Integrated Safety for a Single BMS

White Paper

exida

80 N. Main St.

Sellersville, PA

www.exida.com

August 2020

exida White Paper Library
http://www.exida.com/Resources/Whitepapers

Abstract

There has been an on-going debate in control engineering groups about mixing control and safety in one PLC/DCS controller. But as the field of Functional Safety has matured, a strong majority of functional safety experts agree that mixing control algorithms and safety functions in one microprocessor board is bad practice. Yet perhaps there are situations where the capital cost of a simple system may be lower with both control and safety in one board. However, the operational cost is likely to be considerably higher. Safety is likely to be compromised. Cybersecurity may be weakened. And performance may be degraded. These tradeoffs must be carefully considered. Without careful analysis of the tradeoffs, especially safety, the default choice should be to never mix control and safety in one PLC/DCS controller.

Simple Rules

There are several simple rules suggested for use in safety instrumented system (SIS) design. These simple rules were created to avoid detailed analysis done by experts so that design work is reduced, and the chance of an error is minimized. **One of these rules is that no common equipment should be used for control of a process variable and automatic safety protection of that process parameter**. This rule was created because:

A. There are situations where the failure of control system causes a potential hazard. An SIS must provide protection against this hazard. However, if the piece of equipment that failed in the control system is also needed for protection in the SIS then protection is lost.

B. For those using Layer of Protection Analysis (LOPA) [T1] to establish the needed SIL level, protection credit is often given for alarm functions or shutdown functions implemented in the control system. LOPA credit requires separate equipment where failures do not disable independent layers of protection.

C. For programmable controllers, the management of change rules are often quite different for control systems versus safety systems. Control functions are not as critical, and many sites allow not only control parameter changes but control strategy changes without much formal administrative control and approval. Safety requires far more administrative control with justification and approval required before any changes are made. One easy way to help enforce this is to never have control and safety together within one programmable controller.

There are those in the safety expert community who insist that no common equipment by used for both control and safety. In many companies this rule is part of the “ten commandments” of safety design which must never be violated under any circumstances.

However, there are situations when the design resulting from these simple rules can be costly in terms of capital expense. And safety experts designing systems for operational sites with strong operations/maintenance ability and a strong safety culture may achieve good safety with a combination design but usually at the cost operational expense.

Tradeoffs

When a careful analysis is done and there are required safety functions where a control system failure is NOT an initiating event and no risk reduction credit was given to the control system (alarms or shutdown function) then our functional safety standards do allow combination systems. In such situations the control functions could be put into a safety certified controller. But tradeoffs must be considered.

Capital versus Operational Expense

When there is an attempt to combine control and safety in a SIL 3 certified controller, there are cost tradeoffs. Item C from the above list describes differences in how the administration and control of changes in control and safety are normally done. In a combination system, tight administrative controls justified for safety must be imposed on all control system changes but this will add significant operational expense. Over the lifetime of a system, those costs will likely be much higher than a separated design.

Safety

Safety systems designed per the IEC 61508 family of standards (IEC 61511 for the process industries) use a systematic method to define needed risk reduction and design systems to achieve the needed risk reduction in operation [T2, T3]. Good design tools like exSILentia [T4] use a site-specific measure called the Site Safety Index (SSI) [T5, T6] to help designers create designs that match operational/maintenance capability of a site. Field failure/incident reports show that only sites with effective and rigorous change control can maintain safety in systems where the simple design rules are not followed. This usually means that a site has an SSI 3 rating or higher. If a site has an SSI rating of 2 or lower, combined systems will likely increase risk.

NOTE: An on-line questionnaire for calculating the SSI of a particular site is available at http://www.exida.com/SSI

Cybersecurity

An attack path used in some automation system cyber-attacks requires that the safety PLC be disabled then the controller is set to cause as much damage as possible. Such an attack can be much easier if the control and the safety protection are done in the same controller module.

Performance

The safety PLC must have scan times low enough to perform two cycles within the Process Safety Time. The PID control must have scan times sufficient to maintain precise control. Depending on the system and the configuration loading it may be hard to achieve the required scan times.

Summary

The combination of control and safety into one controller is not prohibited by IEC 61511. But verifying that all design rules have been met is needed (See "Table 1: Combination Design Verification Checklist'). The specific rules that appear in IEC 61511:2016 [N1] must be met. It has become from field event studies that the IEC 61511 rules will likely be violated in any site with average or below average operational/maintenance capability (SSI = 2 or less).

A system designed with separation of control and safety in different purpose-built controllers has the advantage of lower life cycle cost, better safety, stronger cybersecurity, and perhaps even performance.

Table 1: Combination Design Verification Checklist

Requirement	Source
Processor and input/output (I/O) modules are approved or certified by an Accredited Certification Body according to IEC 61508, Systematic Capability of SC3. [T7]	IEC 61508, IEC 61511
No single failure of the common equipment can cause a process hazard and disable the safety function.	IEC 61511
No credit is taken for controller in LOPA.	IEC 61511
Programming and parameter changes in the control configuration meet all management of change requirements for safety functions. Lifecycle cost increase is justified.	IEC 61511
Architecture must consider cybersecurity risk and mitigation.	IEC 62443-2-4, IEC 62443-4-1

Reference Documents

Industry Standards

Item	Identification	Description
N1	IEC 61511: ed2, 2016	Functional Safety: Safety Instrumented Systems for the process industry sector, International Electrotechnical Commission, Geneva, Switzerland
N2	IEC 61508: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, Geneva, Switzerland

N3	IEC 62443-4-1: 2018	Industrial communication networks - Security for industrial and control systems - Part: 4-1: Product development requirements, International Electrotechnical Commission, Geneva, Switzerland
N4	IEC 62443-2-4: ed1, June 2015	Industrial communication networks - Security for industrial and control systems - Part: 2-4: Security program requirements for IACS service providers, International Electrotechnical Commission, Geneva, Switzerland

Technical References

Item	Identification	Description
T1	ISBN 978-1-93497716-3	Scharpf, E., Thomas, H.W., & Stauffer, T.R., Practical SIL Target Selection – Risk Analysis per the IEC 61511 Safety Lifecycle, exida, 2016
T2	ISBN 978-1-93497719-4	Gandy, S.N., Functional Safety for Managers : What Managers Need to Know, Chapter 1, exida, 2020.
T3	ISBN 978-1094554143-8	Van Beurden, I, & Goble, W.M., Safety Instrumented System Design – Techniques and Design Verification, Chapter 1, ISA, 2018
T4		exSILentia 4.0 UserGuide, exida, 2019
T5	White Paper, April 11, 2016	Assessing Safety Culture via the Site Safety Index™, J.V. Bukowski, D. Chastain-Knight, 12th Global Congress on Process Safety, AIChE, GCPS 2016, http://www.exida.com/articles/assessing-safety-culture-viathe-site-safety-index.pdf
T6	White Paper, April 11, 2016	Quantifying the Impacts of Human Factors on Functional Safety, J.V. Bukowski, L. Stewart, 12th Global Congress on Process Safety, AIChE, GCPS 2016, http://www.exida.com/articles/quantifying-the-impacts-of-human-factors-on-functional-safety.pdf
T7	White Paper, V1R2, November 10, 2017	The exida IEC 61508 - Functional Safety and IEC 62443- Cybersecurity Certification Programs, https://www.exida.com/Resources/Whitepapers/the_exida_61508_cybersecurity_certification_program_faq1

Terms and Definitions

BPCS	Basic Process Control System
DCS	Distributed Control System
HFT	Hardware Fault Tolerance
IEC	International Electrotechnical Commission
I/O	Input / Output
LOPA	Layer Of Protection Analysis

PID	Proportional – Integral - Derivative
PLC	Programmable Logic Controller
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SSI	Site Safety Index

Status of the Document

Liability

exida provides services and analyses based on methods advocated in international and national standards. exida accepts no liability whatsoever for the correct and safe functioning of a plant or installation developed based on this analysis or for the correctness of the standards on which the general methods are based.

Revision History

Author: William M. Goble, PhD

Version: 1 Revision: 1

Version History:	V1, R1: Released document, August 30, 2020
	V0, R1: First Internal Draft, August 29, 2020
Release Status:	Released

exida – Who we are.

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

Training

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

Knowledge Products

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool

- PHAx™ (Process Hazard Analysis)
- LOPAx™ (Layer of Protection Analysis)
- SILAlarm™ (Alarm Management and Rationalization)
- SILect™ (SIL Selection and Layer of Protection Analysis)
- Process SRS (PHA based Safety Requirements Specification definition)
- SILver™ (SIL verification)
- Design SRS (Conceptual Design based Safety Requirements Specification definition)
- Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
- PTG (Proof Test Generator)
- SILstat™ (Life Event Recording and Monitoring)

- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
  - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
  - CyberSL™ (Cyber Security Level Verification)

Tools and Products for Manufacturer Support

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC

80 N. Main Street

Sellersville, PA, 18960

USA

+1 215 453 1720

+1 215 257 1657 FAX

info@exida.com