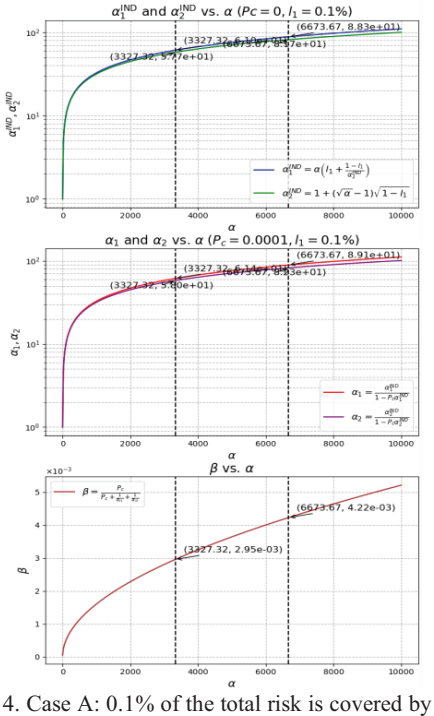

Fig. 4. Case A: 0.1% of the total risk is covered by the 1st layer

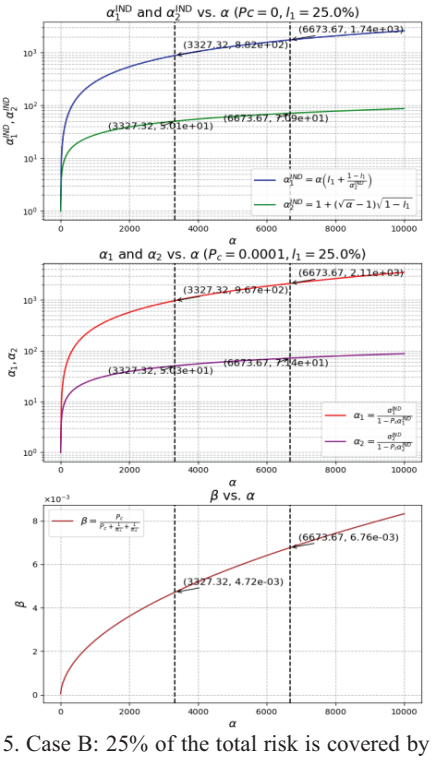

Fig. 5. Case B: 25% of the total risk is covered by the 1st layer

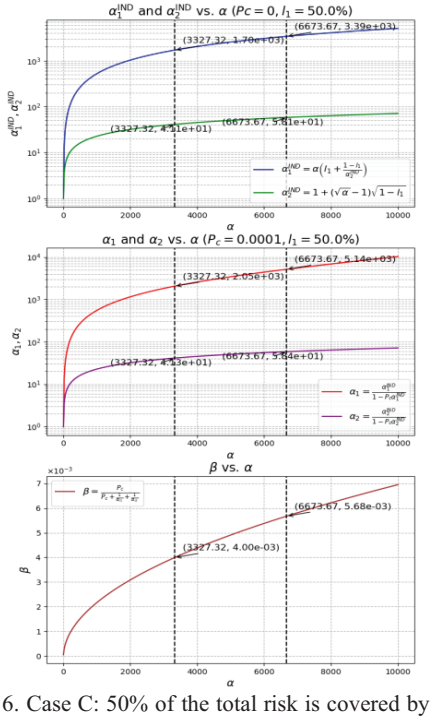

Fig. 6. Case C: 50% of the total risk is covered by the 1st layer

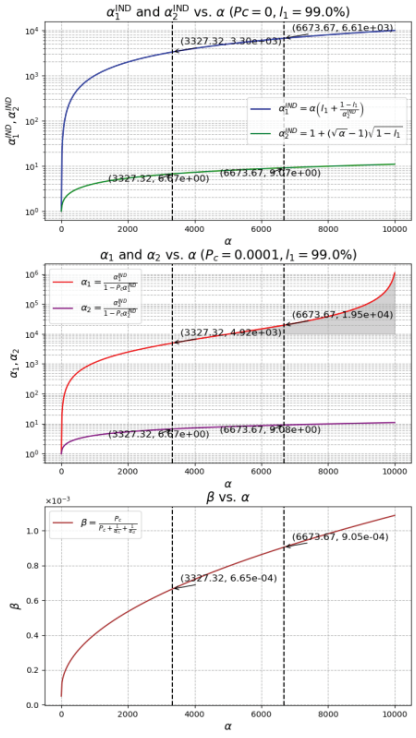

Fig. 7. Case D: 99% of the total risk is covered by the 1st layer

3.3 *Relative sensitivity of the RRFs on small changes in parameter*

When it is decided to incorporate a safety margin into a protection layer's PFD, the RRFs of the implemented SFs need be updated to adequately address the new tolerable risk level. To achieve this, it is necessary to determine which variable have the most impact on the layer's RRF and tune the system accordingly.

It is convenient to use relative sensitivities to express dependency on small changes in variables. The relative sensitivities of $\alpha_k, k=1,2$ with respect to P_c, α, l_1 are calculated using formula

$$S_{f(x),x} = \frac{\partial f(x)}{\partial x}\frac{x}{f(x)} \tag{10}$$

Here, $f(x)$ is the function for which we want to find the sensitivity, and x is the variable of interest. In our case this function is $f=\alpha_k$, $k=1,2$ as given by Eq.(7) and the sensitivity in the vicinity of specific point x_0 is determined for specific values of $P_c = P_{c0}$, $\alpha=\alpha_0$ and $l_1 = l_{1,0}$ using the following formulae:

(i) relative sensitivity of $\alpha_k, k=1,2$ with respect to P_c;

$$S_{\alpha_k,P_c} = \frac{\partial \alpha_k}{\partial P_c}\frac{P_c}{\alpha_k} = \frac{\alpha_k^{IND} P_c}{1-\alpha_k^{IND} P_c}, \tag{11}$$

(ii) relative sensitivity of $\alpha_k, k=1,2$ with respect to α;

$$S_{\alpha_k,\alpha} = \frac{\partial \alpha_k}{\partial \alpha}\frac{\alpha}{\alpha_k} = \frac{\partial \alpha_k}{\partial \alpha_k^{IND}}\frac{d\alpha_k^{IND}}{d\alpha}\frac{\alpha}{\alpha_k}, \tag{12}$$

(iii) relative sensitivity of $\alpha_k, k=1,2$ with respect to l_1;

$$S_{\alpha_k,l_1} = \frac{\partial \alpha_k}{\partial l_1}\frac{l_1}{\alpha_k} = \frac{\partial \alpha_k}{\partial \alpha_k^{IND}}\frac{d\alpha_k^{IND}}{dl_1}\frac{l_1}{\alpha_k} \tag{13}$$

where α_k^{IND}, $k=1,2$ are given by Eq.(6). Typically, overall RRF α is adjusted to increase to $\alpha+\Delta\alpha$ for some positive $\Delta\alpha$. This change aims at recalculating the RRF factors and checking them through the risk equation given by Eq.(3). The updated RRFs based on $\alpha+\Delta\alpha$ are such that the right hand side of Eq.(3) is smaller than its left hand side which is based on α. This indicates that the safety reserve is built in this safety system.

Finally, the design flow for determining and optimizing the minimal factors $\alpha_k, k=1,2$ is given in Fig. 8. The flow is designed to assist designers of SIS systems in systematically allocating RRFs across the layers of protection.

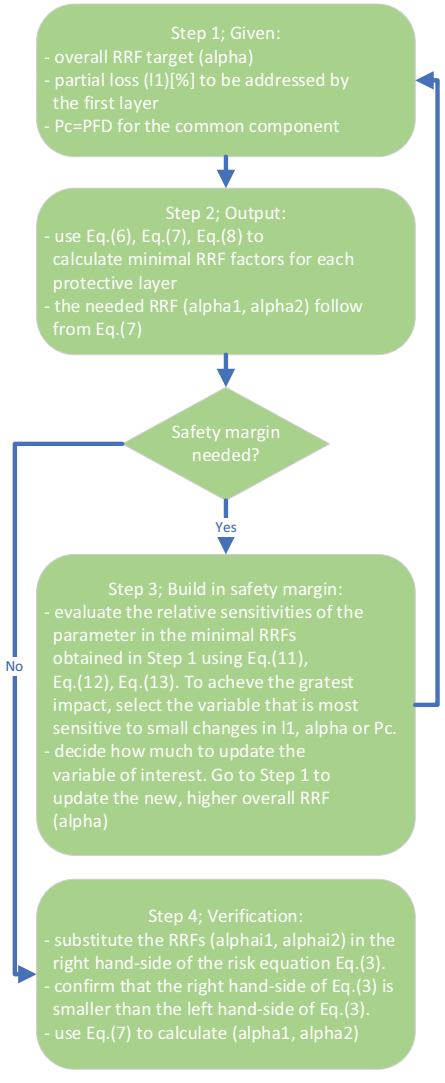

Fig. 8. Four-step procedure for SIL&RRF-allocation in a two-layered SIS with single logic solver.

4. The Proof

In this section we show that α_k^{IND}, $k=1,2$ are indeed optimal for the optimization problem Eq.(5). We use the standard tools from calculus of variations and associate a so-called lagrangian Λ along with the stationarity conditions as per Eq.(5) as follows

$$\Lambda := \lambda\left\{l_1/\alpha_1^{IND} + (1-l_1)/\alpha_1^{IND}\alpha_2^{IND} - \alpha^{-1}\right\} + \alpha_1^{IND} + \alpha_2^{IND} + 1/\alpha_1^{IND} + 1/\alpha_2^{IND}, \quad (14)$$

$$\frac{\partial\Lambda}{\partial\lambda} = 0, \quad \frac{\partial\Lambda}{\partial\alpha_k^{IND}} = 0, \quad k=1,2 \quad (15)$$

where λ is the so-called Lagrange multiplier. The choice of the objective function

$$\alpha_1^{IND} + \alpha_2^{IND} + 1/\alpha_1^{IND} + 1/\alpha_2^{IND}$$

is critical here. The function is chosen to trade-off between the linear growth (captured by $\alpha_1^{IND} + \alpha_2^{IND}$) and the reciprocal decay (captured by $1/\alpha_1^{IND} + 1/\alpha_2^{IND}$).

Applying the stationarity conditions from Eq.(15) on the langrangian from Eq.(14), yields

$$0 = 1 - \frac{1}{(\alpha_2^{IND})^2} + \alpha\left(1 - \frac{1}{(\alpha_1^{IND})^2}\right)\frac{1-l_1}{(\alpha_2^{IND})^2}, \quad (16)$$

$$\frac{1}{\alpha} = \frac{l_1}{\alpha_1^{IND}} + \frac{1-l_1}{\alpha_1^{IND}\alpha_2^{IND}}. \quad (17)$$

Inspection of these equations shows that the conditions:

(i) $\alpha_1^{IND} = \alpha_2^{IND} = 1$ if $\alpha = 1$ (for $\forall l_1 \in [0,1]$),

(ii) $\alpha_2^{IND} = 1$ if $l_1 = 1$ (for $\forall \alpha \geq 1$) and

(iii) $\alpha_1^{IND} = \alpha_2^{IND} = \sqrt{\alpha}$ if $l_1 = 0$ (for $\forall \alpha \geq 1$)

are satisfied, justifying the appropriateness of the chosen objective function. Solving the system given by Eq.(16) and Eq.(17) by first eliminating variable α_1^{IND} leads to a fourth-order polynomial in α_2^{IND}. Further inspection reveals that finding the roots of this polynomial can be simplified, as they involve higher-degree factors of form $l_1(1-l_1)$. As $l_1 \in [0,1]$, these factors quickly tend to zero and can therefore be neglected. This insight leads to the approximants:

$$\alpha_1^{IND} = \alpha\left(l_1 + \frac{1-l_1}{\alpha_2^{IND}}\right), \quad (18)$$

$$\alpha_2^{IND} = 1 + (\sqrt{\alpha} - 1)\sqrt{1-l_1}.$$

This completes the proof.

5. Conclusions

The goal of this paper is to establish a quantitative methodology for calculating the necessary risk reduction factors of two safety functions implemented in a two-layer SIS that utilizes a single logic solver. The safety functions are designed to jointly address a single hazard category. The targets are associated with protection against a single scenario, resulting in consequences of varying severities. The proposed method aims to:

- enhance the LOPA risk analysis tool by enabling more accurate determination of PFD targets, and
- address a serious limitation of LOPA, by considering shared components without jeopardising overall safety.

The minimal RRFs for the safety functions serve as a foundation for functional safety, upon which the safety margin can be built. The extent to which the safety functions share components in this two-layer SIS is constrained by the SIL of the shared component, which defines an upper bound on its SIL capability. Additionally, the loss mitigated by the first protection layer plays a critical role in determining the maximum overall risk reduction achievable for the individual safety functions. The amount of loss addressed by the first layer establishes an upper limit on the maximal RRF that can be allocated to each layer's safety function – as observed in Case D.

Since the determination of PFD/RRF targets is, in general, an underdetermined problem, optimization is employed in this paper to obtain a closed set of equations that enable their calculation while adhering to a cost functional. The functional is designed to minimize the sum of RRF targets without compromising the overall safety target. This additional requirement aligns with the objective of producing a minimal safety requirement specification.

The method described in this paper (see Fig. 8.) applies specifically to two protection layers that share a logic solver. A more general challenge involves evaluating minimal RRFs for safety

functions that protect against multiple hazard categories. Determining a cost-effective design solution for such systems could potentially be addressed through extensions of the method presented in this paper.

References

Alijagic, E. (2015) *Optimization of SIL allocation for Safety Functions Implemented over Layers of Protection,* Proceedings of ESREL2015, Zürich.

ANSI/ISAS84.01 (1996). *Application of Safety Instrumented Systems for the process control industry,* Instrumentation Society of America (ISA), Durham US.

CCPS (2007). *Guidelines for Safe and Reliable Instrumented Protective Systems*, Center for Chemical Process Studies, AIChE Technological Community.

CCPS (2014). *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis,* Center for Chemical Process Studies, AIChE Technological Community.

CCPS (2001). *Layer of Protection Analysis: Simplified Process Risk Assessment*, Center for Chemical Process Studies, AIChE Technological Community.

Cornelliusen K. (2002). *Approaches to the determination of safety integrity levels (SIL) for Safety Instrumented Systems (SIS) - comparison and discussion*. NTNU, Trondheim.

De Salis, C. (2001). *Using Risk Graphs for Safety Integrity Level (SIL) assessment - a user-guide for chemical engineers.* The Institution of Chemical Engineers, UK.

Dowell III, A.M. (1998). *Layer of Protection Analysis for Determining Safety Integrity Level,* ISA Transactions, 37(3): 155-165.

Gruhn P., Cheddie H. L. (2006). *Safety Instrumented Systems: Design, Analysis, and Justification, Ed. 2, The Instrumentation, Systems and Society (ISA)*. Research Triangle Park, NC.

Gulland, W. G. (2004). *Methods of Determining Safety Integrity Level (SIL) Requirements – Pros and Cons. Practical Elements of Safety.* Proceedings of the 12th Safety-Critical Systems Symposium, Birmingham, UK, February 2004. Redmill F. and Anderson T. (eds.), pp 105-122. Springer-Verlag, London, UK.

IEC61508 (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES), 2nd Ed.,* International Electrotechnical Commission IEC, Geneva.

IEC61511 (2003). *Functional safety – Safety instrumented systems for the process industry sector*, International Electrotechnical Commission IEC, Geneva.

IEC61511-4 (2020). *Functional safety – Safety instrumented systems for the process industry sector – Part 4: Explanation and rationale for changes in IEC 61511-1 from Edition 1 to Edition 2*, International Electrotechnical Commission IEC, Geneva.

Marszal, E. & Scharpf, E. (2002). *Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis. Instrumentation, Systems and Society (ISA).* Research Triangle Park, NC.

NORSOK (2020). *S-001 - Technical Safety Standard, Ed. 7,* online available via https://online.standard.no/nb/norsok-s-001-2020ac-2021

Summers, A. (1998). *Techniques for Assigning a Target Safety Integrity Level*. ISA Transactions, 1998. 37(2):95-104.