SAUNIC 2026
The 13th SAU National Interdisciplinary Conference 2026
"HUMANITY IN THE LOOP AI GOVERNANCE AND ETHICAL FUTURES"
"มนุษยชาติในวงจร AI : การกำกับดูแลและอนาคตด้านจริยธรรม"
วันศุกร์ที่ 19 มิถุนายน 2569 โรงแรมแกรนด์ริชมอนด์ สไตล์ช คอนเวนชั่น โฮเทล
ร่วมกับ
No. 50

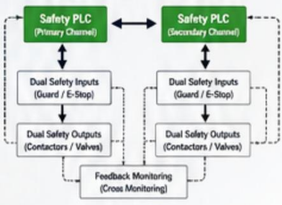
Risk-Based Optimization and Performance Level Verification of Safety-Related Control Systems for Automated Size Sorting Machinery According to ISO 13849-1

Phonnipha Boriboonsuksri | Natth Jun-krob
Department of Safety Engineering, Southeast Asia University

Human-Machine Interaction · Functional Safety · Risk-Based Design · ISO 13849-1 Compliance

1 RESEARCH OVERVIEW

DUAL-CHANNEL SAFETY ARCHITECTURE



2 INDUSTRIAL SAFETY PROBLEM

	Entanglement Hazard	Crushing Hazard	Unexpected Startup	Pneumatic Cylinder Impact	Guard Open During Operation
Hazard					
Injury	Severe Laceration Amputation	Fracture Severe Injury	Sudden Motion Impact Injury	Impact / Struck By Serious Injury	Exposed Zone High Risk
Safety Requirement	Prevent access to moving parts	Prevent crushing between objects	Prevent unexpected energization	Prevent uncontrolled cylinder motion	Prevent operation with guard open
Risk Severity	HIGH	HIGH	HIGH	MEDIUM	HIGH

3 RESEARCH OBJECTIVE

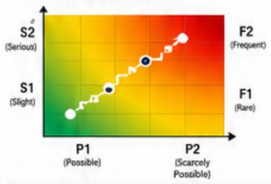
4 ISO 12100 RISK ASSESSMENT FRAMEWORK

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

S = Severity of Injury
F = Frequency / Exposure
P = Possibility of Avoidance

- S1 Slight
- S2 Serious (Severe Injury / Death)
- F1 Rare to Occasional
- F2 Frequent to Continuous
- P1 Possible under specific conditions
- P2 Scarcely Possible

ISO 12100 RISK GRAPH



REQUIRED PERFORMANCE LEVEL (PLr)

Risk Level	Low (Green)	Moderate (Yellow)	High (Orange)	Very High (Red)
PLr	a	b	c	d / e

5 MACHINE SAFETY CASE STUDY

AUTOMATED SIZE SORTING CONVEYOR SYSTEM

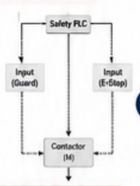
SF1 Emergency Stop of Conveyor — Stops conveyor safely upon emergency.

SF2 Prevent Cylinder Motion when Guard Open — Prevents cylinder actuation when guard is open.

7 ARCHITECTURAL OPTIMIZATION

CATEGORY 3 ARCHITECTURE

- Single Fault Vulnerability
- Limited Diagnostics
- Lower Fault Tolerance
- PLd Capability

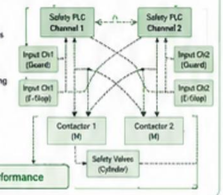


Moderate Safety Performance

VS

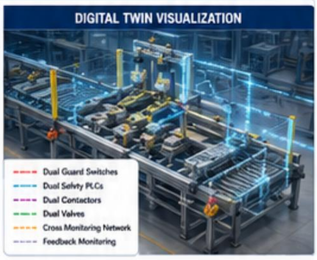
CATEGORY 4 ARCHITECTURE (SELECTED)

- Dual-Channel Redundancy
- Cross-Monitoring
- Feedback Diagnostics
- Fault Tolerant
- Continuous Monitoring
- PLe Capability



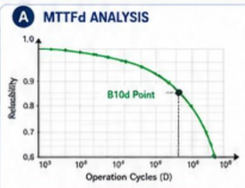
High Safety Performance

DIGITAL TWIN VISUALIZATION



8 RELIABILITY ENGINEERING ANALYSIS

A MTTFd ANALYSIS



MTTFd > 30 YEARS
High Reliability Achieved

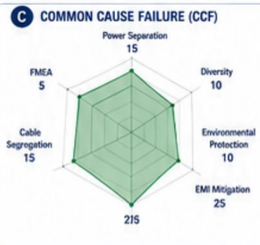
B DIAGNOSTIC COVERAGE

DCavg ≥ 99%

Dual Channel Redundancy	OK
Cross Monitoring	OK
Test Pulse Detection	OK
Safety PLC Diagnostics	OK
Feedback Monitoring	OK

High Diagnostic Coverage Achieved

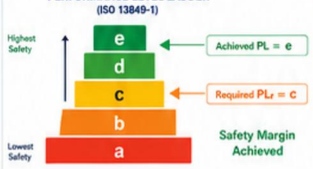
C COMMON CAUSE FAILURE (CCF)



TOTAL SCORE 80 / 100
THRESHOLD ≥ 65
PASS ✓
CCF Risk Acceptable

9 PERFORMANCE LEVEL RESULTS

PERFORMANCE LEVEL LADDER (ISO 13849-1)



11 ISO 13849-1 vs IEC 62061

	ISO 13849-1	IEC 62061
Safety Metric	Performance Level (PL)	Safety Integrity Level (SIL)
Architecture	Category-Based	SIL (1, 2, 3, 4)
Reliability Metric	MTTFd, B10d	PFHd
Suitable Systems	Electromechanical, Pneumatic, Simple E/E	Complex E/E/PE, Software-Based
Application	General Machinery, Small-Medium Systems	Large Automation Systems, Process Industry
Implementation	Easier, Cost-Effective	Complex, Higher Cost

12 KEY FINDINGS

1. Risk-based design improves safety transparency and decision-making.
2. Category 4 architecture significantly improves fault tolerance.
3. High diagnostic coverage enhances system reliability and fault detection.
4. Achieved PLe exceeds required PLr with sufficient safety margin.

10 SENSITIVITY ANALYSIS

SCENARIO	DCavg	MTTFd	ACHIEVED PL	RESILIENCE
Baseline (Optimal)	99%	High (>30 yrs)	e	■■■■■■
Reduced DC	90%	High	d	■■■■□□
Reduced MTTFd	99%	Medium (10–20 yrs)	d	■■■□□□
Both Reduced	90%	Medium	c	■■□□□□

✓ System remains COMPLIANT in all realistic scenarios

11 ISO 13849-1 vs IEC 62061

Safety Metric	Safety Integrity Level (SIL)
Architecture	SIL (1, 2, 3, 4)
Reliability Metric	PFHd
Suitable Systems	Complex E/E/PE, Software-Based
Application	Large Automation Systems, Process Industry
Implementation	Complex, Higher Cost

12 KEY FINDINGS

1. Risk-based design improves safety transparency and decision-making.
2. Category 4 architecture significantly improves fault tolerance.
3. High diagnostic coverage enhances system reliability and fault detection.

13 CONCLUSION

RISK ASSESSMENT → PLr DETERMINATION → CATEGORY 4 OPTIMIZATION → RELIABILITY MODELING → PLe VERIFICATION → SAFE MACHINERY

PLr = c | Achieved PL = e | CCF Score = 80 | DCavg ≥ 99% | MTTFd > 30 YEARS | SAFETY FUNCTIONS FULLY COMPLIANT

ISO 13849-1 CERTIFIED DESIGN FRAMEWORK FOR SAFE MACHINERY

SISTEMA Analysis · Fault Injection Testing · Field Reliability Monitoring