DOWNLOAD PDF IEC 61511 1

Chapter 1 : Recent Changes to the IEC Standard for Functional Safety for the Process Industry

IEC is available as IEC RLV which contains the International Standard and its Redline version, showing all changes of the technical content compared to the previous edition.

Those requirements are listed in a document called the certification scheme. Certification Bodies are accredited to perform the auditing, assessment, and testing work by an Accreditation Body AB. There is often one national AB in each country. IEC certification programs have been established by several global Certification Bodies. Each has defined their own scheme based upon IEC and other functional safety standards. The scheme lists the referenced standards and specifies procedures which describes their test methods, surveillance audit policy, public documentation policies, and other specific aspects of their program. It is being widely adopted by the major car manufacturers. Before the launch of ISO , the development of software for safety related automotive systems was predominantly covered by the Motor Industry Software Reliability Association guidelines. A set of guidelines for the development of vehicle based software was published in November MISRA C has gone on to become the de facto standard for embedded C programming in the majority of safety-related industries, and is also used to improve software quality even where safety is not the main consideration. MISRA has also developed guidelines for the use of model based development. It is intended to cover the development of software for railway control and protection including communications, signaling and processing systems. Process industries[edit] The process industry sector includes many types of manufacturing processes, such as refineries, petrochemical, chemical, pharmaceutical, pulp and paper, and power. IEC is a technical standard which sets out practices in the engineering of systems that ensure the safety of an industrial process through the use of instrumentation. Nuclear power plants[edit] IEC provides requirements and recommendations for the instrumentation and control for systems important to safety of nuclear power plants. It indicates the general requirements for systems that contain conventional hardwired equipment, computer-based equipment or a combination of both types of equipment. It provides requirements that are applicable to the system level design of all types of machinery safety-related electrical control systems and also for the design of non-complex subsystems or devices. Testing software[edit] Software written in accordance with IEC may need to be unit tested , depending up on the SIL level it needs to achieve. The main requirement in Unit Testing is to ensure that the software is fully tested at the function level and that all possible branches and paths are taken through the software. In some higher SIL level applications, the software code coverage requirement is much tougher and an MCDC code coverage criterion is used rather than simple branch coverage. To obtain the MCDC modified condition decision coverage coverage information, one will need a Unit Testing tool, sometimes referred to as a Software Module Testing tool.

Chapter 2 : What is IEC ? - Definition from Safeopedia

IEC standard is a technical standard which sets out practices in the engineering of systems that ensure the safety of an industrial process through the use of instrumentation.

Under a strict interpretation of the IEC definition, these would not even be considered systematic failures! The conflicting messages in the standard are unfortunately often reinforced by vendors and SIL certifying bodies. Worried about plugging, fouling, corrosion, leakage, freezing, wear, vibration, lightning, misconfiguration, operator error? Sorry, those are systematic failures and are not included in your SIL-certificate failure rate! The result is that failure rates from SIL certificates are frequently an order of magnitude lower than field data from end users e. Learn Something New Today! Schizophrenic Standard These quibbles about definitions would not be such a big deal, except that after vastly expanding the world of possible systematic failures, IEC then proceeds to give conflicting guidance on what to do about systematic failures. Regarding measurement of systematic failures, on the one hand it says: Clearly, a systematic failure is still a failure, and failures can be monitored based on field feedback. Elsewhere in the standard, it asserts that systematic failures cannot be modeled quantitatively: Common cause failures are dominated by systematic failures, yet we have no problem modeling them quantitativelyâ€¦? For another example, the entire field of Human Reliability Analysis HRA is dedicated to quantitatively modeling the largely systematic failures of human beings. I believe this is a mistake and leads to nothing but confusion in the SIS field. Clearly, systematic failures can be quantitatively modeled. The key distinction is that they should not only be modeled. Recall that once detected, systematic failures can often be eliminated. The difficulty comes in classifying failure types as random or systematic. But does classification really matter? A Distinction Without a Difference? The classification of a failure as random or systematic is difficult because it is largely a subjective exercise. Is this a random failure since the temperature was less than the design temperature? Or was it a systematic failure because the specification failed to include adequate safety margin to account for variations in temperature? A case could be made either way. Is there a difference, really? Classifying things as systematic failures really just acknowledges that there are failure mechanisms that do not fall neatly into the physics models and accelerated test plans used to predict failure rates. In addition to the aleatory uncertainty that exists even in relatively ideal conditions, there will always exist additional epistemic uncertainty due to things like human error, application condition changes, supplier quality issues, etc. The end result is simply that uncertainty is higher than we might expect in the idealized model. This can be visually demonstrated in the traditional stress-strength model of reliability: It seems to me an unnecessary and unfortunate distinction. A SIL calculation based on end-user failure rate data containing both random and systematic failures will more accurately represent the probability of failure on demand. As per the IEC definition above, the important question is now that you know about it, can it feasibly be eliminated? Now this becomes a question not of philosophical classification, but just practical questions of i whether the fault can feasibly be eliminated and ii what safeguards can be put in place to prevent the same problem from occurring elsewhere. A Bayesian Side Note I think part of the reason the standards distinguish between random and systematic failures is that they are influenced by Frequentist statistical thinking, which often separates aleatory uncertainty i. Epistemic uncertainty does not fit well into the frequentist philosophy, so they try to avoid or eliminate it. A funny example I heard somewhere: What is the probability that an asteroid will destroy the earth tomorrow? The probability is either 1 or 0. I will let you know day after tomorrow. On the other hand, Bayesians treat epistemic uncertainty the same way as aleatory uncertainty. For frequentists, epistemic uncertainty must be qualitatively avoided or minimized. For Bayesians it can be treated as part of the quantitative model. SIS engineers are inherently Bayesian see my Bayesian paper and should embrace this philosophy Conclusions This post has been longer and more philosophical that many of my posts, so let me try to sum it up succinctly. My key points are: IEC expands the definition of systematic failures beyond IEC and leads people to think that many common SIS failures are systematic and therefore need not be quantitatively modeled. This is an error since the PFDavg calculation should incorporate all available available information to make it an accurate and useful metric. Many systematic failures are stochastic in nature and can and should be probabilistically modeled. Rough estimates of systematic failure rates can be found by comparing end-user data to theoretical data. These estimates can be refined per application based on user data. The distinction between systematic failures and random failures is not as important as people make it seem. Every failure should be considered a potential systematic failure until it is determined to be infeasible to address it. My colleague was intrigued but not convinced. Maybe this post will help. Please checkout other popular SISEngineer.

Chapter 3 : IEC is Wrong About Systematic Failures | calendrierdelascience.com

IEC , is integrated into an overall system that is to be used for a process sector application but does not apply to manufacturers wishing to claim that devices are suitable for use in safety instrumented systems for the process sector (see IEC and.

Presented here is a summary of what IEC is, the changes that have been made and how Asset Guardian provides a solution in relation to complying to the standard. The focus is on Part 1 of the standard. What is IEC ? It sets forth a number of best practices to ensure the safety of Industrial Processes and covers the management, specification, design, verification and validation of these systems. It is the national standard of Great Britain and the European Union. The increase in the connectivity of computerised industry across the world would have been hard to predict in and as a consequence Digital cyber security is now considered in the standard. Digital Security assessments must now be carried out in order to prevent unauthorised access and external cyber security threats such as malware, ransomware and denial of service attacks. There is also now a greater focus on the competence of personnel, with requirements to record more details such as training and competency records. How Asset Guardian helps compliance with IEC part 1 The new edition on the standard specifically states that SIS software, hardware and procedures must be subject to configuration management and are maintained under revision control. This is the primary function of Asset Guardian. Software, Hardware and Documents are recorded in Asset Guardian and given a unique identifier and all aspects of configuration management may be planned, managed and reported on. Modified software, maintained under revision control, is not made available until authorisation is given by someone in the correct responsible role. All aspects of change management, workflows and authorisation may be tailored to the specific needs of an organisation. Asset Guardian Software, Hardware and Documents are always logged in against version numbers and a full Revision History is available showing the active version and all previous versions. In addition, documentation may also be attached to specific items of software or hardware as Supporting Documentation. Other key features of Asset Guardian that meet requirements in the new edition: To meet the new requirements on Digital Security, Asset Guardian provides sections for cyber security management where the planning and co-ordination of cyber security activities may be carried out. Asset Guardian may also be used as part of the organisations disaster recovery plan. Software backups required for disaster recovery may be stored in Asset Guardian under full revision control. The standard requires that modifications to the SIS are carried out by suitably qualified and trained personnel. Asset Guardian offers the facility to limit user access to software and hardware records, assign roles and responsibilities in regards to such things as authorisation, approvals and close out of modification request workflows. Competency Records may also be attached to users in Asset Guardian. Asset Guardian can also send automatic notifications to responsible and affected personnel for that system, giving full details of the change or modification made. Asset Guardian can be used to store, control and communicate documentation and information within the organisation. In fact Asset Guardian can be used as part of any audit process to schedule, record and document all associated tasks. Modifications to the documentation and improvements to the processes required by the standard may be tracked in the Change Requests section of Asset Guardian. Observations made during the audit process may also be recorded as Change Requests. Nonconformities raised during the audit process may be recorded as Faults. The Asset Guardian Change Request section also allows the initiation, documentation, review, approval and implementation of changes to the safety instrumented system SIS. Further details of reviews can also be logged in the Design Reviews section and linked to the Change Request. The requirements for testing e. Test Results may be scanned and logged into the Documents section. Failures from testing may be logged and tracked in Asset Guardian as Fault Logs. This allows the reason for failure to be entered and analysed using Root Cause Analysis and the corrective actions documented. Tests carried out as part of the implementation of change may be attached to the relevant Change Request. If you would like any more information on Asset Guardian, please fill out the contact form below and a member of our team will be in contact soon.

Chapter 4 : Edition Method Functional Safety

IEC has been developed as a process sector implementation of IEC The contents of the corrigendum of September have been included in this copy. This consolidated version consists of the first edition (), its amendment 1 () and its amendment 2 ().

Scope[edit] The process industry sector includes many types of manufacturing processes, such as refineries, petrochemical, chemical, pharmaceutical, pulp and paper, and power. The process sector standard does not cover nuclear power facilities or nuclear reactors. IEC covers the application of electrical, electronic and programmable electronic equipment. While IEC does apply to equipment using pneumatic or hydraulic systems to manipulate final elements, the standard does not cover the design and implementation of pneumatic or hydraulic logic solvers. This standard defines the functional safety requirements established by IEC in process industry sector terminology. This document sets the standards for safety-related system design of hardware and software. IEC is generic functional safety standard, providing the framework and core requirements for sector specific standard. IEC provides good engineering practices for the application of safety instrumented systems in the process sector. It primarily mirrors IEC in content with the exception that it contains a grandfathering clause: For existing safety instrumented systems SIS designed and constructed in accordance with codes, standards, or practices prior to the issuance of this standard e. This means that in each of the member states of the European Union, the standard is published as a national standard. The content of these national publications is identical to that of IEC Note, however, that is not harmonized under any directive of the European Commission. It starts in the earliest phase of a project and continues through startup. It contains sections that cover modifications that come along later, along with maintenance activities and the eventual decommissioning activities. The standard consists of three parts: Framework, definitions, system, hardware and software requirements Guidelines in the application of IEC Guidance for the determination of the required safety integrity levels ISA An SIS is composed of a separate and independent combination of sensors, logic solvers, final elements, and support systems that are designed and managed to achieve a specified safety integrity level SIL. An SIS may implement one or more safety instrumented functions SIFs , which are designed and implemented to address a specific process hazard or hazardous event. The essential roles of the various personnel assigned responsibility for the SIS should be defined and procedures developed, as necessary, to support the consistent execution of their responsibilities. A hazard and risk analysis is used to identify the required safety functions and risk reduction for specified hazardous events. Safety functions allocated to the SIS are safety instrumented functions; the allocated risk reduction is related to the SIL. Field data are collected through operational and mechanical integrity program activities to assess actual SIS performance. When the required performance is not met, action should be taken to close the gap, ensuring safe and reliable operation.

Chapter 5 : IEC - Wikipedia

IEC has been developed as a process sector implementation of IEC In particular, IEC a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (e.g., designers, suppliers, owner/operating company, contractor).

Chapter 6 : Functional Safety Standards - IEC vs. IEC | exida

The relationship between IEC and IEC is also defined in Part 1. Sep. definitions and abbreviations (same apply as for part 1). The key differences between IEC and IEC are discussed in Part 1. Annex A. this part of IEC corresponds to part 6 of IEC and 4 of IEC have thus been combined into part 1 of IEC

Chapter 7 : INTERNATIONAL STANDARD IEC - IEC Webstore - calendrierdelascience.com

DOWNLOAD PDF IEC 61511 1

IEC is a technical standard that is applied to Safety Instrumented Systems (SIS). It sets forth a number of best practices to ensure the safety of Industrial Processes and covers the management, specification, design, verification and validation of these systems.