Streamlining Process Safety Management for Reduced Risk

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

February 2018

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

Keywords: exida, exSILentia, Process Safety Lifecycle Management, IEC 61511, ISA 84, SIS, PSM 1910.119, Seveso II

Abstract

ARC Advisory Group recently met with exida to discuss the company's safety lifecycle management solution, exSILentia. The product is exida's response to the pressing need for comprehensive safety lifecycle management tools to manage the increasingly mandated safety regulatioons and standars. End users across a variety of industries are rapidly recognizing the need for better solutions to manage safety systems to reduce compliance costs and risk.

According to exida, the solution:

- Allows users to leverage data throughout the safety lifecycle so that data is only entered once for better accuracy
- Captures and institutionalizes corporate knowledge
- Spans across the entire enterprise

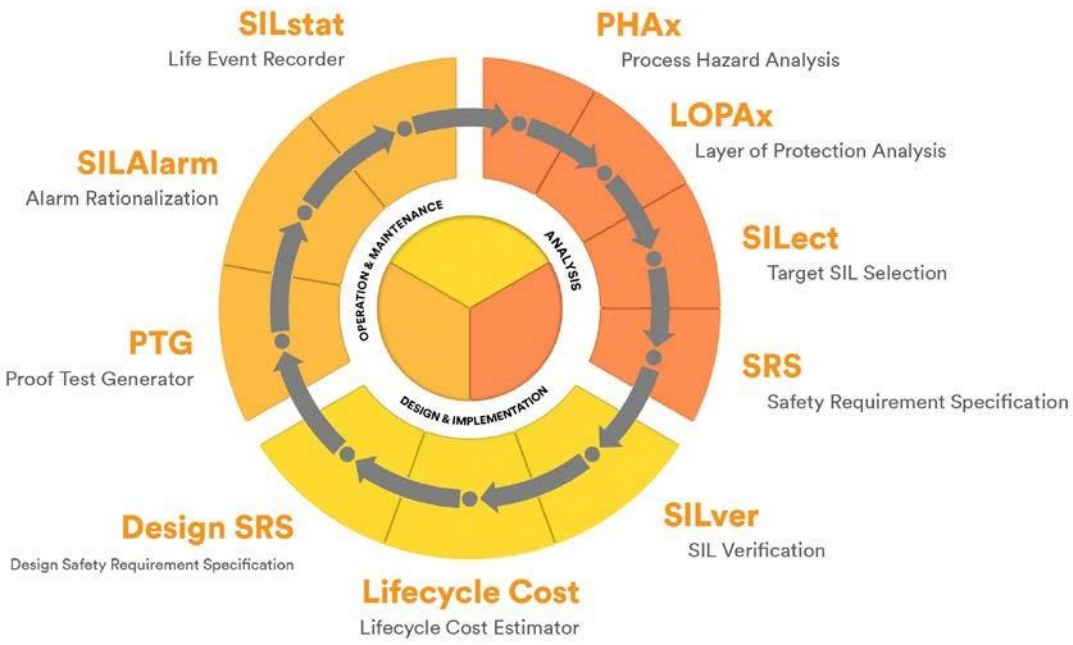
Creation of exSILentia

Founded in 2000 by several reliability and safety experts, exida is a leading product certification and knowledge company specializing in automation system safety, cybersecurity, and availability. The company began as a consulting organization, guiding end users through processes like process hazard analysis and evaluating various layers of protection and risk mitigation. exida leveraged this experience to produce tools used by its own consultants to expedite safety projects and increase its competitiveness and effectiveness. Eventually, the company made these tools into products for end users. It has worked to optimize these tools over time.

exSILentia: What It Does

According to exida, the current version of exSILentia integrates all safety lifecycle tools to create a coherent platform to manage a company's safety systems. Data is entered once and then exchanged between the different tools corresponding to phases of the safety lifecycle. This helps ensure efficiency and consistency in all safety lifecycle activities. It is deisnged to support the Process Safety Management (PSM) work process and the Safety Instrumented System (SIS) Fnctional Safety Lifecycle.

Cause-consequence pairs identified during the process hazard analysis (PHA) can be grouped in hazard scenarios. High-risk hazard scenarios can be flagged for further evaluation using layers of protection analysis (LOPA). Causes and associated safeguards are automatically identified for the selected hazard scenario and serve as a starting point for the protection layers to be considered in the LOPA. Alarm safeguard information can be brought into SILAlarm so that it is available during alarm rationalization.



exida's Intelligent Lifecycle Integration Model

The hazard scenario accident frequency calculated during LOPA becomes an input into the SIL target selection. If the accident frequency is higher than the consequence-based tolerable frequency, then additional risk reduction requirement for a safety instrumented function (SIF) may be required. exSILentia makes it possible to directly assign a risk reduction requirement to a SIF in the LOPA. In both cases, this risk reduction requirement and need for a SIF lead to the creation of a safety requirements specification (SRS). Information from the PHA, LOPA, and SIL target selection will feed directly into the SRS.

The solution automatically links safeguards identified as SIFs to the SRS. The company's SILver conceptual design evaluation/SIL verification tool then enhances these. The detailed modeling in the SILver tool is further extended, providing the user with more options to model more complex configurations as well as considering maintenance effectiveness and other issues. The embedded Safety Equipment Reliability Handbook (SERH) database (a comprehensive reliability database for automation equipment) is then applied to calculate the safety integrity level of the safety instrumented function.

The results from the conceptual design lead to the definition of a design SRS. This detailed design input document specifies implementation requirements for the evaluated SIF. The data flows to the SILStat software, through which users can define a model for capturing SIS operation and maintenance data, such as proof tests and SIS demands, while they are documenting the detailed design. This ensures that all important lifecycle information is documented in a single sourc

Industry Challenged in Safety

One of the key challenges in industry today is the largely "set-and-forget" mentality with regard to safety. But safety systems are "living" entities and don't generally age well. There is a very solid methodology for the initial design and implementation of an overall safety system. However, maintaining a safety instrumented system over time can be labor intensive and the appropriate safety expertise is neither cheap nor easy to come by. Complying with the ISA-84 and IEC61511 guidelines is difficult at best, and many companies continue to have differing, even conflicting views on how to implement and operate in accordance with the guidelines.

Regardless, an enterprise cannot address issues it cannot see. A disparate collection of offline documentation, spreadsheets, and instrument databases hamper visibility, exacerbating the challenge users face to maintain their safety systems for optimum performance.

Current methodologies lack adequate techniques to monitor the performance of the implemented systems based on real-world interactions. As such, end users lack a single view to help identify shortcomings easily. Instead, this arrangement relies on several individuals to enter and maintain the records and other individuals to pull the data together and interpret the meaning. In the case of an audit, the reports are time consuming, tedious, and likely to contain errors. Given the current state of the labor market, it's often difficult to keep safety-qualified personnel at site. This can also complicate record keeping and monitoring of the overall safety systems' status. ARC believes comprehensive, integrated "cradle-to-grave" tools are critical for end users. Most end users have a menagerie of disjointed data repositories that are difficult to maintain. Solutions like exSILentia are crucial for companies serious about process safety compliance and industry leadership.

The solution offers another benefit in that the safety knowledge is no longer floating in several different databases or with different personnel who might leave due to retirement, for example. Instead, it is captured in a single referenceable repository; accessible and auditable. This is important as safety talent becomes more difficult to replace.

Revision History

Author: Mark Sen Gupta

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