Safety Accuracy is Dead; Long Live Safety Deviation!

White Paper

exida
80 N. Main St.
Sellersville, PA
www.exida.com

August 2015

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

Abstract

Safety deviation is a term used in functional safety. The term is defined, some of its history is described, the reasoning for its existence is given, and its application is presented.

Definition

Accuracy is defined as "degree of conformity of a measure to a true or standard value[1]." For the purposes of this paper, the definition can be further refined as "the degree of conformity of the output of a device to the physical variable the device is measuring."

Safety deviation (formerly safety accuracy) is the change in output due to (internal) component failures not analyzed in a Failure Modes, Effects, & Diagnostic Analysis (FMEDA). Safety accuracy is an input to the FMEDA analyst to advise the level of analysis detail for critical analog components. Therefore an engineer setting a trip point should set the trip point including safety accuracy less/greater.

Purpose

Why safety deviation? Why not just report the statistical accuracy of the device and leave it at that? There are several answers to this question.

Requirement of Safety Instrumented Function

In many cases the safety function requires an accuracy that is less than the "conventional" accuracy of the instrument. A pressure transmitter, for example, may be employed to sense overpressure in a vessel in which the normal pressure is 300 lbs/in^2 and the burst rating is 600 lbs/in^2 minimum. The threshold for the overpressure would typically be ~450 lbs/in^2. In this application the value reported by the transmitter could be several percent off without compromising safety.

Effect on Safety Metrics

If safety deviation was not considered and the tighter stated accuracy was to apply for functional safety, both dangerous and safe (spurious) failure rates would increase. Drift errors, for example, on components such as resistors and voltage references would be classified as safe or dangerous failures rather than having no effect on the safety function.

Tractability of Analysis

When performing an FMEDA, there are frequently secondary components whose failures can be ignored with a wider safety deviation.

HART

The circuitry connecting the HART modem to the current loop is typically isolated by capacitors. In most cases short circuit failures of these capacitors will not deviate the output beyond the safety deviation, but would deviate the output beyond the rated accuracy.

[1] http://en.wiktionary.org/wiki/accuracy

Temperature Compensation

In some gas sensors and many pressure sensors obtaining ultimate accuracy requires measuring and compensating for the sensor temperature. If the safety deviation is limited to the uncompensated value, the temperature sensing circuit can be considered to have no effect on the failure rate.

EMC

The functional safety of the device should be valid for all environments stated by the manufacturer. In some cases, exposure to electromagnetic stress may result in deviations beyond the rated accuracy.

Requirements on Diagnostics

The accuracy of a device will be checked via automatic diagnostics and/or proof testing. Greater accuracy of the device will require correspondingly greater accuracy of the checking system. Consider a device rated to 0.5% accuracy. If it is evaluated by a checking system with the same accuracy, there will be a considerable number of cases where a) an acceptable device will be flagged as unacceptable or b) a device which is beyond its rated accuracy is diagnosed as acceptable. Since the device accuracy itself may be pushing the state of the art, this may place unrealistic demands on the checking system.

In some cases, a relatively complex calculation may be required to derive the value of the process variable. If a simplified calculation is used as a diagnostic, the safety deviation is limited to that of the simplified calculation.

Drift in some types of gas sensors can be detected by going to a safe state when a negative gas concentration is detected. In some of these sensors the drift is endemic, requiring calibration with “bump gas” as often as once every 90 days. The safety deviation is limited to the negative drift that sends the transmitter to its safe state, usually -10%.

Use of Safety Deviation at the System Level

In a low demand application, the probability of the safety deviation being exceeded is the same or less than the PFD_{avg}. In a system context, this implies that safety deviations do not add in the same way as “normal” accuracies.

Consider a SIL 2 system in which the sensor, logic solver and final element each have a PFD_{avg} of 0.002. The sensor has a safety deviation of 2%, the logic solver a safety deviation of 3%. (We will assume the final element is discrete rather than analog). So about once every 500 demands either the sensor or the logic solver will exceed its safety accuracy. But note that the PFD_{avg} of the sensor is independent from that of the logic solver. (Since the sensor and logic solver are typically not co-located and use different technology we will ignore common cause factor). Therefore the logic solver and sensor will both exceed their safety deviation only about once every 500^2=250000 demands! The clear implication here is that the safety deviation at the system level is essentially identical to that of the component with the worst (highest number) safety accuracy.

References

[N1]	IEC 61508 (Parts 1 - 7): 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems

Terms and Definitions

Architectural Constraint	The SIL limit imposed by the combination of SFF and HFT for Route 1_H or by the HFT and Diagnostic Coverage (DC applies to Type B only) for Route 2_H
DCS	Distributed Control System
exida criteria	A conservative approach to arriving at failure rates suitable for use in hardware evaluations utilizing the 2_H Route in IEC 61508-2.
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (IEC 61508-4, 3.6.3)
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
FMEDA	Failure Mode Effect and Diagnostic Analysis
HFT	Hardware Fault Tolerance
Low demand mode	Mode, where the demand interval for operation made on a safety-related system is greater than twice the proof test interval..
PFD_{avg}	Average Probability of Failure on Demand
PVST	Partial Valve Stroke Test It is assumed that the Partial Stroke Testing, when performed, is automatically performed at least an order of magnitude more frequent than the proof test, therefore the test can be assumed an automatic diagnostic. Because of the automatic diagnostic assumption the Partial Valve Stroke Testing also has an impact on the Safe Failure Fraction.
Random Capability	The SIL limit imposed by the PFD_{avg} for each element.
SFF	Safe Failure Fraction summarizes the fraction of failures, which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
Systematic Capability	The SIL limit imposed by the capability of the products manufacturer.

Type A element	"Non-Complex" element (using discrete components); for details see 7.4.4.1.2 of IEC 61508-2
Type B element	"Complex" element (using complex components such as micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508-2

Revision History

Version:	V1	
Revision:	R1	
Version History:	V1, R1:	Released, 2015-08-10
	V0, R4:	Adopted term "safety deviation," 2015-08-10
	V0, R3:	corrected spelling and grammar, 2015-06-02
	V0, R2:	updated per internal review
	V0, R1:	Draft; 2015-04-02
Authors:	Rudolf Chalupa	
Review:	V0, R4:	Courtney Linde (*exida*), 2015-08-10
	V0, R1:	William Goble (*exida*); 2015-03-30
Release status:	Released	

Release Signatures

Rudolf P. Chalupa, Senior Safety Engineer

Dr. Wiliam Goble, Principal Partner

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