



Setting the Standard

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

May 2011

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

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

Introduction

Process industry safety standard IEC 61511 and its parent, functional safety standard IEC 61508, have been in existence for several years now, and have enjoyed widespread acceptance as an effective method for managing high levels of industrial risk. Despite this success, some may view these standards as another complex, onerous burden imposed by regulators, with little tangible benefit to the end user. However, as we will explore in this article, the reality is far different.

The standards, which have grown out of industry needs rather than being imposed from outside, bring considerable benefits if applied properly. These benefits take the form of improved safety, cost-effective design and maintenance processes, and reduced downtime – all of which impact positively on the bottom line. Compliance also helps to demonstrate to the authorities that all reasonable precautions are being taken to prevent major accidents, as required safety legislation nowadays.

Functional Safety Concept

The underlying need for IEC 61511 arises from the fact that processes involve major hazards, with significant potential to cause losses and harm. The risk of these undesirable outcomes is a function of both their severity – for example, how many people injured or killed, and how much damage and lost production – and their frequency, that is, how often such an event can be expected to occur.

We seek to control these hazards by reducing the risk to a tolerable level. How we do that is up to us, but it usually involves a range of measures, some engineering, some procedural, and some down to process technology.

But even after applying as many of these measures as we can, it is likely that a number of risks will still be too high. Simply loading up our plants with more alarms, relief valves and operating procedures will not resolve the issue; a law of diminishing returns applies, for reasons beyond the scope of this article. In such cases, we have to go to our next line of defense: active, automated trip systems, known properly as safety instrumented systems (or SISs).

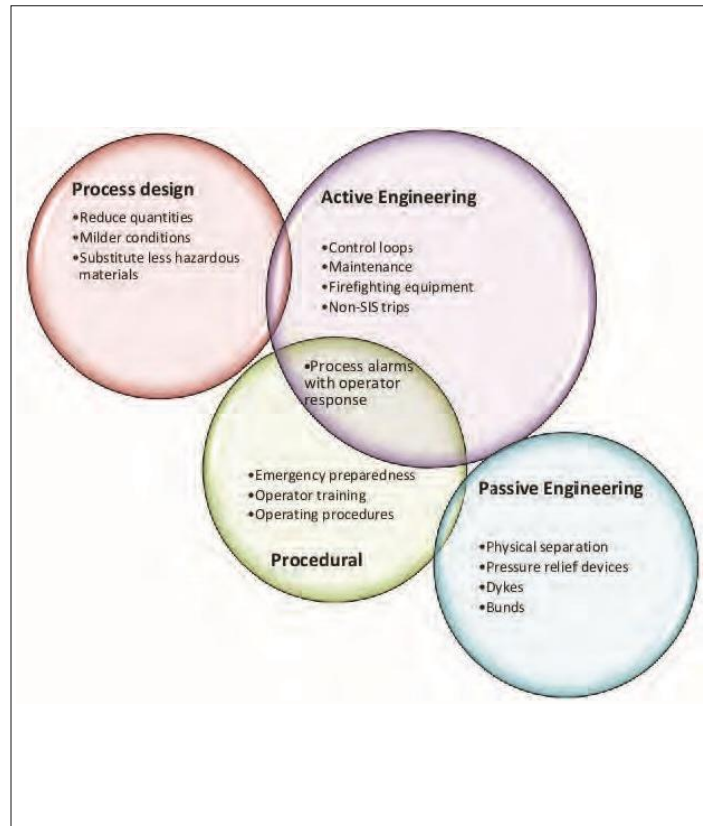
Because of the weight of risk reducing responsibility placed on SISs, we must employ them with great care. There is no such thing as an off-the-shelf SIS, or a one-size-fits-all trip that we can simply install and forget. Each risk has to be matched with a custom designed safety function from the SIS. If we don't design, install and maintain these correctly, they are more likely to fail on demand, trip when not required, or provide insufficient protection against the harm we are seeking to avoid. For the process industry, our guiding hand through the complex and challenging world of SIS is the international standard IEC 61511. It explains that our SIS needs our attention from cradle to grave – and even before the SIS arrives in the cradle, when we are still wondering whether we need to install a SIS at all.

The standard addresses this lifetime care through the concept of a safety lifecycle. Broadly speaking, the lifecycle can be separated into three periods, in which we ask respectively:

- Do I need a SIS, and if so, what type?
- How can I design a SIS to meet that need?
- When I'm up and running, how can I make sure the SIS keeps working?

Examining the Safety Lifecycle

In the first lifecycle period, we *analyze* the risks involved in running the plant. First, we must decide how much safety risk we can tolerate; optionally, we can also consider other types of harm such as environmental damage, downtime, equipment damage and loss of reputation. Zero risk is not a meaningful target, because it is unachievable – however much our top management team might like to believe otherwise. So, we have to set finite risk targets, as the basis for all our subsequent lifecycle activities.



Typical (non-SIS) measures to reduce hazards in process plants.

Next, we examine the process to identify all the causes of risk. For each event that can lead to unwanted outcomes, we have to determine the probable frequency of the event (for example, how many times per year) and the severity (for example, the cost of damage to the plant). We assign risk reduction measures – safety features like those depicted (left) – and decide how much additional protection is needed from an SIS.

For each intolerable risk, a safety function is defined, that is, an action to take when specified dangerous conditions are met. Based on this, we prepare a specification known as an SRS (we'll discuss this later). The SRS will document, among other aspects, how reliable each safety function must be, in terms of its probability of failure to act when required due to some random hardware fault. This safety integrity measure is defined in terms of a safety integrity level or SIL, which is a numerical value from 1 to 4.

In the second safety lifecycle period, we *design* an SIS to meet the specification. Hardware is selected; calculations are performed to ensure the hardware can achieve the specification; software and maintenance procedures are written; and extensive tests and checks are performed, both before and after the safety equipment is installed and commissioned. And then in the third lifecycle period, we *operate* the plant with the SIS in place. We document the performance of the SIS and the demands that are made on it by the plant (whether real events or spurious). We carry out the maintenance of the SIS as planned; and we carefully control every change to the SIS design through a management of change procedure (discussed in detail later in this article).

Control of Design Errors

So far, in our discussions of SIS reliability, we have implicitly considered only one type of failure: a random component failure, caused by natural degradation and/or unpredictable external stressors such as heat, cold and vibration.

In reality, another type of failure is just as important – in fact, even more so, in the case of tech-heavy equipment such as safety PLCs. This type is characterized by *design errors*, which may lie hidden like the proverbial snake in the grass until an unfortunate combination of circumstances conspires to bring it to full, ugly manifestation.

In instrumented safety parlance, these undesirable incidents are known as *systematic failures*, because they occur *systematically* whenever the right conditions exist. Some typical systematic failure types are listed in Table 1. A simple (non-SIS) example is a check valve (non-return valve) installed the wrong way round: on the day when a backpressure occurs, it's guaranteed to allow the reverse flow you don't want. In other words, its failure is *deterministic*: failure is determined only by circumstances, and is not dependent on random outside influences.

The approach to dealing with these two types of failure – random and systematic – is radically different. Random failures will always be with us, and can never be engineered away entirely. We see this in our own bodies: we get sick due to random outside influences, we have accidents, and our bodies eventually wear out and die. That's why we have health checks, preventative maintenance (do you brush and floss regularly?), and insurance. These have echoes in the maintenance strategies we apply in the operational third period of the safety lifecycle.

Systematic failures, on the other hand, can be eliminated by good engineering and management practices. Indeed, not only *can* they be eliminated, but they *must* be. Providing the methodology for dealing radically with the causes of systematic failure is one of the great strengths of IEC 61511.

Multi-Layered Strategy

IEC 61511 develops a multi-layered strategy for tackling systematic failures. To understand this, we can divide our focus into three main concepts: components, SIS design, and project management.

At the Component Level

IEC 61511 requires us to take steps to eliminate design errors in the components of our SIS. This can be done in one of two ways: either we buy components whose design and construction methods are proven adequate (the SIL certification route), or we select components with a good track record (the prior use or proven-in-use route). Getting SIS components such as sensors, valves and safety PLCs SIL-certified is usually the responsibility of the equipment manufacturer. The requirements for SIL certification are detailed in IEC 61508, which is the “mother standard” of IEC 61511 (and of other sector-specific standards dealing with safety instrumented systems, such as IEC 62061 for the machine industry).

More and more equipment vendors are recognizing the value of SIL certification; it generates an easy pathway for end users to justify selection of their equipment, and also provides assurance of the quality of their manufacturing and design processes.

SIL certification services are provided by a handful of independent auditors, including TÜV Rheinland, TÜV Nord and Exida. The latter also maintains a Safety Automation Equipment List, which is available for consultation online (www.sael-online.com), and is also built in to the risk analysis software exSILentia.

When a product is SIL certified, the certificate will specify the maximum SIL that is achievable by any safety function using that component. All the data required to quantify the reliability of the safety function should also be provided, either in the certificate or in the associated assessment report, and many other sources of failure rate data are available.

Prior use, the alternative, and generally more arduous, approach is for individual users to show that the components perform as well as expected in real applications. The standard does not define exactly how much history is required, but typically the minimum requirement for SIL 1 will be for 100,000 operating hours and 10+ items in different applications over at least one year, with failure rates no worse than those predicted by theoretical calculations. The higher the intended SIL of the proposed application is, the more prior use evidence is needed.

Prior use data need not necessarily refer only to safety applications; non-safety applications, such as basic process control systems, can also be taken into consideration. Crucially, however, the standard does require that the historical data be demonstrably relevant to the intended application. In practice, this means the item must be essentially exactly the same as the ones used before – in particular, the revision number of any built-in software must match; and the components must have been used in “similar operating profiles and physical environments”, in the words of IEC 61511. Proving this is often a major stumbling block to the successful deployment of prior-use justification. Clearly, it also depends critically on the quality of reliability data collection – a topic we will return to later.

Because of these challenges, many users are inclined to default to the use of SIL certified components for all SIS applications. However, this is not always the best strategy. Sometimes it is better to stick with the equipment you already know well, if it has been performing incident-free in your application for many years. There are several reasons for this:

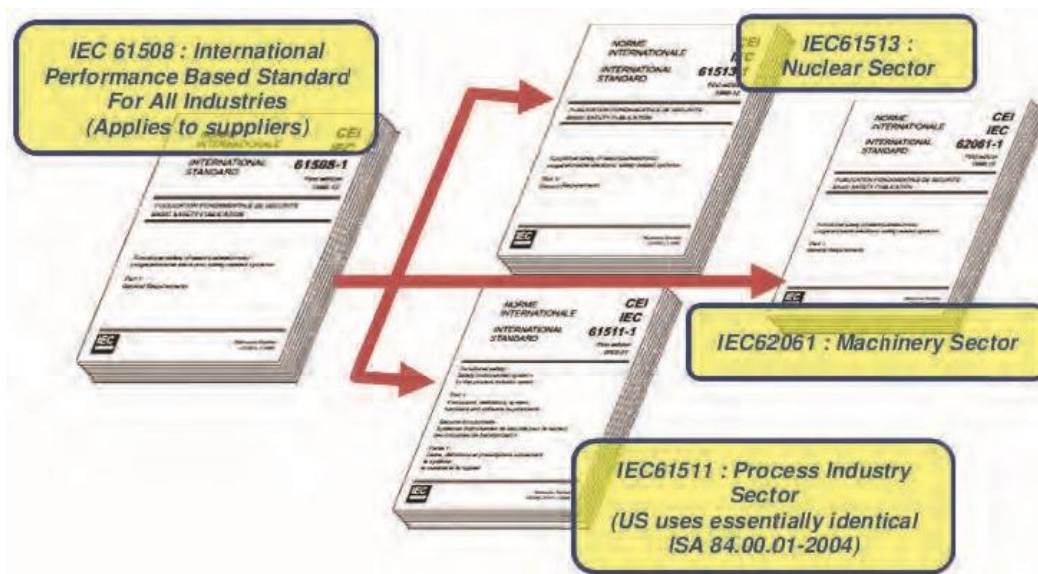
- Your technical personnel are already familiar with it, and are therefore less likely to make mistakes during installation and maintenance.
- Fewer different models of equipment onsite means fewer spares and, again, reduced likelihood of errors.

- You already know, from direct experience, what its performance limitations are – for example, how long it lasts before wear out in your specific plant environment.

Thus, users should not rule out the “prior use” route, despite its difficulties. And software tools such as exSILentia are available to help with the process of developing prior use justification.

SOFTWARE-RELATED	HARDWARE-RELATED
Bugs in the application software	Unsuitable for process or physical environment
Errors in user programming	Wrong material of construction
Software bypasses left in place	Manufacturing flaws or errors
Out of date versions or version mismatches	Incorrect installation
Inadequate training or bad information provided to operators	Hardware bypasses or forces left in place
Inadequate training or bad information provided to maintenance personnel	Wrong specification in SRS (e.g. due to poor risk analysis)
Miscalibration	Design does not meet specification in SRS
Wrong set point or other parameter	Equipment not installed according to design
Confusion over engineering units	Equipment limitations (as listed in safety manual) not complied with
Uncontrolled changes	Uncontrolled changes

Table 1: Typical systematic failures.



The requirements for SIL certification are detailed in IEC 61508, which is the “mother standard” of IEC 61511 and other sector-specific standards dealing with safety instrumented systems.

At the SIS Design Level

Compliance with IEC 61511 helps us to eliminate design errors in the SIS itself. Again, there are two aspects to this, both of which run like a mantra throughout the subtext of the standard: designing it right, and documenting it right.

First of all, let's look at designing it right. Because IEC 61511 places a heavy emphasis on upfront risk analysis, it compels us to make sure we really understand the demands we are making of our safety functions. Historically, improper specification is known to be one of the major factors that can lead safety functions to fail in their objective of preventing accidents. Getting to a correct specification requires us to go meticulously through a thorough risk analysis process, with all of its attendant benefits.

Up to this point, we know what our risk reduction target is. The next crucial step is to ensure our design can achieve it. IEC 61511 once again drives this process by requiring a calculation of the theoretical risk reduction achievable by our design, long before we ever go on site to install the hardware. The calculation is not trivial to perform, and can be delegated to outside consultants, but suitable software tools – even for highly complex safety functions – are also available.

As for documenting it right, today's large projects are becoming more and more subdivided and distributed among different contractors – a process which, whilst it has its advantages, can lead to communication breakdown and nebulous responsibility. The ultimate consequence can be disastrous, as numerous process plant disasters have shown.

To address these issues, IEC 61511 places a strong emphasis on effective documentation at every stage of the safety lifecycle. In particular, it requires the creation of a document known as the safety requirements specification (SRS), which we met briefly earlier.

The SRS is first generated when the requirement for a SIS has become clear, and the target performance specification of the SIS is known – for example, how much risk reduction it should provide, what hazards it is designed to address, and what it must do to prevent harmful outcomes when those hazards arise. Later in the design process, the SRS is revised to include specific details of the hardware that will be used to realise these objectives.

The SRS is a critical document in the safety lifecycle, for many reasons, but particularly because:

- It provides a touchpoint for all parties involved in the safety lifecycle, whether they are designing, constructing, commissioning, maintaining, or modifying the SIS.
- It defines a benchmark against which the performance of the safety lifecycle is measured. This applies to every aspect of the lifecycle. For example, designers must check that their designs match the requirements of the SRS; maintenance personnel must ensure they carry out the maintenance as detailed in the SRS; and operational management must confirm that the real-world situation (magnitude of the risks and performance of the SIS) matches the assumptions made in drawing up the SRS. All of these checks are explicitly demanded by the standard.

Thus, the SRS serves as a hub for validation of all subsequent lifecycle activities. Compiling an effective SRS is an onerous task but, as with many other aspects of lifecycle activity, consultants and tools are available to help.

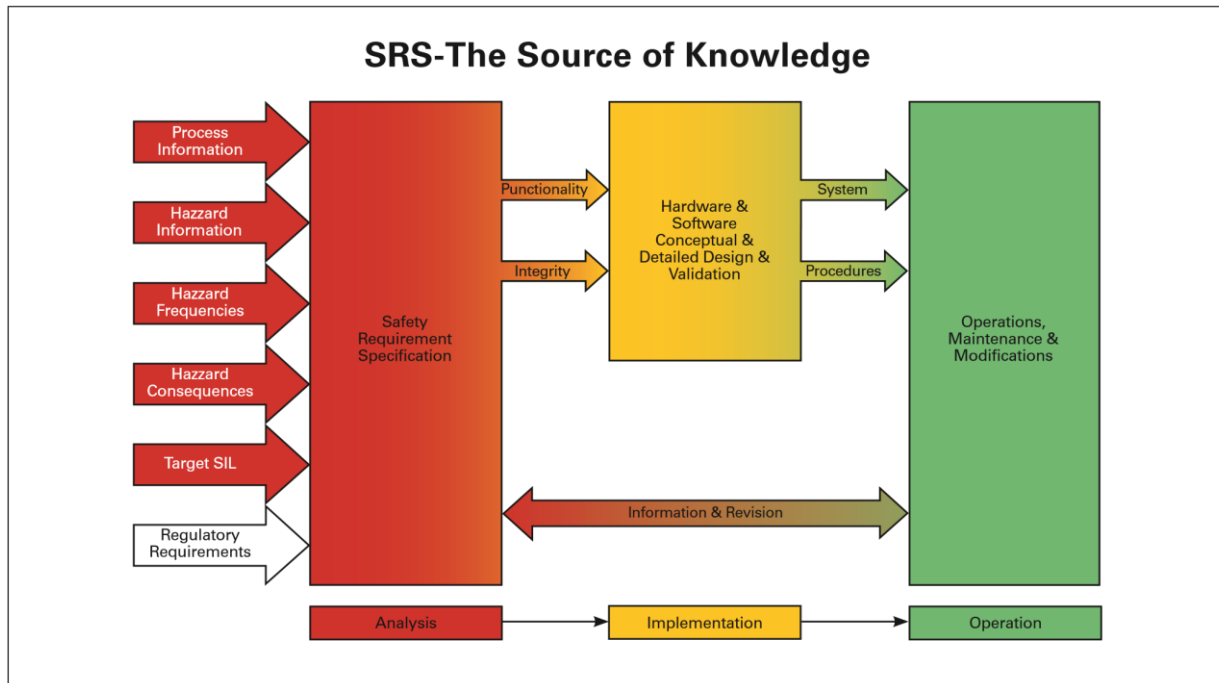
At the Project Management Level

In parallel with all the phases of the safety lifecycle, IEC 61511 demands proper management of every activity undertaken, from first concept to final disposal of the safety equipment. There are many aspects to this – competency requirements, planning, and documentation control, to name a few – but, for our purposes, we will focus on two particular aspects here: confirmation that the lifecycle is doing its job in delivering safety, and management of change.

Confirming lifecycle performance is not a new concept to those familiar with ISO 9000. Not only must procedures be followed, but they must be shown to be followed. Not only must procedures be written, but they must be shown to achieve the objectives for which they were designed. Not only must quality be pursued, but it must also be achieved in real life. Not only must we say it, but we must also prove we do it (and know how to do it).

These four axioms of quality management are right there in IEC 61511, too. In the safety world, they are referred to respectively as Verification, Validation, Functional Safety Assessment, and Auditing. They may seem tough, but they allow us to reap rewards by getting it right the first time, and ensuring all the mistakes are found while they exist only in ink, and not in hardware – or in disasters.

Because the standard is performance-based, it does not impose many specific, prescriptive demands on our plant design, or on the process by which we achieve that design. Thus, we can develop a safety management strategy that suits our own corporate culture and framework. It is not necessary to develop a whole extra tier of paperwork to manage the safety lifecycle; integrating the lifecycle requirements into our existing procedures for planning, design, construction and maintenance is just as acceptable.



A critical document, the safety requirements specification (SRS) provides a touchpoint for all parties involved in the safety lifecycle

For the second aspect, there is nothing extraordinary about requiring a management of change (MoC) procedure in an operating plant. What is noteworthy is the thoroughness of the MoC approach required for IEC 61511 compliance.

Indeed, it is at this stage that the cyclic nature of the lifecycle becomes most apparent: for the MoC strategy demands that we analyse all the possible effects of any changes to the plant, however trivial, and, if necessary, revert to an earlier stage of the lifecycle. Thus, we may need to revisit and revise our risk analysis steps, SRS, design, and/or maintenance procedures. Again, the value of excellent documentation is highlighted: if we took the trouble to write everything up properly the first time around, the impact of plant changes will be that much easier to evaluate later.

Demanding a thorough analysis of the impact of potential changes is a good discipline that chokes off the cause of many accidents. For example, the terrible disaster at the Flixborough chemical plant in the UK in 1974, which cost 28 lives, could have been avoided by proper MoC. Another benefit of rigorous MoC procedures is that they should prevent the “stealth” changes that gradually insinuate their way into a plant over time: set points changed, trips overridden, and hardware bypassed. They should spell the end of unforeseen impacts due to staffing reductions, loss of experienced staff, and temporary fixes left in place for months.

Bottom Line Benefits

So what is the benefit of adopting an IEC 61511 approach to functional safety? The short answer: it pays. Proper risk analysis avoids dangerous under-engineering that leaves a plant vulnerable to huge losses; it also cuts back on over-engineering, often paying for itself many times over in reduced upfront and maintenance costs, not to mention significant gains in operational uptime.

Thorough attention to design integrity provides the only viable way to eliminate systematic failures, which can otherwise take out an entire safety system in one step. Detailed management of the design process ensures costly errors are eliminated before purchase orders are written for pricey safety hardware. Finally, the rigorous discipline of planned, appropriate maintenance procedures and scrupulous management of change are practically guaranteed to pay for themselves in reduced downtime and enhanced safety.

IEC 61511 helps you win all of these benefits through its integrated approach to instrumented safety, which you will be able to enjoy for the entire lifetime of your plant.

For process plant owners, through its integrated approach to instrumented safety, IEC 61511 can pay for itself many times over.

Revision History

Authors: Dr. Peter Clarke

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



excellence in dependable automation

- 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