TAKING THE CONTROL SYSTEM FOR GRANTED – ENSURING THE INTEGRITY OF SUB-SIL INSTRUMENTED FUNCTIONS[†1]

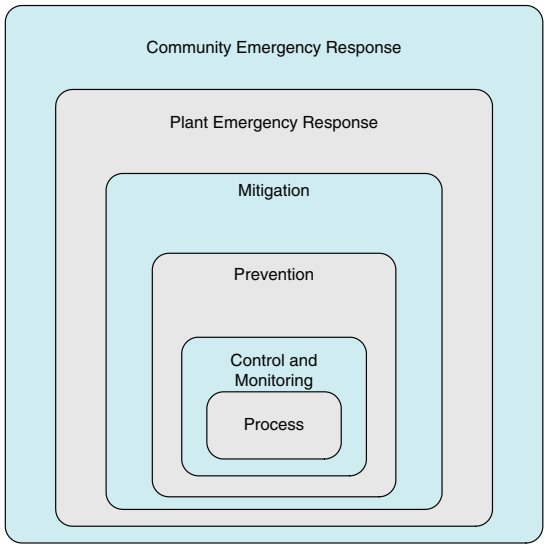
P. Lucas, J. Walkington and T. Atkinson
ABB Engineering Services

Most organisations are routinely claiming the maximum permitted contribution for non-safety (sub-SIL 1) Instrumented Functions during their SIL determination reviews. Similarly, claims for the reliability of the Basic Process Control System (BPCS) also impact on the calculation of safety requirements. Often these claims are made in terms of alarm system performance, operator response and control system availability. This paper will examine a cost-effective, qualitative methodology for demonstrating the risk reduction performance claim, both for new and legacy installations.

INTRODUCTION

Functional safety standard IEC61511 (IEC 2003) describes methods of hazard and risk assessment based on 'the allocation of safety functions to specific protection layers for the prevention, control or mitigation of hazards from the process and its associated equipment' (IEC, 2003: 9.2.1). These protection layers are shown in the following diagram, IEC61511, Part 1 Figure 9, shown below. These layers of protection are:

- Process – the use of inherent safety principles to remove hazards by design, for example reduced inventories, temperatures or pressures.
- Control and monitoring – control systems, process alarms and operator supervision. This layer is designed to maintain the process within its normal operating limits



- Prevention – process alarms with mandatory operator corrective actions, safety instrumented control systems and safety instrumented protective systems. These devices are designed to return the process to a safe state if it moves outside the normal operating limits.
- Mitigation – devices such as pressure relief valves or fire sprinklers that are designed to reduce the impact or consequence of the hazardous event.
- Plant Emergency Responses – fire alarms and toxic alerts leading to evacuation.
- Community Emergency Response – actions to be taken by the local community and local authorities.

Each of these layers provides some form of control, protection or mitigation from the effects of the process and the potential hazardous events that can arise from the process. The risk of any of these potentially hazardous events propagating to cause harm to people or the environment is reduced to some extent by each by these layers. This paper will concentrate on the contribution of the control system (termed Basic Process Control System, BPCS, in IEC61511) in providing an amount of risk reduction from the potentially hazardous event.

IEC61511 gives us some guidance as to the role of the BPCS in risk reduction. It states in Part 1, clause 9.4 that:

- Basic Process Control system may be identified as a protection layer
- The risk reduction factor claimed for the Basic Process Control System shall be less than 10.
- If a risk reduction factor of greater than 10 is claimed for the Basic Process Control System, then it shall be designed to the requirements of IEC61511 or IEC61508.

IEC61511 further states in Part 1, clause 8.2.2 that:

- The dangerous failure rate of a BPCS (which does not conform to IEC61511) that places a demand on a protection layer shall not be assumed to be better than 10^{-5} per hour.

These instrumented functions and alarms are not Safety Instrumented Functions, and are not designed to achieve a Safety Integrity Level (SIL); however they do

#	1	2	3	4		5		6	7	8	9	10	11
					PROTECTION LAYERS								
	Impact event description F.3 F.14.1	Severity level F.4 F.14.1	Initiating cause F.5 F.14.2	Initiation likelihood F.6 F.14.3	General process design F.14.4	BPCS F.14.5	Alarms, etc. F.14.6	Additional mitigation, restricted access,F.8 F.14.7	IPL additional mitigation dikes, pressure relief F.9 F.14.8	Inter-mediate event likelihood F.10 F.14.9	SIF integrity level F.11 F.14.10	Mitigated event likelihood F.12 F.14.10	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0,1	0,1	0,1	0,1	0,1	PRV 01	10^{-7}	10^{-2}	10^{-9}	High pressure causes column rupture
2	Fire from distillation column rupture	S	Steam control loop failure	0,1	0,1		0,1	01	PRV 01	10^{-6}	10^{-2}	10^{-8}	Same as above
N													

IEC 3025/02

NOTE Severity Level E = Extensive; S = Serious; M = Minor.
Likelihood values are events per year, other numerical values are probabilities of failure on demand average.

Figure 1. Layer of Protection]Analysis (LOAP) report

provide a contribution to the total risk reduction strategy. Some companies have termed these functions 'SIL 0' or 'SIL a' to indicate that the desired performance is below SIL 1, but require attention above that of a general instrumented function. ABB ES have used the term 'Sub-SIL' for these functions.

So what does this mean in practice? To evaluate the contribution made by each of the protective layers to the total risk reduction required to meet the tolerable risk for a specific hazardous event and determine the target Safety Integrity level (SIL) of the Safety Instrumented Function, a process analysis tool called Layer of Protection Analysis (LOPA) is increasingly used. A detailed description of this methodology can be found in Layer of Protection Analysis: Simplified Process Risk Assessment (CCPS, 2001), however a simplified example SIL Determination exercise using LOPA is given in IEC61511, Part 3 Annex F and we will use this example to illustrate the risk reduction contribution of these 'Sub-SIL' instrumented functions.

In this case it can be seen that the risk reduction claimed by the BPCS is a factor of 10 (0.1) and the risk reduction claimed by Alarms is also a factor of 10 (0.1).

At this stage, we should clarify what constitutes the BPCS. It is not just the DCS/ SCADA/ PLC logic solver. It is the complete end to end, sensor to actuator, instrumented function that changes the state of the process. Similarly for the alarm, the risk reduction is provided by the sensor, the logic solver, the alarm indicator and the human responding to the alarm.

In the example above, and in our experience of a wide number of SIL Determination studies from a number of sectors, this claim of a risk reduction factor of 10 is made almost as a default value. Remember that the IEC61511 guidance is that the risk reduction factor claimed for the BPCS shall be less than 10, so this implies that to claim a risk reduction of the upper limit of 10, the BPCS has been specified, designed, installed, commissioned, operated, maintained, modified and managed at a high level.

WHAT AFFECTS THE BPCS PERFORMANCE?

What factors affect the performance of the BPCS in delivering control and alarms to this level of risk reduction? What requirements are there for a Sub-SIL instrumented function or alarm?

For the BPCS, IEC61511 Part 2, Clause 9.4 mentions . . .

- Any claim for risk reduction should be justified by the consideration of the integrity of the BPCS
- . . . and the procedures used for configuration, modification, operation and maintenance
- . . . important to ensure that access security and change management are provided.

HSE guidance provided in the Technical Measures Document for Control Systems (HSE 2008) advises that:

- The control system should be sufficiently independent of the safety systems.
- Consider all expected normal and upset modes of operation, including start up and shut down.
- The dangerous failure modes of the control system should be determined
  - This should include the analysis of I/O, power and communications failure
- Consideration should be given to change control and backup systems
- Consideration of survivability during hazardous events and emergency responses

For the alarms, IEC61511, Part 2 Clause 8.2.1 mentions that:

- Human factors must be carefully considered
- Claims for risk reduction should be supported by a documented description of the operator response, that there is sufficient time for the operator to take corrective action and assurance that the operator will be trained to take the protective actions

The HSE guidance references the EEMUA 191 (EEMUA 2007) guidelines for best practice in alarm handling.

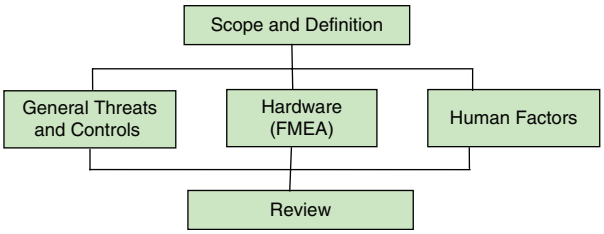
ABB Engineering Services use a form of a Computer Hazard and Operability (CHAZOP) process based on a set of structured reviews to gain assurance that all issues raised in available guidance are analysed, addressed and documented.

THE CHAZOP PROCESS

There are several forms of CHAZOP documented in literature, most of them based upon the guideword driven Hazop process (for example Andow 1991 and Kletz 1995). The ABB ES version is derived from the early work done by ICI (Nimmo 1997), and evolved in the intervening years into a set of structured reviews providing a qualitative process based on standards, guidance, learning, improvement and experience. This is a time efficient method that is designed to give confidence that instrumented functions and alarms in the BPCS have been designed, installed, operated and maintained using current good practice and can be considered to be performing at the high end of the allowable range.

The process consists of three main reviews covering general threats, hardware and human factors.

The CHAZOP reviews are team based activities, led by an experienced facilitator and comprising of operations, process, control and systems representatives. The reviews can be performed at different stages of the lifecycle; during the design phase to improve the design, after the design phase to verify the design, during the operational phase to understand the impact of modifications and before the replacement or upgrade of a system.



The General Threats and Controls review is based on experience of previous failings of control systems and consider issues such as:

- The effect of external influences such as heat, humidity, lightening, static, dust, contamination, heating, cooling, fire and smoke detection.
- The effect of power supply distribution and failures, including the use of UPS's, volatile memory and failsafe position of equipment on power failure.
- Security and access issues including physical access, remote access and authorisation levels.
- Service and maintainability including time to repair/replace equipment, level of spares holdings, ability to service or repair legacy equipment, access to settings or software that needs to be loaded onto equipment and procedures/controls in place to ensure necessary checks performed before repaired or spare equipment brought into use.
- Disaster recovery/contingency planning including availability of spares, backups of data, recovery plan and trial runs of restoring equipment and settings.
- Modification including assessing the process, documentation and approvals.

The detection, indication, required actions and repair to each of these potential threats is identified, assessed and documented.

The Hardware review utilises a Failure Mode and Effect Analysis (FMEA) to assess credible failure modes and their effect on information flow. The study is aimed at functional module failure rather than component level, for example failures of I/O boards, controllers, communication modules, operator stations and historians.

For each module, relevant failure modes are suggested and the effect of any data loss investigated. For each I/O signal used for risk reduction, the different failure modes (for example low, high, drifting and bad signal) for the signal are considered. The detection, response and recovery action to each failure is discussed and recorded. The process enables the team to logically break down problems, discuss solutions and document results. It is especially useful in assessing the level of redundancy required and investigating independence between control, alarm and safety functions.

Unlike the Safety Instrumented System, where safety responses are defined and unambiguous, the BPCS performance is often critically dependent on both the BPCS and the associated operator(s). Diagnosis of process conditions and faults, response to alarms and operator performance during high risk activities (such as unit start-up) all require the 'human element'. It follows that the BPCS should support the operator in all process modes; normal, planned abnormal (such as process maintenance and start-up/ shutdown) and unplanned abnormal (major process incident). Elements that are examined during this CHAZOP review and assessed for effectiveness include:

- Consistency of presentation
- Design of graphics
- Design for operating modes
- Alignment with procedures
- Operator Training and competence

Process alarms are particularly important in the effectiveness of the BPCS. In addition to the need for process alarms to inform and guide the operator in all modes of operation, the alarm is often claimed as a Layer of Protection contributing a factor of 0.1 to the overall risk reduction. It is important that the alarm system itself is performing to good engineering practice standards, such as those specified in the EEMUA 191 guide. The CHAZOP process looks at the requirement for alarms, their claimed contribution to overall risk reduction and the design and operational controls in place to ensure that best possible performance is achieved, typically including:

- The requirement for alarms. Number, priority, required response from the operator and time to respond. Criticality of alarms and consequence of inappropriate response
- Design of the alarm system
- Measurement of alarm system performance
- Management of the Alarm System throughout the operational lifecycle. This includes risk management (temporary defeat, change management) as well as nuisance alarm reduction and overall performance management.

CONCLUSIONS

The CHAZOP process is based upon learning from previous incidents involving BPCS failures and is a team based methodology utilising structured reviews to examine potential threats to the claimed performance of the BPCS. The structure of the reviews and use of an experienced leader ensure a cost effective approach to enable the process plant owner to analyse the BPCS and provide documented assurance to themselves and the regulators that:

- The hardware architecture has sufficient redundancy, separation and independence to achieve the claimed performance
- Support systems are in place to reduce downtime, enable prompt recovery and re-build following equipment failures and that the BPCS is resilient to environmental threats and secure from unauthorised operations.
- The claimed performance of operations and maintenance staff is achievable with respect to human factor constraints.

REFERENCES

Andow, 1991. Guidance on Hazop procedures for Computer Controlled Plants, HSE contract research report No. 26/ 1991, P. Andow, Her Majesty's Stationary Office, 1991.

CCPS, 2001. Layer of Protection analysis: Simplified Process Risk Assessment, Centre for Chemical Process Safety, Wiley-AIChE, 2001.

EEMUA, 2007. Alarm Systems, A Guide to Design, Management and Procurement, The Engineering Equipment and Materials Users' Association Publication No 191, Edition 2, ISBN 0 85931 155 4.

HSE, 2008. Control Systems Technical Measure @ http://www.hse.gov.uk/comah/sragtech/techmeascontsyst.htm.

IEC, 2003. IEC61511 Functional safety – Safety instrumented systems for the process industry sector, Parts 1–3.

Kletz, 1995. Computer Control and Human Error, T Kletz, etal., Institute of Chemical Engineers, 1995.

Nimmo, 1997. Lessons learnt from the failure of computer system controlling a Nylon polymer plant, Nimmo, I., Nunns, S. R., & Eddershaw, B. W., Safety & Reliability Society Symposium, Altringham, UK, November 1997.

AUTHORS

PRINCIPAL AUTHORS

Paul Lucas, Principle Safety Consultant, Safety Solution Group, ABB Engineering Services

Tony Atkinson, Principle Consultant, Operator Effectiveness and Alarm Management Team, ABB Engineering Services

CONTRIBUTING AUTHOR

John Walkington, Senior Business Development Manager, ABB Engineering Services

AUTHORS

Paul Lucas is a Principle Safety Consultant and TÜV approved Functional Safety Engineer with over 25 years experience of real-time computing and safety in the process chemical, oil & gas and pharmaceutical sectors. He has worldwide experience of performing audits and gap analyses against IEC61508/IEC61511 and delivers training courses and seminars on the practical implications for end users, system integrators and instrument technicians in the use of the IEC61511 functional safety standard.

Tony Atkinson is a Principal Safety Consultant with ABB Global Consultancy and a TÜV Certified Safety Engineer.

He has over 30 years experience in the process industries, both within operating companies as a Responsible Control System Engineer and as a consultant. He has a keen interest in Human Factors and control room issues and currently leads the Operator Effectiveness and Alarm Management teams in ABB Global Consulting.

John Walkington is a senior business development manager for engineering within the oil & gas and Chemicals sectors. He has some 28 years experience from a combination of operational, maintenance and business development roles within ICI, BASF and ABB and in particular for the management, design and operation of instrumented safety systems.