Risk-Based Optimization and Performance Level Verification of Safety-Related Control Systems for Automated Size Sorting Machinery According to ISO 13849-1

Phonnipha Boriboonsuksri[1] and Natth Jun-krob[2*]

[1]Department of Safety Engineering, Southeast Asia University,19/1 Petchkasem Rd. Bkk.10160
[2]Department of Computer Engineering, University, 19/1 Petchkasem Rd. Bkk.10160
*Corresponding author: natthj@sau.ac.th

Abstract The increasing integration of human– machine interaction in industrial automation necessitates robust functional safety design methodologies. This study proposes a structured risk-based engineering framework for the design and verification of Safety-Related Parts of Control Systems (SRP/CS) in accordance with ISO 12100 and ISO 13849-1. The methodology establishes explicit traceability from hazard identification to Performance Level (PL) verification while incorporating architectural optimization, reliability modeling, and diagnostic coverage quantification. A case study involving an automated conveyor system equipped with pneumatic sorting actuators was analyzed. Risk assessment identified two critical safety functions requiring a Required Performance Level (PL_r) of c. Although Category 3 architecture satisfies PL_r, a Category 4 dual-channel redundant architecture with high diagnostic coverage was selected to enhance lifecycle robustness and international compliance readiness. Quantitative reliability modeling incorporating $MTTF_d$ aggregation, Diagnostic Coverage (DC_{avg}) estimation, and Common Cause Failure (CCF) scoring yielded PLe for both safety functions. Sensitivity analysis demonstrated architectural resilience under conservative parameter variation. The results confirm that risk-driven architectural optimization enhances functional safety robustness while ensuring regulatory compliance and long-term operational reliability.

Keywords: Functional Safety; ISO 13849-1; Risk Assessment; Performance Level; Reliability Engineering; Machine Safety; Diagnostic Coverage; Common Cause Failure

1. Introduction

Industrial automation systems increasingly operate in environments where human operators perform feeding, inspection, and troubleshooting tasks in proximity to moving machinery. Conveyor systems with pneumatic sorting mechanisms present significant hazards including[1]-[3]:

-Entanglement and crushing
-Unexpected startup
-Actuator-induced impact injuries
-Hazardous zone access during operation

ISO 12100 establishes a structured risk assessment framework[4], while ISO 13849-1 provides performance evaluation criteria for safety-related control systems[5], [6]. Despite widespread industrial use, many implementations lack:

(i) Quantitative reliability modeling
(ii) Architectural optimization justification
(iii) Sensitivity validation
(iv) Explicit hazard-to-safety-function traceability

This study addresses these gaps by proposing an integrated engineering methodology.

2. Materials and Methods

2.1 Theoretical Background

2.1.1 Risk Assessment (ISO 12100)

Risk is determined by [7]:

$$R = f(S, F, P)$$

Where:

S = Severity
F = Frequency/Exposure
P = Possibility of avoidance

The Risk Graph methodology determines Required Performance Level (PLr) [8]

2.1.2 Performance Level Determination (ISO 13849-1) [5]

Performance Level Requirement and Achieved Performance Level

In safety-related parts of control systems (SRP/CS), two categories of performance level are defined. The first is the required performance level (PLr), which represents the

level of safety performance necessary to adequately reduce risk according to the identified hazard severity and exposure conditions. The second is the achieved performance level (PL), which is determined through the technical evaluation and validation of the implemented SRP/CS design.

Both PLr and PL are classified on a five-level scale ranging from "a" (lowest reliability) to "e" (highest reliability) as show in Fig.1.

PLr (Required Performance Level): The safety performance level that must be achieved by the SRP/CS to ensure sufficient risk reduction.

PL (Achieved Performance Level): The performance level obtained after evaluating the reliability and effectiveness of the implemented safety control system.

For compliance with functional safety requirements, the achieved performance level (PL) must be equal to or higher than the required performance level (PLr). This ensures that the implemented safety function provides an adequate level of protection relative to the assessed risk.

The performance level of the machine under assessment depends on the parameters of each device component, which includes::

- Category (B, 1, 2, 3, 4)
- MTTFd
- DCavg
- CCF

Performance Level (PL)	Probability of Dangerous Failure per Hour (PFHd) 1/h
a	$\geq 10^{-5}$ and $<10^{-4}$ ⟨0.001% to 0.01%⟩
b	$\geq 3 \times 10^{-6}$ and $<10^{-5}$ ⟨0.0003% to 0.001%⟩
c	$\geq 10^{-6}$ and $<3 \times 10^{-6}$ ⟨0.0001% to 0.0003%⟩
d	$\geq 10^{-7}$ and $<10^{-6}$ ⟨0.00001% to 0.0001%⟩
e	$\geq 10^{-8}$ and $<10^{-7}$ ⟨0.000001% to 0.00001%⟩

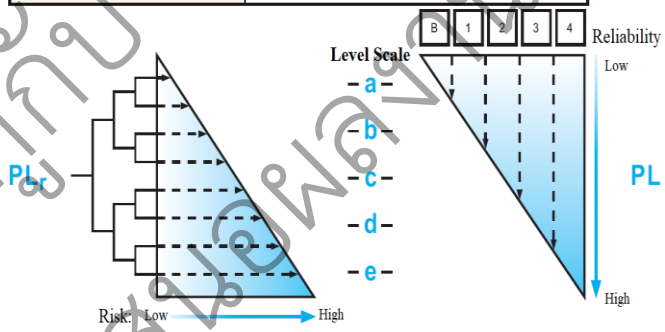

Fig.1 Scaling of Requirement Performance and Achieved Performance level

2. 2 Determining PLr using risk graph method

The required performance level (PLr) for SRP/CS is determined through a systematic risk assessment process. The PLr obtained from this assessment represents the target safety performance that the SRP/CS must achieve during system design to ensure adequate risk reduction.

PL_r is typically established using the risk graph method, which considers three key parameters: the severity of possible injury (S), the frequency and/or duration of exposure to the hazard (F), and the possibility of avoiding or limiting harm (P). Based on the combination of these factors, the resulting risk level is categorized into one of five performance levels, ranging from "a" (lowest safety performance requirement) to "e" (highest safety performance requirement) as show in Fig.2.

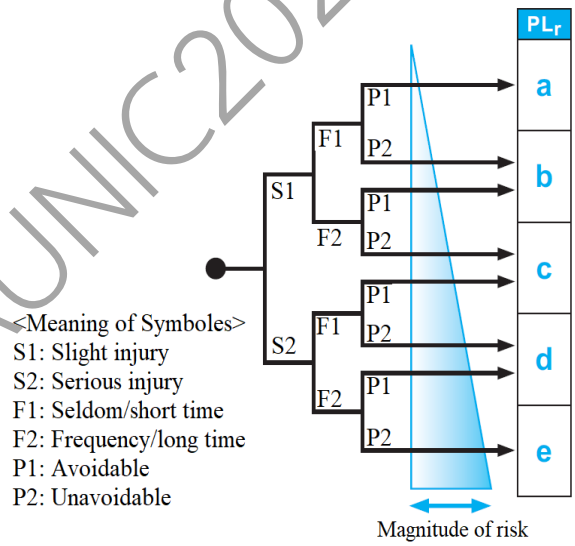

Fig.2 Graph method evaluated risk

2.3. METHODOLOGY

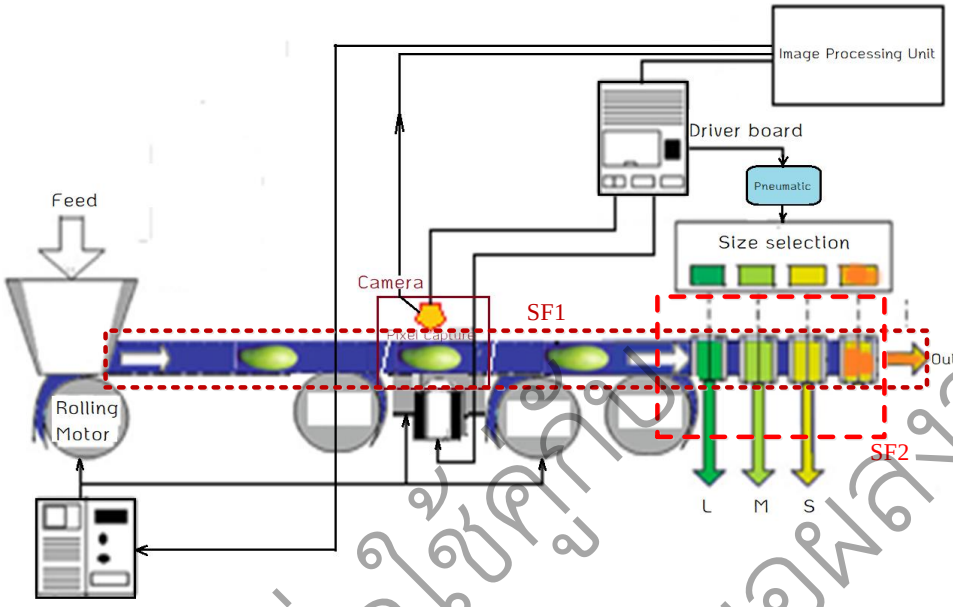

Fig. 3 Schematic Layout of the Automated Size Sorting Machinery, illustrating the integration points for Emergency Stop devices and Movable Safety Guards

RESEARCH FRAMEWORK

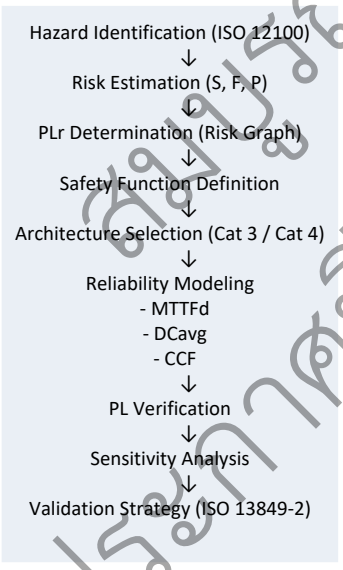

Fig.4 The research work flow

The Fig.4 show the engineering workflow of research methodology, which consequence consists of:

(i) Hazard identification
(ii) Risk parameter evaluation
(iii) PLr determination
(iv) Safety function definition
(v) Architectural selection
(vi) Reliability modeling
(vii) Sensitivity analysis
(viii) Validation roadmap development

A brief description of the experimental procedure and analysis and sufficient information for others to be able to reproduce the experiments. [9] –[12]

2. 4 CASE STUDY: AUTOMATED SIZE SORTING SYSTEM CONVEYOR

The operation mechanism of system is shown in Fig.3, which consists of:

(i) Conveyor drive (inverter controlled)
(ii) Pneumatic cylinder sorter
(iii) Movable safety guards
(iv) Operator interaction zones

In Hazard identification and Risk parameter evaluation process found the hazard exposure risk on the operation of conveyor zone and cylinder motion when guard open at size sorting zone of this automatic machine.

For safety operations of this machinery, two Safety Functions (SF) were identified:

-SF1: Emergency stop of conveyor
-SF2: Prevention of cylinder motion when guard open

Channel 1:
EMG → Safety PLC → Contactor/Inverter → Conveyor

Channel 2:
EMG → Safety PLC → Contactor/Inverter → Conveyor

Cross Monitoring:
- Channel 1 ↔ Channel 2
- Feedback loop from inverter

Fig.5 Two Safety Functions were identified

EMG1 ┐
├ PLC CH1 — INV1 — Motor
EMG2 ┘

EMG3 ┐
├ PLC CH2 — INV2 — Motor
EMG4 ┘

Feedback loop → PLC monitoring

Guard Switch 1 ┐
├ PLC CH1 — Safety Valve 1 — Cylinder
Guard Switch 2 ┘

Guard Switch 3 ┐
├ PLC CH2 — Safety Valve 2 — Cylinder
Guard Switch 4 ┘

Feedback: Valve position monitoring

Fig. 6 state diagram of Safety Function: SF1 and SF2

3. RESULTS AND DISCUSSION

3.1 Risk Assessment and PLr Determination

The risk results of SF1 and SF2 by using the graph method evaluated are show the PL_r = “c” for both functions as Table1.

Table1 risk results of SF1 and SF2

Safety Function	S	F	P	PL_r
SF1	S2	F2	P1	“c”
SF2	S2	F2	P1	“c”

3.2 Architectural Optimization

Although Category 3 satisfies PL_r, Category 4 was selected based on:

3.2.1 Fault Tolerance

Category 4 tolerates single faults without loss of safety function.

3.2.2 Accumulated Fault Resistance

Continuous diagnostics detect fault accumulation.

3.2.3 Lifecycle Reliability Enhancement

Reduces latent failure probability.

3.2.4 Regulatory Strategy

Facilitates CE marking and international export compliance.

While the risk assessment indicated a Required Performance Level (PLr) of 'c' for both SF1 and SF2, this study intentionally adopts a Category 4 architecture (achieved PLe) . This 'safety over- design' strategy is justified by several factors:

Enhanced Fault Tolerance: Category 4 ensures that a single fault does not lead to the loss of the safety function and that accumulated faults are detected.

Market Readiness: Achieving PL e facilitates compliance with stringent international standards, such as those required for CE marking, providing a competitive advantage for global export.

Lifecycle Robustness: The higher diagnostic coverage ($DC_{avg} \geq 99\%$) significantly reduces the probability of latent failures over the machine's operational lifespan.

3.3 Reliability Modeling

3.3.1 MTTFd Calculation

For components with $B10_d$:

$$MTTFd = \frac{B10_d}{0.1 \times n_{op}}$$

Where as:

$B10_d$: Specifies the number of cycles at which 10% of the components have failed dangerously for pneumatic and electromechanical components.

n_{op} : Annual operation cycles

All subsystems achieved:

$MTTFd \geq 30$ years (High)

To ensure the accuracy of $MTTF_d$ calculations, reliability data was sourced directly from component manufacturers' $B10_d$ values. For the electromechanical contactors and pneumatic valves used in the case study, $MTTF_d$ was aggregated based on an estimated annual operation cycle (n_{op}) , resulting in a 'High' rating for all subsystems, exceeding the 30-year threshold defined by the standard.

3.3.2 Channel Aggregation

For series elements:

$$\frac{1}{MTTF_{d,Total}} = \sum \frac{1}{MTTF_{d,i}}$$

For redundant structures, ISO 13849-1 Annex K methodology was applied.

3.3.3 Diagnostic Coverage (DC_{Avg})

Diagnostic mechanisms F(implemented:

-Dual-channel redundancy
-Cross monitoring
-Test pulse detection
-Feedback loop monitoring
-Certified safety PLC

Conservative estimate:

$$DC_{avg} \geq 99\%$$

Table2 Effect of MTTFd and DCavg to PL

	DC High	DC Medium	DC Low
MTTFd High	e	d	c
MTTFd Medium	d	c	b
MTTFd Low	c	b	a

3.3.4 Common Cause Failure (CCF)

Common Cause Failure (CCF) describes the simultaneous malfunction of multiple components or systems triggered by a shared underlying cause or event, as opposed to failures occurring independently through random mechanisms. The CCF evaluation results per Annex F:

Table3 the Common Cause Failure (CCF) evaluation score

Measure	Score
Separation of power	15
Diversity	10
Environmental protection	10
EMI mitigation	25
Cable segregation	15
FMEA analysis	5

Total = 80 (> 65 threshold)

The Common Cause Failure (CCF) evaluation yielded a total score of 80, which exceeds the ISO 13849-1 minimum threshold of 65. This high score is attributed to specific engineering controls:

- *EMI Mitigation* (25 points): Implementation of shielded cabling and robust grounding techniques to prevent simultaneous failures from electrical interference.
- *Physical Separation* (15 points): Distinct routing for power and control signal cables to minimize the risk of localized physical damage affecting both channels.
- *Diversity* (10 points): Utilization of different technologies or physical principles within the dual- channel structure to prevent systematic failures

3.4 Performance Level Results

Safety Function	PLr	Achieved PL
SF1	“c”	“e”
SF2	“c”	“e”

Thus: PL ≥ PLr , As can be seen, the Achieved Performance Level obtained from the design is higher than the Required Performance Level that was set.

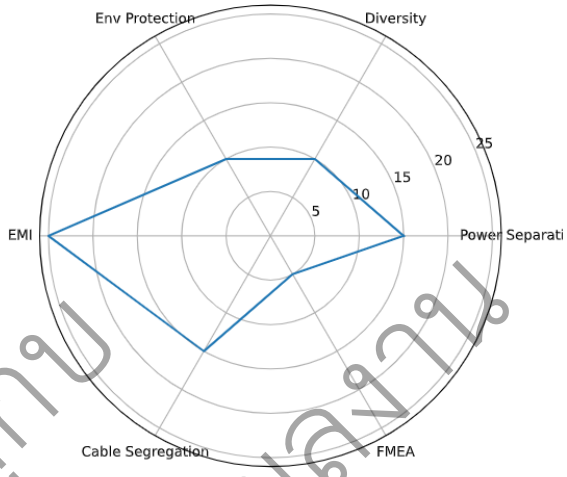

Fig. 6 Quantitative Radar Chart showing the distribution of CCF Evaluation scores across the six mandatory safety measures

3.5 Sensitivity Analysis

Parameter variation scenarios:

Scenario	DC_{avg}	$MTTF_d$	PL
Baseline	99%	High	“e”
Reduced DC	90%	High	“d”
Reduced $MTTF_d$	Medium	99%	“d”
Both reduced	90%	Medium	“c”

The architecture remains compliant even under conservative degradation.

3.6 Discussion

Key findings:

(i) Architectural overdesign improves lifecycle robustness.

(ii) Category 4 significantly reduces undetected fault probability.

(iii) Sensitivity modeling confirms resilience. Risk- based traceability improves engineering transparency.

(iv) The framework supports digital safety design workflows.

Comparative Analysis: ISO 13849-1 vs. IEC 62061

Comparison with IEC 62061[13] indicates ISO 13849 is advantageous for electromechanical systems with complex redundancy structures.

Although both standards are harmonized under the Machinery Directive to ensure functional safety, they differ significantly in their

mathematical approaches, technological focus, and architectural modeling.

(i) Practical Selection Criteria

The choice between these two standards typically depends on the **technology used** and the **complexity of the system**:

- ***Technology-Driven Selection*:** ISO 13849-1 is a "technology-neutral" standard, making it the preferred choice for systems integrating **pneumatic, hydraulic, and mechanical components** alongside electronics. In contrast, **IEC 62061** is specifically tailored for **Electrical, Electronic, and Programmable Electronic (E/E/PE)** safety systems.
- ***System Complexity*:** For machine builders using "off-the-shelf" safety components (like the safety PLCs and contactors used in this case study), ISO 13849-1's **Category-based approach** (B,1,2, 3, 4) provides a more intuitive workflow for verifying Performance Levels (PL). IEC 62061 is often preferred for large-scale integrated systems with complex logic solvers.

(ii) Advantages and Limitations

Feature	ISO 13849-1	IEC 62061
Risk Metric	**Performance Level (PL a–e)**	Safety Integrity Level (SIL 1–3)
Architecture	**Pre-defined Categories (B, 1-4)** provide a rigid but clear structural framework.	Flexible architectural modeling based on Subsystem Limit Values.
Reliability Logic	Uses *MTTFd* (Mean Time to Dangerous Failure) and *B10d* for mechanical parts.	Uses *PFHd* (Probability of dangerous Failure per Hour).
Advantages	Better for **electromechanical and pneumatic systems**; easier for non-electronic engineers to apply.	Better for **complex software-driven safety functions** and large-scale plant automation.
Limitations	The simplified "Category" structures can sometimes be restrictive for highly customized electronics.	Mathematical complexity is higher; requires detailed data for every electronic sub-component.

(iii) Machine-Type Applicability

- ***Discrete Automated Machinery (e.g., the Size Sorter in this study):*** These machines often rely on **pneumatic actuators and electromechanical contactors**. ISO 13849-1 is superior here because it offers clear formulas for converting mechanical cycles (*B10d*) into reliability data.
- ***Process-Integrated Machinery*:** For machines heavily reliant on complex data communication and variable speed drives (VSD) across a wide network, IEC 62061 offers a more robust framework for calculating the safety integrity of the entire data loop.

Validation Roadmap (ISO 13849-2)

Future validation plan:
- Fault injection testing
- Proof test interval definition
- Periodic functional testing
-SISTEMA computational verification
- Field reliability monitoring

4. Conclusion

This study has successfully established a structured, risk-based engineering framework for the design and verification of Safety-Related Parts of Control Systems (SRP/CS) in automated machinery. By integrating ISO 12100 risk assessment with ISO 13849-1 reliability modeling, the methodology provides a transparent and replicable path from hazard identification to final technical validation. For the automated size sorting case study, although the risk assessment identified a Required Performance Level (PLr) of 'c', this research demonstrated that adopting a Category 4 dual-channel architecture—achieving an Achieved Performance Level of 'e'—significantly enhances the system's fault tolerance and lifecycle robustness. This architectural optimization provides a strategic advantage for manufacturers seeking international regulatory compliance, such as CE marking, and ensures that the machinery remains resilient against undetected fault accumulation. Furthermore, sensitivity analysis confirmed that the proposed safety functions maintain high reliability even under conservative parameter variations. While this study highlights ISO 13849-1 as an advantageous standard for machines utilizing complex electromechanical and pneumatic redundancy, the framework is also compatible with modern digital safety design workflows.

In summary, the transition from qualitative risk estimation to quantitative reliability verification is essential for ensuring long- term operational safety. Future research will expand upon this framework by incorporating field reliability monitoring and advanced computational validation using tools like SISTEMA to further bridge the gap between theoretical design and real- world functional performance.

5. ACKNOWLEDGEMENT

Thank you to the Safety Engineering students from the Faculty of Engineering, Southeast Asia University, for assisting in collecting data for this research analysis.

References

[1] Birolini, A. (2017). Reliability engineering: Theory and practice. Springer.

[2] Catelani, M., Ciani, L., & Patrizi, G. (2022). Logic solver diagnostics in safety instrumented systems for oil and gas applications. Safety, 8(1), 15. https://doi.org/10.3390/safety8010015

[3] Ebeling, C. E. (2019). An introduction to reliability and maintainability engineering. Waveland Press.

[4] ISO 12100:2010. (2010). Safety of machinery — General principles for design. International Organization for Standardization.

[5] ISO 13849-1:2015. (2015). Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design. International Organization for Standardization.

[6] ISO 13849-2:2012. (2012). Safety of machinery — Safety-related parts of control systems — Part 2: Validation. International Organization for Standardization.

[7] Henley, E. J., & Kumamoto, H. (1992). Probabilistic risk assessment and management for engineers and scientists. IEEE Press.

[8] Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. CRC Press.

[9] Li, Z., Xu, T., Gu, J., Wang, H., & Zhao, J. (2019). Reliability modeling of redundant systems considering common-cause failures based on dynamic Bayesian network. Arabian Journal for Science and Engineering, 44(11), 2567–2577. https://doi.org/10.1007/s13369-018-3307-y

[10] Pedroni, N., & Zio, E. (2010). Reliability estimation by advanced Monte Carlo simulation. In J. Faulin et al. (Eds.), Simulation methods for reliability and availability of complex systems (pp. 3–39). Springer. https://doi.org/10.1007/978-1-84882-213-9_1

[11] Gao, K., Peng, R., Qu, L., & Wu, S. (2020). Evaluation of availability and reliability of standby repairable systems incorporating imperfect switchovers and breakdowns. Reliability Engineering & System Safety, 202, 107366. https://doi.org/10.1016/j.ress.2020.107366

[12] Rausand, M. (2014). Reliability of safety-critical systems. Wiley.

[13] IEC 62061:2021. (2021). Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems. International Electrotechnical Commission.

Authors' Biography:

Phonnipha Boriboonsuksri PhD. (Occupational Health and Safety), Thammasat University.
Research focused on ergonomics, industrial hygiene, risk assessment, and industry..safety management.

Natth Jun-krob
Master of Engineering (Electrical Engineering), KMITL. Interested in research in industrial and communication electronics, power engineering, safety engineering, and environmental engineering.