Integrating an IEC61508/11-compliant Safety System with a DCS

Michiel Bloemen (*), Massimiliano Veronesi (**)

(*) Product Manager ProSafe-RS Safety System,
Yokogawa Europe BV, Databankweg, Ameersfort, NL
michiel.bloemen@nl.yokogawa.com

(**) Product Manager Process Automation Systems and solutions
Yokogawa Italy, Vicolo D. Pantaleoni 4 20161 Milano
max.veronesi@it.yokogawa.com

Abstract – The need to ensure safety and prevent industrial accidents - and to limit the impact of any that do occur – focuses considerable attention on safety instrumented systems and the way they are applied. A key issue is the segregation of the safety system and the control system. On the one hand, safety standards require a high degree of separation between the two: on the other, users demand the benefits of improved ergonomics, lower costs, and better information management that only integrated systems can deliver. The development of the ProSafe-RS Safety System demonstrates that it is possible for manufacturers to reconcile the apparently conflicting demands of international standards and user needs. In this article, we will discuss the main points of IEC61508 and IEC 61511, and show how Yokogawa has ensured that ProSafe-RS meets these standards' requirements within an integrated safety system.

I. INTRODUCTION TO IEC61508-511

Recent industrial and railway accidents happening right before our eyes serve as a painful reminder that safety will always be paramount. Manufacturers and their customers agree - it's 'safety first', with no argument, and today we call on range of good technologies and sound techniques to ensure the safe operation of industrial processes.

But there's another issue: safe operation may be the priority, but today's users are also looking for better usability, lower costs, and improved ergonomics alongside safe operation. These all depend on a high degree of integration between safety systems and control systems. And that brings them into apparent conflict with the requirements of the major safety standards, which stipulate that safety and control functionality should be segregated.

Before looking at how Yokogawa has addressed the issue of reconciling the demands of the standards with those of its customers, it is useful to first outline the requirements of the relevant international standards, both to understand why there may be a potential conflict here, and to clarify some of the terminology.

The IEC 61508 and IEC 61511 standards set out a policy of deciding on quantitative goals for risk reduction, and for realizing those goals in practice. The approach is based on the idea that safety is “absence of intolerable risks”; so quantitative goals for risk reduction are clearly defined.

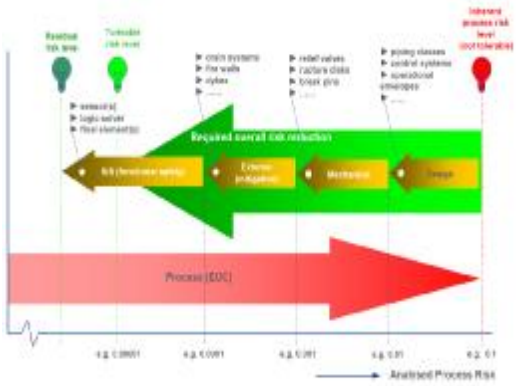

Figure 1. Risk reduction approach

IEC61508 applies to any safety application using an electrical circuit, electronic circuit, or a programmable electronic system (E/E/PES:

Electrical/Electronic/Programmable Electronic System). In 2003, IEC61511 (Functional safety: Safety Instrumented System for the process industry sector) was published under the umbrella of IEC61508 for process industries which employ this standard most frequently.

The term “Safety Instrumented System” or SIS is applied to emergency shutdown systems and fire and gas protection systems in industrial plants. When a process – and that includes the control system for that process – deviates from normal operation, the SIS serves to prevent the occurrence of a hazardous event.

An SIS consists of sensors to detect process abnormalities, logic solvers to conduct preset algorithms using information from sensors, and actuators such as shutdown valves. The standards state that the safety instrumented system must be separated from the control system - so, for example, shared or common sensors must NOT be used.

IEC61508 and IEC 61511 define a quantitative index for risk reduction and specify the management of safety related systems through their lifecycle. (Methods for risk analysis are not pre-defined, and so a range of techniques such as a Hazard and Operability or HAZOP studycan be used.)

TABLE I. SAFETY INTEGRITY LEVELS

Safety integrity level (SIL)	Low demand mode (PFD)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

The safety integrity requirement is a requested specification in which the extent of risk reduction in a plant is quantified. The risk is represented by multiplying the consequence of harm by the frequency of the occurrence of the hazard: the function of the SIS is to reduce the frequency of the occurrence of that hazard.

The term “safety” - as applied to safety systems - means the level of accuracy at which plant shutdown is performed when a problem occurs. It includes the characteristic that safety systems will behave toward the fail-safe side - i.e. plant shutdown - even if they themselves fail. In contrast, "availability" refers to the probability of a plant being shut down due to a failure in a safety system (so for high availability, the error trip rate must be low).

The Safety Integrity Level (SIL) was introduced as a method for expressing the safety integrity requirement. It is classified into four levels (SIL1 to SIL4) as shown in Table 1. A measure for the safety integrity level in the low demand mode is Probability of Failure on Demand (PFD). PFD is the probability that the safety instrumented system will not operate due to a failure when actuation of the system is requested. So the lower the probability, the higher the safety integrity level.

The target safety integrity must be specified for each safety instrumented function (SIF) separately, and sensors, logic solver, valves and all other devices in the safety function must be included (see figure 2).

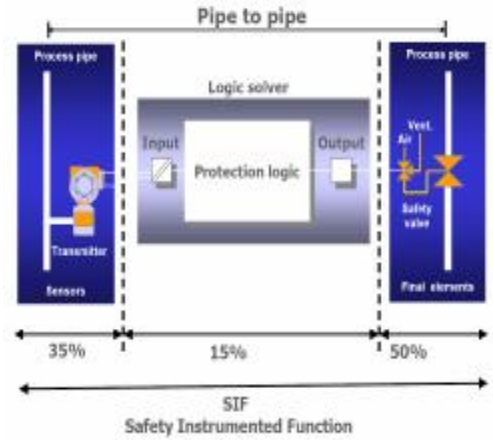

Figure 2. Pipe-to-pipe approach

The “failure rate” (l) is not really a “probability” but it’s rather defined as “the number of times that a component fails during a specific time interval”. Basing on the fact that what is important is the “dangerous-undetected” fraction, the PFD at time t (after 1st run) is evaluated as:

$$PFD(t) = 1 - e^{-l_{DU}t}$$

So, higher is l_{DU} and faster the PFD will approach to 1.

Basing on the definition of safety instrumented system given above, it is worth stressing that the total PFD has to be evaluated as

PFD (sis) = PFD (sensor) + PFD (safety system) + PFD(actuator)

Then the average-PFD can be calculated as

$$PFD_{AVG} = \frac{1}{T} \cdot \int_0^T PFD(t)dt$$

The standard requires a response to “random hardware failures” of the components used in equipment and preparation of preventive measures for “systematic failures” named in the standard, such as improper specification, design, and operation of equipment.

Figure 3. The failure rate classification

In the case of control systems, hardware failures are treated by classifying them into the part where failures can be detected through self-diagnosis and the part where failures cannot be detected through self-diagnosis. Each failures can be a ‘safe failure’ (the output is conducted in the direction in which the plant is shut down or there is no impact) or a ‘dangerous failure’ (the output function to shut down the plant is lost). Further, failures are classified into detected safe failures, undetected safe failures, detected dangerous failures and undetected dangerous failures (see fig.3). The problem is the treatment of undetected dangerous failures. Since this type of failure cannot be detected by self-diagnosis, it can be detected only by the operation test (proof test) carried out during regular inspections. The aim of inspections and maintenance is to reduce periodically the PFD in such a way the SIL3 can be achieved for a long time (see figure 4).

The safety standards (IEC61508, part 3) require detailed specifications to be drawn up, to avoid any misunderstandings: the manufacturer must then design the system in accordance with those specifications, using properly managed design tools, to verify competent module levels and system levels planned in the pre-design stage.

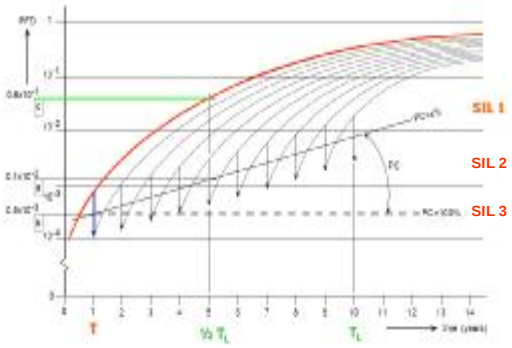

Figure 4. the PFD trend

Management must be rigorous, and including impact analysis for design changes, and demonstrate a structure which can prevent systematic failures.

The safety standards also require the application of a Functional Safety Management system to assure that all safety related activities are planned, executed and documented. Our own FSM, certified by TÜV Rhineland as compliant with the requirements of the IEC standards, serves as a good example:

- All relevant working procedures, work instructions, tools, template documents and checklists are in accordance with the requirements from the standards.
- For each safety project a Safety Validation Plan is made.
- The architecture of the safety related systems complies with IEC 61508 and/or IEC 61511.
- Reliability calculations are performed to confirm the achieved Safety Integrity Level (SIL).
- Review- and test-checklists contain safety related checks.
- Functional safety assessment and validation is executed by an independent group.
- Periodical functional safety audits are also executed by an independent group.
- Personnel are trained and re-trained to achieve and maintain the required level of competence for functional safety.

IEC 61508 and IEC 61511 state that the SIS must be separated from the control system (DCS). But the same standards also allow that, under specific conditions, parts of the SIS and the DCS may be shared.

IEC 61508 commands separation and independence between the SIS (or any protection layer) and the process. The focus here is on the execution of safety functions, and the possibility (or otherwise) of effecting them.

Then the standard also uses the phrases: "wherever practical" and "sufficient independence". This is completely in line with the spirit of the standard, which is performance driven – it accepts that the risk can never be reduced to zero, and that absolute separation is not achievable.
When looking at table B.6 (which is mandatory) the standard advises separate physical locations for high effectiveness. How should we interpret this? When we assume that high effectiveness must be used for SIL3 SIFs, for example, is it permissable to include a part of your SIF in the same rack as parts of your control system that are safeguarded by this SIF? Is it permissable to share the same cabinet?
IEC 61508 does not specify, but it is clear that using separate racks for SIS and DCS is (much!) better than mixing modules in one rack.
IEC 61511 takes a somewhat different approach: it recognizes so-called "layers of protection", with the SIS being one of these layers. But it allows the DCS to be considered as another layer of protection. However, the DCS as a layer of protection has an important limitation: the risk reduction is less than 10, which implies that one cannot even claim SIL1 capabilities for the DCS.

When claiming risk reduction as a function of the DCS, one has to consider the following, according to the IEC 61511, part 2, 9.4 :

- reliability analysis of the DCS
- procedures for configuration, modification, operation and maintenance
- access security
- change management

This implies that, although the full requirements of the IEC 61511 are not applicable for such a part of the DCS, many additional measures have to be taken, compared to an ordinary control system. In other words, you must treat this part of your control system differently from the rest of your control system. How can you organize that in practice?

IEC 61511 also requires (clause 9.5) that the layers of protection are independent from each other. The standard also states that this independence must be checked carefully - not that easy, especially when devices are shared between layers.

The safety system “ProSafe-RS” recently developed by Yokogawa Electric Corporation is certified by the third party body TÜV that its responses to both random hardware failures and systematic failures described above comply with the standard IEC61508.

II. INTEGRATION BETWEEN DCS AND SAFETY SYSTEM

Yokogawa has an extensive safety pedigree - our ProSafe-SLS is synonymous with the solid-state safety systems first developed in the 1960s, for example, and is still used in projects with the highest (SIL4) requirements up to SIL4, and our EJX pressure transmitter is recognized by TÜV as fit for use in SIL2/3 as standard. For safety PLCs, SIL3 has been defined as the highest level in accordance with international functional safety standards.

In integrating a DCS and a Safety System different issues have to be considered. From one side, in fact, IEC regulations requires separation, segregation and fail safe operation. On the other hand, the common criteria for plant control optimization need integration, ergonomic and availability (fault tolerant).

One solution is represented by integrating the Logic Solver as a sub-system of the DCS, as shown in figure 5. In this case some severe drawbacks arise, such as:

- different networks are used, so additional communication modules are required
- HW diagnostic is not built-in so it requires additional engineering work
- heavy engineering work (driver communication, alarm management, …)
- no integrated Sequence Of Events

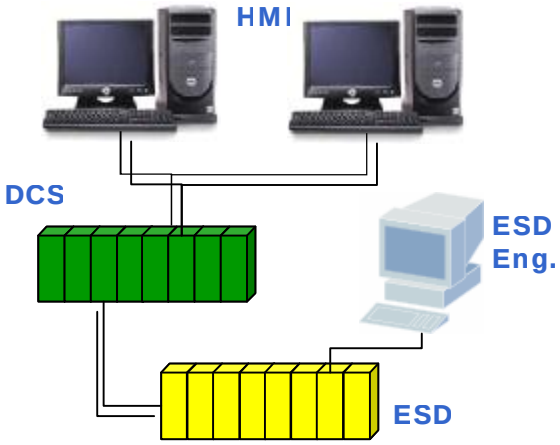

Fig. 5 – ESD as a subsystem of the DCS

A second suitable solution is shown in figure 6. it is based on the OPC technology, actually widely used in the process automation. The situation is a little bit better but the following items have to be considered:

- a redundant OPC server has to be included in the system architecture
- data coming from the Logic Solver can be imported in the HMI, but not always are available for the DCS controllers
- additional engineering work is needed (OPC)
- HW diagnostic is not built-in so it requires additional engineering work
- The functionality of DCS tags and OPC tags are usually different

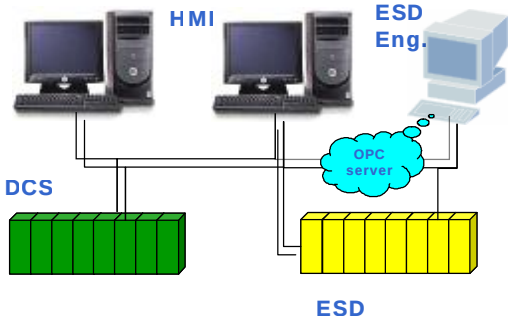

Fig. 6 – ESD in the OPC network

The really integrated solution is shown in figure 7. Here the Logic Solver is one node of the system network as well as each DCS controller. The clear benefits of this solution are the following:

- One redundant high-speed network
- Full built-in diagnostic
- No additional engineering for data exchange
- Integrated alarm list and SOE
- One single gateway to the PIMS/MES level

It is clear that the latest solution can be provided only from vendors able to provide both DCS and Safety System.

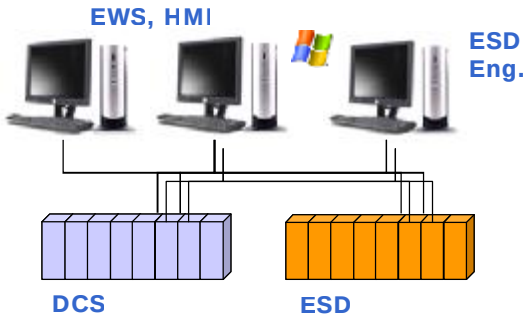

Fig. 7 – ESD in the system network

ProSafe-RS is a new safety system, based on the field-proven concept of the Yokogawa DCS. Its key features include:

• Fit for use in SIL3 level with single modules

• High availability in a single and redundant configuration (CPU, PWS, I/O)

• Integration with DCS

• IEC 61131-3-compliant engineering tools

Figure 8 shows an example of an integrated configuration of the ProSafe-RS safety system and the CENTUM CS 3000 production control system. In the ProSafe-RS, the safety engineering PC (SENG) and safety control station (SCS) are connected directly using a V net control bus. The SENG is a PC on which software having engineering functions and maintenance functions runs. The SCS is a safety controller that performs logical operations such as shutdown by downloading application(s) created on the SENG.

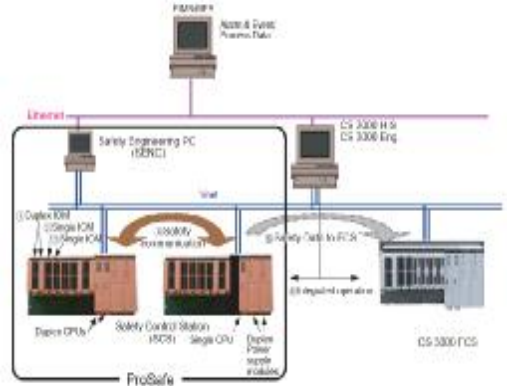

Figure 8. Integrated ESD+DCS solution

The key to this unified DCS-SIS architecture is a highly robust protocol which was developed specifically to support safety-related communications on a common DCS data highway. This protocol segregates DCS and SIS communications logically, to ensure the integrity of ProSafe-RS safety communications on the shared Vnet - which already implements dual-redundancy for non-stop reliability of the DCS.

Using a common bus simplifies system building and interface design, thus significantly improving total engineering efficiency - including the design and installation costs of system building and interfaces.

The function of an SIS is to shut down a plant safely if a problem occurs that neither the DCS nor human operators can handle – so by definition, cases where SIS operation or monitoring is required are very rare.

So, if the SIS and DCS can be operated and monitored using the same HMI, operators do not have to remember the operations of two HMIs. When necessary, operators can take any action required using the HMI of the DCS they are familiar with.

In addition, having the same interface to the MES domain for the DCS and SIS provides a platform offering an integrated solution with virtually no distinction with regard to:

- OPC data to the PIMS/MES level
- Alarms management and optimization
- Sequence of events archiving and analysis

As noted earlier, international safety standards require the DCS and SIS to be segregated in order to protect the function of safety protective layers even if control functionality is lost.

For this reason, even if a Vnet bus failure occurs, safety diagnostics focusing on detecting the Vnet bus failure will protect the SCSs from communication attacks, or shut-down a safety loop configured by SCS-to-SCS connection. This means that any effects from the DCS via the Vnet do not cause a dangerous failure in the ProSafe-RS.
In other words, non-interference from the DCS to SIS is assured - the DCS *cannot* cause a loss of SIS safety functions.

ProSafe-RS incorporates a redundant matching mechanism and self-diagnostic mechanism in each I/O module and CPU module to comply with the SIL3 level defined in IEC 61508 by a single component. Both the CPU module and I/O modules can realize a safety loop meeting SIL3 in a single configuration. Because ProSafe-RS performs SIL3-level diagnosis in each module, no inter-CPU module comparison is made. This means that no error trip occurs unless two failures simultaneously occur in both CPU modules, making the system exceptionally reliable.

A key feature of the newly developed ProSafe-RS hardware is the application of dual microprocessor technology, not only on the CPU module, but also on I/O modules. This feature affords an SIL3 in a single configuration as well as in a redundant configuration. The processor module, I/O modules, power module, and communication buses can all be made redundant (see the architecture in figure 9).

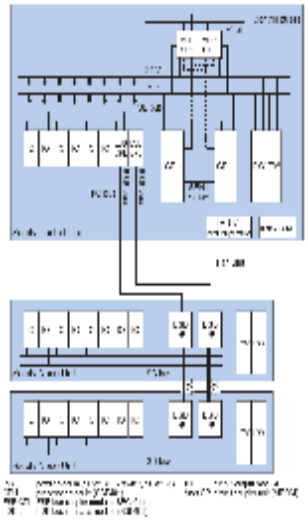

Figure 9 – The ProSafe-RS architetcture

To achieve a self diagnostic rate of 99% or above requires measures such as the use of two microprocessors (MPUs) to compare calculation results. ProSafe-RS processor modules employ a redundant - 'Pair & Spare' - matching method that has a proven record in the CENTUM (figure 10).

That means that each module contains a pair of MPUs to achieve SIL3 capability – a spare module may be used to achieve very high availability. In addition, we employ conversion of the I/O circuits to multi-system form, inter-system comparison, and activation diagnostics of the I/O circuits to achieve high self-diagnostic coverage. The comparators, main storage, groups of associated registers, watchdog timers and so on are made redundant, to eliminate any factors that might result in a common-cause failure.

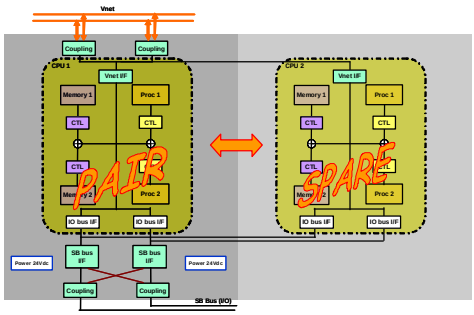

Figure 10 – The Pair-&-Spare concept

An input module consists of two MPUs, two input circuits per channel, and a diagnostic circuit to check the input circuits and peripheral circuits. Input signals from the field are fed to the two MPUs via the two independent input circuits. The MPUs check if data input to each MPU matches by mutual comparison, to assure the soundness of the input circuits and the MPUs themselves. When they agree with each other, the data is transmitted to the processor modules via the safety layers configured by the firmware. To avoid dangerous situations, the input channels are regulary and routinely activated to check for a 'stuck at' failure.

On the output side, an output module compares the results of the check between the MPUs. After verifying the soundness of the command, the module outputs an instruction value. The output value is read back by the two MPUs to check that it always agrees with the instruction value. Because an output signal also does not change unless a shutdown request occurs, the output channel circuit is periodically activated to check for a 'stuck at' failure in the output switches and read-back circuits. If an output switch is stuck ON and fails, the other switch arranged in series with that output switch is turned off. This allows the output to be forcibly shut off (Figure 11).

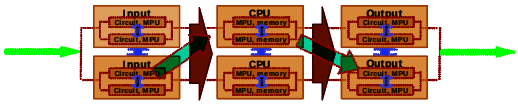

Figure 11 – The ProSafe-RS-high reliability

ProSafe-RS's compliance to SIL3 has been proved using a technique known as "failure modes effects and diagnostic analysis" or FMEDA. During FMEDA, the failure rate, failure mode, and effects caused by the failure of a component on all of the constituent components were analyzed. Among those failures found in these analyses, we quantitatively estimated the dangerous failure rate (λ_{DU}) that could not be detected by self-diagnostics, calculated the PFDavg value and verified that it was better then 1.5×10^{4}.

TÜV has certified that ProSafe-RS' responses to both random hardware failures and system failures comply with IEC61508.

ProSafe-RS engineering functions support languages compliant with the IEC 61131-3 international standard (Function Blocks Diagram – FBD and Ladder Diagram – LD).

ProSafe-RS 's ability to modify an application without stopping the safety controller, i.e., without shutting down the plant, has been officially certified. This safety engineering function reports modified areas and affected areas, which limits the testing time significantly.

In the CPU and I/O modules of the SCS, self-diagnostics are performed periodically by the hardware and software. Where modules are operated in a redundant configuration, should a failure occurs in one of the modules, the other continues to operate alone without interrupting the running process.

Safety communication is a communication method that incorporates a mechanism for

checking that safety-related data is passed to the communication counterpart, without fail, on an existing non-safety communication system. In safety communication, an additional safety layer is implemented in the place of the application layer to separate the safety functions from the outside, non-safe, world (see figure 12).

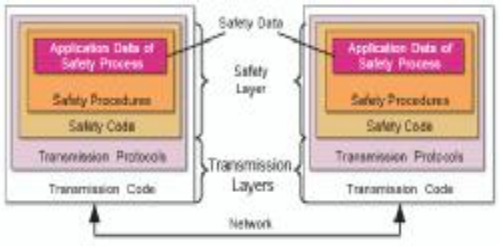

Figure 12 – Safety communication

To perform inter-SCS safety communication, dedicated function blocks (FB) are used to describe the safety logic. Problems that may occur in communication (such as data corruption, omission, or delay) are all checked by the consumer SCS FB. If a fault is detected, a pre-defined fail-safe value is output, and information identifying the faulty data and the cause of the fault are notified by an alarm.

To meet SIL3-level for a system having both safety and non-safety functions the validity of the safety functions and safety communication must be assured, and non-safety functions must not interfere with safety functions. The following summarizes the most important measures that Yokogawa has designed into ProSafe-RS to assure that the SIS will always execute its task correctly.

- Safety logic can be downloaded to the SCS only after checking whether user-created safety logic is properly and safely configured.
- CRC (cyclic redundancy check) codes are appended to individual files and operation data that are loaded from the SENG to SCS to check that the files or data are not corrupted on the SCS side.
- Software is monitored for a runaway using a watchdog timer (WDT). If a fault occurs, the output modules output a fail-safe value, shutting down the plant securely.
- The memory area used by the safety functions in the SCS is protected against being written from non-safety functions.
- The priority of executing a safety functions is set to a higher level than that of the non-safety functions in the SCS. Thus, even if a non-safety function enters an endless loop, the safety functions can be securely executed every scan period.
- In the SCS, the processing time of Vnet communication made per scan period is measured to perform control such that the processing time does not exceed the upper limit of a set processing time. Thus, even if a malicious communication attack on the SCS is made, the safety functions can be executed every scan period.
- At the operation level, the SCS does not accept operations that modify a safety function, such as off-line download, online change, or forcing (operation of fixing or changing safety logic data value(s) forcibly). To perform SCS maintenance, it is necessary to input a password that has kept in the SCS, to change the security level to the maintenance level.
- An override execution command from the HIS cannot be accepted unless the override FB is in the permission status. If the permission or execution status of the override FB changes, an alarm is reported from the SCS to the HIS, so that it is possible to check which override FB is operated and what condition it has entered. Override request data from the HIS to SCS is assigned a CRC code, and the validity of the data is checked by the SCS. Further an alarm is reported from the SCS to HIS if the override condition continues for more than a specified time.

One issue that the safety standards do not address specifically, is the human interface of a safety system, so no clear requirements can be found. That's perhaps not surprising, as the safety system should be independent from any human intervention. But the operator has to know the precise status of all safety signals, so the information from the SIS must be available to him.

Until recently, many organizations bought their safety system from a different supplier to the control system. There can of course be advantages in using diverse and discrete systems - the major drawback, is that information on the SIS status is also diverse and discrete.

This means that in daily operations an operator either has to look at two process MIMICs, behaving differently, or that he has only a limited view of the devices connected to the SIS. The alarms from the SIS might also deviate in their representation from those of the control system, and the formats of the SIS might be different from the information that the operator looks at all day on his control system. Worse still, they may be truly separate, on their own SIS monitor and SIS event recorder.

So when an abnormal situation occurs in the plant, the operator has to interpret diverse and / or separate information - something that does not support good, safe actions and decisions.

Of course the SIS sub-suppliers advertise "easy integration", but in practice good results are difficult to achieve, expensive, and difficult to maintain.

The data from the SIS may "integrated" in the control system via MODBUS or OPC, for example. MODBUS is simple and cheap, but the functionality is very limited. OPC is more powerful, but it is technically complex and requires detailed software configuration and maintenance. And at the end of the day, while the information from the SIS might appear on the same screens as the information from the control system, the format and the functionality will still be different. And an integrated shift report, reporting both BPCS and SIS issues, is very rare indeed.

These are worrying issues, given what we know from investigations into real life accidents about the many problems that are caused by incorrect human intervention.

We believe that in the interests of the smooth operation of the plant, data from the safety system and the control system should be exactly the same and seamlessly integrated. This will prevent mistakes when operators are under pressure, and for this reason we have put a great deal of effort in integrating the information from SIS and DCS - while keeping interfaces to the field separated**.**

For environmental resistance, the ProSafe- RS has met the requirements of IEC61131-2 (Programmable Controllers-Equipment requirements and test) in which test conditions stricter than general DCS are required, EN298 (burner management standards), and EN54-2 (fire protection and fire extinguishing system standards). Furthermore, the ProSafe-RS's corrosion resistance meets the G3 specifications of ANSI/ISA S71.04 as standard.

The operating ambient temperature of the safety control unit is from -20ºC to 50ºC as standard, but wider temperature-capable specifications that are equipped with cooling fans and can cope with a maximum of 70ºC are also available. Moreover, the IRIG-B (GPS connection) interface for realizing high-precision time-of-day synchronization between SCSs is also available as an option.

III. Conclusion

The ProSafe-RS from Yokogawa demonstrates that it is possible for a safety system to run on the same network as a DCS, while maintaining compliance with the requirements of the IEC 61508 standard in terms of design as well as segregation from the control system.

REFERENCES

IEC 61508/11

Akai Hajiime – “IEC61508 Compliant Safety System”, Yokogawa Technical Report N.ro 40, 2005

Nishida Jun, Matsuda Toshihiko – “Aims and features of the Prosafe-RS Safety System”, Yokogawa Technical Report N.ro 40, 2005

Sato Masahito, Kuwatani Motojiki – “System generation and maintenance functions for the Prosafe-RS Safety System”, Yokogawa Technical Report N.ro 40, 2005

Emori Toshiyuki, Kawakami Shigehito – “Safety technologies incorporated in the safety control station”, Yokogawa Technical Report N.ro 40, 2005

Y. Yasuhiko, S. Hiroyoshi, S. Ryoutarou, K. Yoshinori – “Hardware features of the Prosafe-RS”, Yokogawa Technical Report N.ro 40, 2005