The Meaning of Diagnostic Test Interval and Its Impact on the Performance of Safety Instrumented Functions

White Paper

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

July 2017

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

Copyright exida.com L.L.C. 2018-2020

Abstract

This paper explains what a diagnostic test interval (DTI) is, how it is measured, and how it impacts the safety performance of a safety instrumented function (SIF). In applications where a dangerous condition occurs infrequently, the DTI has an insignificant impact on PFDavg. For example, if a dangerous condition occurs once a week, then a DTI less than 1.68 hours will be insignificant. This calculation uses the 100X factor described in IEC 61508:2010. In applications with more frequent demands the impact can be determined as described below. However, the 100X factor is not always applicable. More accurate factors can be calculated even when the factor is as low 2X.

What is DTI and How is it Measured?

Many SIF include automatic self-diagnostics (ASD) which allow the SIF periodically to run internal tests of the correctness of certain SIF functionalities and to detect and annunciate failures of these functionalities. Since such failures can often be repaired while the SIF is operational, these ASD capabilities improve the safety that the SIF provides.

The ASD require certain resources also used by the SIF to perform its safety functions. Since the resources must be shared, the ASD are run periodically, rather than continuously, in such a manner as not to degrade the SIF safety functionalities. In some cases, the complete set of ASD tests are run from start to finish at designated time intervals. This is illustrated in Figure 1 which shows a timeline where the green areas represent times when the SIF is using resources to perform its safety functionalities and the blue areas represent the two times when the complete set of ASD tests are performed. In Figure 1 the first test in the ASD test series begins at T_1 for the first diagnostic cycle and the first test in the ASD test series begins at T_2 for the second diagnostic cycle. More commonly the set of ASD tests are run piecemeal interspersed with the safety functionalities as shown in Figure 2. In Figure 2 the first test in the ASD test series begins at T_1 for the first diagnostic cycle and the first test in the ASD test series begins at T_2 for the second diagnostic cycle. In both Figures 1 and 2, the DTI is measured from the time that the first test in the diagnostic test series is begun until the time that the first test in the diagnostic test series is next begun, i.e., the length of time from T_1 to T_2, as noted in Figures 1 and 2.

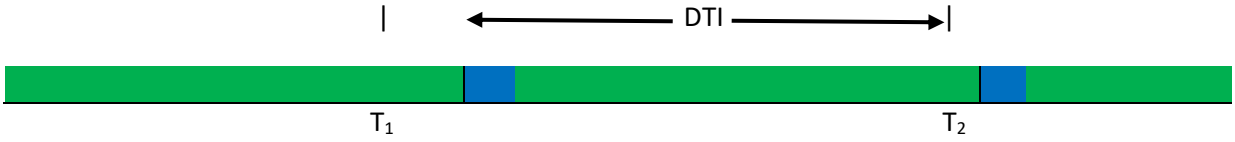

Figure 1. Illustration of DTI when ASD test series are run from start to finish at designated test intervals.

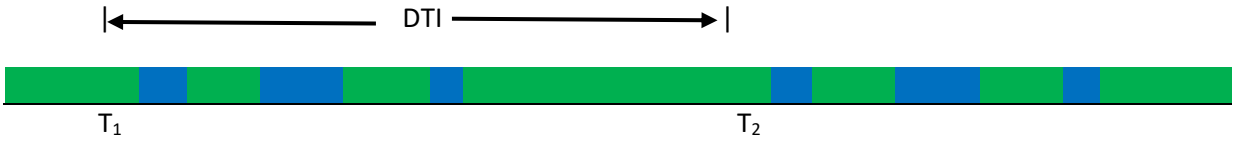

Figure 2. Illustration of DTI when ASD test series are run piecemeal between time intervals when the SIF functionality is using the SIF resources.

Typically, DTI can be as short as a few microseconds and for newer equipment is rarely more than 30 minutes. Some older equipment may have a DTI up to 2 hours. The rate of ASD is designated as λ_{Diag} and is defined as

$$\lambda_{Diag} = 1/DTI.$$

How Does DTI Impact SIF Safety Performance

The dangerous failure rate of a SIF is generally designated λ_D. If a SIF has ASD then λ_D is usually written as

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

where λ_{DU} represents the failure rate of those dangerous failures undetected by the ASD and λ_{DD} represents the failure rate of those dangerous failures detected by the ASD.

The purpose of ASD is to alert the user to dangerous failures so that ideally the failure can be repaired before the next demand on the SIF. This is how ASD improves SIF safety performance. Of course, the effectiveness of this approach is dependent on the rate at which demands are presented to the SIF. The demand rate is generally designated λ_{Demand}.

SIF safety performance metrics are always a function of λ_{DU} and a portion of λ_{DD} determined by the ratio of $\lambda_{Diag}/\lambda_{Demand}$. The larger the ratio, the more credit is given for the ASD meaning the greater the portion of λ_D that can be eliminated when computing safety performance metrics. Table 1 summarizes how credit is given for ASD and what portions of λ_D are used in evaluating the appropriate safety performance metric.

Table 1. Summary of How Credit is Give to ASD based on $\lambda_{Diag}/\lambda_{Demand}$ and what Dangerous Failure Rate is used in Computing Safety Performance Metrics.

Size of Ratio $\lambda_{Diag}/\lambda_{Demand}$	Credit Given to ASD	Dangerous Failure Rate Used in Computing Safety Performance Metric
$\lambda_{Diag}/\lambda_{Demand} \geq 100$	Full credit, i.e., λ_{DD} not used in computing metrics	λ_{DU}
$2 \leq \lambda_{Diag}/\lambda_{Demand} < 100$	Partial Diagnostic Credit (PDC)	$\lambda_{DU} + (1 - PDC)\ \lambda_{DD}$
$\lambda_{Diag}/\lambda_{Demand} < 2$	No credit	$\lambda_D = \lambda_{DU} + \lambda_{DD}$

Now the Partial Diagnostic Credit (PDC) is computed as [1]

$$PDC = (\lambda_{Diag}/\lambda_{Demand})\ (1 - \exp[-\lambda_{Demand}\ /\lambda_{Diag}]).$$

Figure 3 plots PDC vs $\lambda_{Diag}/\lambda_{Demand}$. Note that due to the exponential nature of PDC as a function of $\lambda_{Diag}/\lambda_{Demand}$, even for small values of $\lambda_{Diag}/\lambda_{Demand}$, relatively large portions of λ_{DD} are eliminated when computing safety performance metrics. Table 2 provides numerical values for PDC for a few sample points.

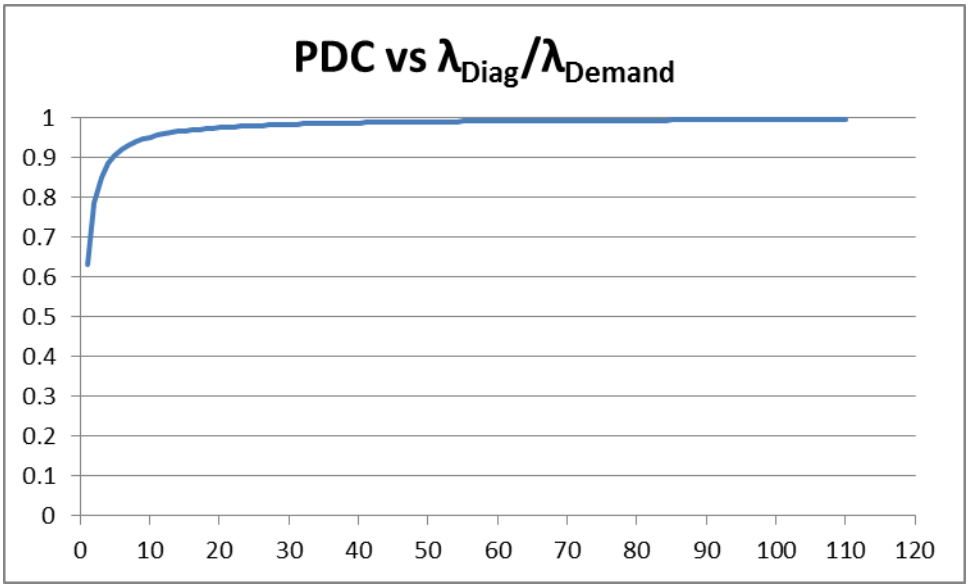

Figure 3. Plot of PDC vs $\lambda_{Diag}/\lambda_{Demand}$.

Table 2. Sample Numerical Values for PDC as a Function of $\lambda_{Diag}/\lambda_{Demand}$.

$\lambda_{Diag}/\lambda_{Demand}$	PDC
2	0.7869
10	0.9516
20	0.9754
50	0.9900

In Table 2, note how values of $\lambda_{Diag}/\lambda_{Demand}$ as little as 2 earn more than 78% credit for ASD. Clearly, if manufacturers have previously decided not to include ASD in a product because of a concern that ASD ran too infrequently to be given credit, this decision bears revisiting.

References

1. Bukowski, J. V. and Goble, W. M., "Properly Crediting Diagnostics in Safety Instrumented Functions for High Demand Processes," *Proceeding of the 2017 Annual Reliability and Maintainability Symposium*, Orlando, FL, January 2017.

Revision History

Authors: Dr. William M. Goble, CFSE, Dr. Julia V. Bukowski

Draft, V0, R1:	William Goble	
Release, V1, R1:	July 2017	Julia Bukowski, William Goble

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