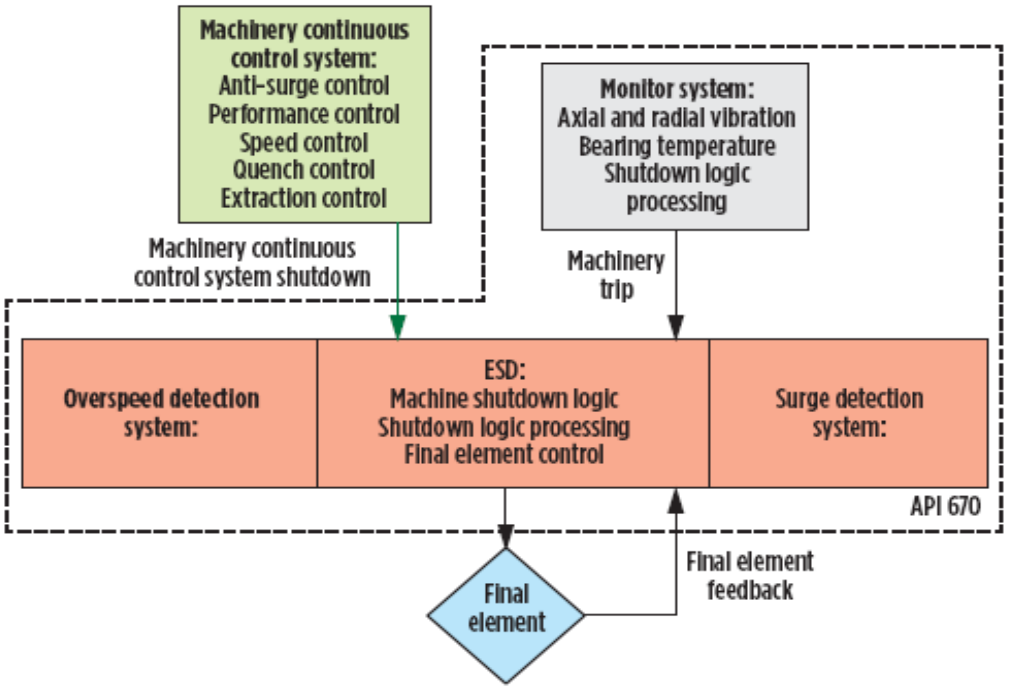
Honeywell
CCC

WHITEPAPER

Control and Safety for Turbomachinery



Publish Date: 12/1/2014
Author: Serge Staroselsky, Jeff McWhirter, Wayne Jacobson

It is crucial to realize that SIL rating is not synonymous with higher levels of availability. Proper use of redundancy, diagnostic coverage and control algorithms allow non- SIL rated control systems to achieve similar availability levels to SIL-rated systems.

All plant workers want to reduce the safety risk associated with turbomachinery operation while avoiding nuisance trips. The goal is to run machines in an efficient manner. In this context, safety risk refers to catastrophic events, such as turbine overspeeding, which can lead to severe injury or death, not to mention lost revenue and extensive repairs. Rigorous analysis of the failure causes and their mitigation can significantly reduce the risk of catastrophic failure. However, full compliance with the safety standard requirements, such as IEC61508, can lead to additional complexity and cost in regard to control and safety system procurement. This places a greater burden on the plant engineers for selecting a safe, reliable system, and one that actually improves process operations. Thus, it is important to clarify some of the ambiguities in the definitions and usage of safety instrumented systems (SISs) and turbomachinery control systems (TCSs) and to have a discussion about various approaches to SIS and TCS implementation.

Over the last 15 years, requirements based on IEC61508 specifications have gained acceptance within a large portion of the turbomachinery controls market. IEC61508 andIEC61511 (TABLE 1) provide common methodology for equipment manufacturers, control system vendors, engineering companies and end users. In the past, many machinery protection functions directly related to the unit were incorporated within the TCS. To reduce risk today, those functions deemed a safety hazard are separated in some manner from the control functions. Safety functions must also be certified to the appropriate safety integrity level (SIL). The required SIL rating of the SIS is based on the tolerable risk criteria, as defined by the plant operator. In the SIL calculations, the equipment under control (EUC) risk is compared to the tolerable risk. EUC may include the control system and instrumentation. IEC61508 quantifies SIS risk (FIG. 1) in terms of probability of failure on demand (PFD). If the EUC risk is above the tolerable risk, then an SIS is required. The required average PFD of the SIS translates into the risk reduction factor, which is necessary for bringing the EUC calculated risk below the tolerable risk. A given SIL rating guarantees a certain PFD level. Typically, turbomachinery safety functions are SIL 2 or SIL 3.

Deconstructing peril

The risk analysis covers not just the microprocessor-based controller (logic solver), but the entire system, including the transmitters and actuators. The PFD analysis of the logic solver includes software as well as the hardware. The SIL system rating is equal to the lowest rating of its components. Purchasing a controller that has a certain SIL rating does not guarantee that the entire SIS has the same SIL rating. In fact, most SIS failures (FIG. 2) are due to field instrumentation, not the logic solver. On another note, SIL rating may be a testament to the rigorous design practices used in building the controller. However, it may not mean that a SIL- rated controller is more reliable than a non-SIL controller. The control system availability is not equivalent to the PFD.

Besides the equipment design, the control hardware and the instrumentation, there are two main methods for reducing risk. The first is the separation of the safety and non-safety functions; the second is redundancy. In terms of the software, TCS may be a complex system, consisting of multiple proportional-integral-derivative (PID) loops, signal selectors and complicated logic. It may be difficult to predict and validate all of the interactions between various control, monitoring and protection functions. It is much easier to separate the safety functions and to analyze and validate them separately. Therefore, the logic solver, which is a part of the SIS, should contain simple code that can be easily validated. Moreover, the code should require minimal adjustments throughout the lifetime of the system, as SISs should have rigorous lifecycle management procedures, limiting the access to the logic solver's code and parameters. In terms of hardware, the common mode failures between the safety and non-safety functions must be minimized. This means that SISs and TCSs should have separate power supplies, I/O modules, communication buses and processors. An exception to this under IEC61508 would be if it can be shown that a sufficient level of

independence exists between safety and non-safety functions.

TABLE 1. IEC 61508 and IEC 61511 standards[1]

IEC 61508	IEC 61511
Generic safety standard for broad range of applications	Sector-specific safety standard for the process industries
Applies to all safety-related systems and external risk reduction facilities	Applies only to safety-instrumented systems
Primarily for manufacturers and suppliers of safety systems and devices	Primarily for system designers, integrators and safety system users and devices

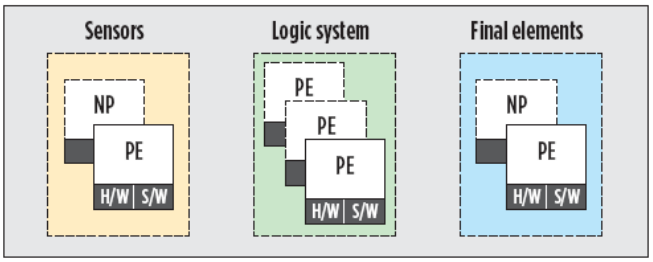


Fig.1-SIS components as shown in IEC 61508

Function vs. function

The separation of the safety and non-safety functions can increase the implementation complexity and cost. Implementation complexity increases in part because, in many cases, the signals that are used in the TCS for various logic and sequencing tasks are also used in the SIS for safety functions. Therefore, the overall system either requires redundant transducers or stipulates that TCSs and SISs must share I/O, without violating the separation principle. To avoid such complications, some vendors offer integrated TCSs and SISs, which have the appropriate SIL ratings. These systems provide a certifiable separation level between safety and non- safety functions without using separate hardware.

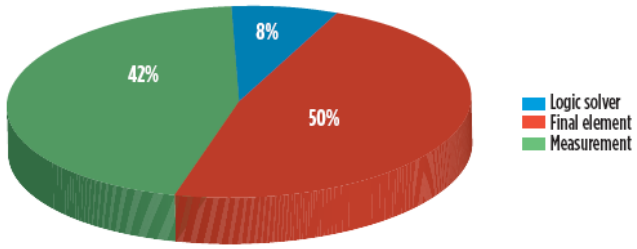


Fig. 2 - Main causes of SIS failure[1]

Consequently, in terms of software, an integrated system may contain safety and non-safety parts, with the TCS software running in the non-safety part of the system. If TCS is running in the SIL- rated safety portion of the system, then the overall control software (which may include turbine, generator or compressor control) must undergo safety analysis and limitations must be imposed on any modifications. This includes parameter changes, so that compliance is kept with the appropriate SIL. Thus, it may be difficult to adjust such a system to match the varying process requirements and to support and maintain it over its lifetime.

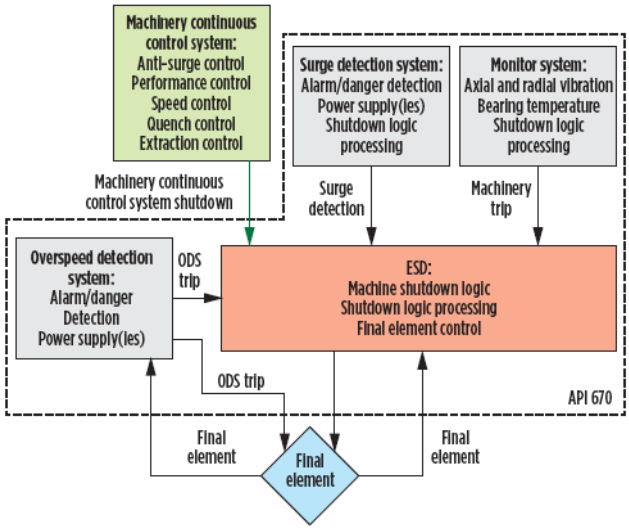


Fig. 3 - Distributed API670 architecture for the MPS[2]

In general, TCSs and SISs have different objectives. TCSs should provide for reliable unit operation and improve process reliability. It is vital to have a TCS running the unit for as long as is safely possible. This may imply sophisticated control algorithms being able to operate the unit even with some input signals in a failed condition or involve load sharing between compressors. Still, the job of the SIS is to safely shut down the unit and prevent catastrophic failure. SIS reliability is inversely proportional to its complexity: in most cases, the simpler the shutdown algorithm, the more reliable its functionality. While a TCS may require adjustments during com- mission and throughout its lifetime (as the process conditions may change), changes are strongly discouraged for the SIS.

The design and capabilities of the TCS may affect the required SIL of the SIS. A well-designed TCS may reduce the risk associated with operating the unit. For example, the function of preventing discharge pressure from exceeding the structural piping limitations may be included in the SIS due to the potential safety hazard. The risk may be reduced by building in provisions in the TCS for preventing the pressure rise by several means, such as reducing turbine speed and opening appropriate valves. A TCS may be well suited for the task, as it may already be carrying out related functions and, therefore, be capable of a fast response.

Redundancy is often employed by SIS vendors to reduce the PFD while maintaining high availability. Most of SIS redundancy is either triple modular redundancy (TMR) or dual redundancy. TCSs for critical units must also have very high availability numbers, which are not achievable without using redundancy. TCSs use essentially the same technology for redundancy. However, for SIL certification purposes, SIS design process must undergo a greater level of scrutiny. Also, the required diagnostic coverage for SISs may be larger than for TCSs. While the increased coverage reduces PFD, it may also result in larger overhead and increase software execution cycle time. While the plant is running in steady state, the TCS execution time may be less of an issue, but, during upsets, a fast response may prevent unit shutdown.

Blending standards

The 5th edition of the API Machinery Protection Standard API670 provides detailed guidelines on the implementation of the machinery protection systems (MPSs), taking into account IEC61508 and IEC61511. The standard covers the minimum requirements for an MPS. Basically, the standard divides MPS functions into several categories, which are vibration monitoring, overspeed detection, surge detection and emergency shutdown systems (ESDs). As defined in the standard, “the function of the ESD is to act as the logic solver that consolidates all shutdown commands to ensure proper timing and sequencing for a safe shutdown.” Relative to turbomachinery systems, an MPS measures:

- Radial shaft vibration
- Casing vibration
- Shaft axial position
- Shaft rotational speed
- Overspeed
- Compressor parameters (such as flow, pressure and temperature)
- Critical machinery temperatures.

The MPS functions architecture can be distributed (FIG. 3) or integrated (FIG. 4), with the distributed architecture being the default case. The compliance to IEC61508 and IEC61511, including SILs, is mentioned only regarding the ESD system (specifically, that the ESD system should have all the attributes of an SIS). However, there is a growing trend for requiring certification to the applicable SIL for all MPS components. By using the definition of the SIS, all components of an integrated system should then be SIL rated. While vibration monitoring and overspeed protection have been part of machinery protection in the past, surge detection—independent from the antisurge control—has been added for the first time. The standard mandates an independent surge detection system for axial compressors and advocates such systems for centrifugal compressors, particularly in cases of high pressure ratios or power density. However, as mentioned previously, there are no requirements for the surge detection system to comply with IEC61508. Whether surge detection should have a certain SIL depends on the risk analysis of the consequences of surge for each particular application.

Per the definition of a SIS, it is not only the ESD system that must comply with the required SIL, but also the entire sys- tem, including sensors and actuating elements. Therefore, PFD analysis should be carried out for the entire system to ensure SIL compliance. ESD system certification is not a sufficient condition for SIL compliance.

Function segregation is one of the main MPS principles. The protection functions are segregated from each other (and from the control system) in both distributed and integrated approaches. The intent of the standard is for an MPS to be physically separated from the control system, eliminating any common mode failures or interactions.

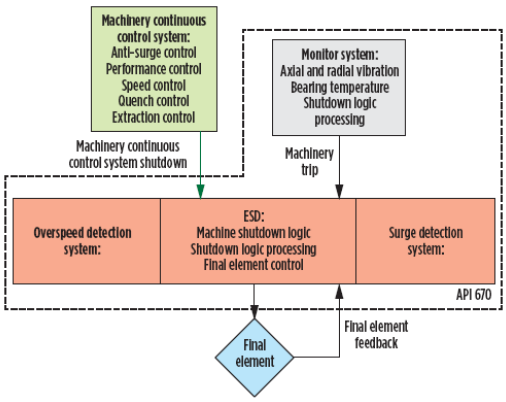


Fig. 4 - Integrated API670 architecture for the MPS[2]

The IEC61508 standard has added rigor to the risk assessment and considerations for selecting SISs. The standard's wide acceptance provides common ground for control equipment vendors and end users to select the right SIS for the application. The SIL analysis is greatly simplified through separation of the safety and control systems. Even without considering the IEC61508 standard, it has long been understood in the industry that, as far as safety is concerned, simplicity is synonymous with reliability. Thus, it is possible that extending requirements for SIL certification to control systems may be detrimental to both safety and control systems. In general, the complexity of the control system may be justified by its superior performance. However, this very complexity may make it difficult to achieve SIL certification. Putting TMC software applications into SIL-capable hardware does not automatically make the entire system SIL rated—unless the software is included in the PFD analysis of the overall system. Software applications with extensive functionality and flexibility can significantly increase the difficulties for PFD analysis and actually lower the achievable SIL. The 5th edition of API670, drawing from industry experience, mandates control and protection system segregation and provides guidelines for implementing machinery protection.

Summation

It is crucial to realize that SIL rating is not synonymous with higher levels of availability. Proper use of redundancy, diagnostic coverage and control algorithms allow non- SIL rated control systems to achieve similar availability levels to SIL-rated systems.

Literature Cited

[1] ARC White Paper, ARC Advisory Group, 2004.
[2] American Petroleum Institute Standard 670, 5th Edition, Machinery Protection Systems.

About The Author:

Serge Staroselsky is the chief technology officer (CTO) at CCC Global. He began his career with CCC in 1987 as a field engineer and has held various roles in project engineering and control systems design. Mr. Staroselsky also spent nine years at GE working on compressor and turbine control systems. He earned a BS degree from the University of California at Berkley, and MS degree in mechanical engineering from the University of Minnesota.

Wayne Jacobson is global technology manager for Compressor Controls in Des Moines, Iowa. He joined the company in 1996 as a systems engineer. He has a degree in mechanical engineering. His responsibilities include providing technical guidance and support, developing control applications, maintaining standard engineering and overseeing the overall technical development of the company's engineering staff.

Jeff McWhirter, P.E., is Compressor Controls' Gulf Coast manager. He has 30 years of experience with turbomachinery controls in a variety of industry segments, including natural gas, ethylene and ammonia. He is involved with the new MPS API 670 5th edition. He received an engineering degree from Texas A&M University.

Compressor Controls Corporation
4745 121st Street
Des Moines, IA 50323-2316 USA
+1-515-270-0857
process.honeywell.com/us/en/ccc
dl-ccc-solutions@honeywell.com