"Assurance and Verification Practitioner's Guide" – Three Years On

David Richardson and Nigel Bowker, Atkins, Aberdeen, UK

The concept of Safety Critical Elements (SCEs) was introduced in the UK oil and gas sector by the legislation enacted following the Piper Alpha disaster in 1988. As part of the management of Safety Critical Element effectiveness, Duty Holders are expected to have assurance processes in place and to have appointed Independent and Competent Persons (ICPs) to undertake verification of safety-critical plant and equipment.

As a result of a major review undertaken by the Health and Safety Executive between 2004 and 2007, it was concluded that verification was not delivering the benefits expected by stakeholders.

Step Change (a cross-industry group) responded to this by publishing the "Assurance and Verification Practitioner's Guide". This provided guidance on the development of performance standards for the management of Safety Critical Elements using the functionality, availability, reliability, survivability and interaction (FARSI) format. It also provided guidance on the verification of SCEs.

Atkins has worked across many assets to develop documents that combine the Safety Critical Element Performance Standards and Verification Requirements in a single easy-to-use tabulated format. This has allowed us to develop a number of insights into some of the successes and continuing challenges of managing Safety Critical Elements. Some of these are:

- Recognising the difference between design and operational Performance Standards.
- The effective construction of Safety Critical Element Performance and Verification Standards.
- The interactions between Safety Critical Element functionality, assurance and verification.
- Ensuring that Safety Critical Element performance standards lie at the heart of integrity management.

This paper enlarges on these matters.

Keywords: Safety Case, Safety Critical Element, Performance Standard, Verification Standard, Independent and Competent Person, H&SE.

Introduction

The Piper Alpha disaster of 6th July 1988 in which 167 people died led to a radical change in the offshore oil and gas regulatory regime. This included:

- The transfer of responsibility for regulation from the Department of Energy to the Health and Safety Executive.
- The extension of the Health and Safety at Work etc. Act 1974 to include the offshore oil and gas industry.
- The introduction of the Offshore Installations (Safety Case) Regulations 1992 (referred to as the OSCR) and other regulations addressing the management of Major Accident Hazards (MAHs).

The OSCR introduced the concept of safety critical elements (SCEs), defined as ""such parts of an installation and such of its plant (including computer programs), or any part thereof (a) the failure of which could cause or contribute substantially to; or (b) a purpose of which is to prevent, or limit the effect of, a major accident."

The Offshore Installations and Wells (Design and Construction, etc.) Regulations 1996 (DCR) introduced requirements for the Safety Critical Elements to be verified as suitable by an Independent and Competent Person (ICP) at all phases of the asset life cycle.

During 2004 and 2007, the Health & Safety Executive (H&SE) undertook a review of safety equipment and the supporting management processes. This review concluded that verification was not delivering the benefits expected by stakeholders.

In response to this Step Change in Safety - which is a cross-industry body representing the workforce, regulator and employers – created a sub-group in 2010 to develop guidance. This is guidance was published as the "Assurance and Verification Practitioner's Guide".

The guidance addressed the following:

- The barrier model for managing major accident hazards.
- Performance Standards.
- Assurance and integrity management.
- Verification.
- Training, competence and roles and responsibilities.
- Management of change.

- Temporary equipment.

The recommended model for developing Safety Critical Element Performance Standards is based on the Functionality, Availability, Reliability, Survivability and Interaction (FARSI) format where:

Functionality refers to the purpose that the Safety Critical Element has to be able to perform to prevent, detect or mitigate a hazardous event or to protect people.

Availability refers to the proportion of the time that the Safety Critical Element will be required to perform on demand.

Reliability refers to how likely the Safety Critical Element is to perform on demand.

Survivability refers to how the Safety Critical Element will perform after a major accident has occurred, i.e. how well it will survive a fire, explosion, dropped object, etc.

Interaction refers to the way that the Safety Critical Element in question is dependent upon other SCEs to operate or otherwise interacts with other SCEs.

The Step Change guidance then discusses the appropriate approach to verification.

Atkins Experience

Atkins has significant experience of preparing systems that include both Performance Standards and Verification Requirements for a wide range of assets. These span the period before the Step Change guidance was introduced and the time since. This includes both UK-based clients and some overseas clients, since the concepts used in the UKCS have been widely adopted as good practice.

Our experience includes preparing design and operational Performance/ Verification Standards, working in collaboration with Duty Holders and ICPs.

The remainder of the paper describes the learning arising from this experience.

Design and Operational Performance Standards

It is a legislative requirement that Performance Standards are prepared/ maintained through the life cycle of the asset. Crucially, this includes having such standards at both the design and operational phases of a project. These fulfil very different requirements.

At the design stage, the Performance Standards are establishing the design functionality, the relevant codes and standards to be applied, etc. to the Safety Critical Element.

Taking the example of a fixed firewater system, the design Performance Standard will specify the discharge flow and pressure requirements for the fire water pumps, the availability requirements, the protection to be applied to key parts of the firewater system, the appropriate design standards, and the availability, reliability and survivability requirements, etc to deliver ALARP.

At the operational stage, the performance standards are concerned with how the functionality as determined at the design stage is being maintained. Hence for a fire water pump the operational Performance Standard is concerned with how it is being ensured that the design requirements (such as pump flow and discharge pressure) are being assured on an ongoing basis. It is taken as read that the requirements established during the design stage are correct. The effect of modifications during design, commissioning or operations also needs to be taken into account where applicable.

We have found situations where the mindset has been to regard the design Performance Standards as requiring just a few tweaks to convert them into operational Performance Standards rather than recognising that the two documents serve very different purposes. Furthermore, we have found examples of operational Performance Standards not being prepared at all i.e. the design Performance Standards have been carried through unaltered into the operational phase, in at least one case for several years.

Availability of Design Information

Many operational Performance Standards contain extensive design details of the Safety Critical Elements which can make them unwieldy. Sometimes (as noted above) this is because design Performance Standards have been carried forward into operations. A standard response to the suggestion that this data should be stripped out is “But we don’t want to lose this information”. That is certainly true but the operational Performance Standards are the wrong place for it. The information should be contained in the design Performance Standards or in a separate data base which can even be hyper-linked or otherwise cross-referenced from the operational Performance Standard. Part of the problem is that the design Performance Standards are often unavailable as indeed is frequently the original design data itself. The transfer of assets between duty holders with the consequent risk of losing data in the process does not help. This potentially places the Duty Holder in a difficult position, as it is difficult to demonstrate compliance with the necessary safety standards if a clear link to design information is not possible. In cases like this it is often necessary to make indirect assertions of compliance through adoption of FARSI parameters and performance criteria regarded as good practice, by comparison to similar situations in the industry.

The Effective Construction of Performance and Verification Standards

The exact format of a combined Performance/ Verification Standard has to be agreed with each client, of course, and many clients have their own approach. Where there is freedom to choose or influence the client, we have found the following process to be extremely helpful.

It commences with getting clarity over the precise hazard management goal and the hazard management role (i.e. is it there to prevent a MAH event, to control it, to mitigate it or to provide emergency response of some kind?).

It then moves to on to clarify the system limits (i.e. what is included within the particular Safety Critical Element – and hence what is excluded).

The dependencies and interactions with other Safety Critical Elements are then captured, usually in matrix form on a "reasonably foreseeable" direct basis.

The Performance/ Verification Standard then has a section to capture issues that are generic to all Performance Standards: frequently this is (a) the need for the Management of Change (MOC) system to take account of the impact on Safety Critical Elements; and (b) the need for defects to be captured via the maintenance management system.

We then get into what might be regarded as the guts of the document where we lay out the Performance Standard and the Verification Requirements alongside each other. This helps to show the flow through the system of:

- Determining the functionalities for the Safety Critical Element.
- Determining the appropriate assurance requirements for each functionality. Typically this will take the form of maintenance routines, inspection routines, testing routines or other relevant procedures as required.
- This can then neatly segue into stating the verification requirements, including the discipline involved and the frequency.

One advantage of this approach is that it provides an 'at a glance' guide for each functionality. Another is that it allows for a rigorous linkage between functionality, assurance and verification to be developed. Adoption of the cross-functional document format also makes subsequent reviews and updates much more straightforward.

In some other approaches it is difficult to see how the verification process is linked to the performance requirements for the Safety Critical Element; indeed, we have found examples of the two being totally separate activities.

The required availability of the Safety Critical Element, its reliability and its survivability are likewise addressed using the process of model of functionality, assurance and verification where applicable.

The SCE Performance/ Verification Standards Should Lie at the Heart of the Integrity Management System

It is a regrettable fact that all too often much effort is expended on developing Performance/ Verification Standards, only for the preparation of them to be seen to be an end in itself. A possible cause in some situations is the cumbersome nature of the Performance Standards and the poor linkage between Performance Standards and the associated verification requirements. How can you know that a safety critical element has been impaired if it isn't absolutely clear what it is meant to do? That is where simple Performance/ Verification Standards with clarity over what role the Safety Critical Element has to perform is key.

At their best, we have found Performance/ Verification Standards that:

Are widely available both onshore and offshore. Traditionally, this would have been via paper copies. Increasingly they are now being made available electronically. The key, though, is not so much the medium that is used to store and communicate the documents as the system for making personnel aware of their existence and purpose. When visiting offshore installations, we have sometimes found it hard to obtain the Performance Standards. Sometimes they are regarded as being something which is purely dealt with onshore. There is frequently confusion between Safety Critical Elements and Safety Critical Equipment. The Safety Critical Elements are the major "barriers" to prevent, mitigate, control or respond to a major accident event. Safety Critical Equipment are individual pieces of equipment which may form part of a Safety Critical Element.

Are clearly linked with the maintenance and inspection regime. Clear functionalities should be defined for each Safety Critical Element. Then specific maintenance and inspection activities should be specified for continuously assuring these functionalities. It is important that so far as possible these are activities are focussed on the functionalities themselves rather than being some existing routines that have been 'slotted in' to fill the box.

Are clearly linked with the verification programme. As with the assurance activities the verification activities should be specific to the required functionality. They are frequently developed by the operator and agreed with the ICP. Verification can consist of visible inspections, witnessing of performance tests, review of documentation (such as maintenance and inspection records) or a mixture of these things. There has sometimes been an attitude that verification is performed because it is required by legislation rather than it being a crucial part of the integrity management system. At its best, the Duty Holder, its maintenance and inspection contractors and the ICP are working together to reduce the risk of a major accident.

Are regularly reviewed and updated. Regrettably, sometimes the drafting of Performance/ Verification Standards is seen to be an end in itself. At its best, though, we have found examples of Duty Holders reviewing the Performance/ Verification Standards on an annual basis using all the available data to develop the best possible insight into how well the Safety Critical Elements are performing and how their performance may be improved. The data used includes:

- Maintenance results.
- Inspection results.
- Verification results.
- Availability data.
- Reliability data.
- Insights from accidents and incidents.
- Insights from wider industry data.

The data can be used to develop:

- Improved approaches to maintenance and inspection.
- Hardware modifications.
- Procedural improvements.

All of this can be seen to be in the interest of improving – and demonstrating - the ALARP status of the installation.

Have a clear process for evaluating the risk associated with Safety Critical Element impairment. There needs to be instant recognition of when a Safety Critical Element has been impaired, i.e. is no longer able to fulfil its purpose. This needs to link into a process for assessing the risk posed by this impairment and what risk reduction measures are required. The evaluation should include an analysis of whether there are still an adequate number of barriers in place. On occasion, a total installation shutdown and even partial de-manning may be required. We have found examples of some basic decision-making being contained within the Performance/ Verification Standard. So far as possible, we seek to discourage this since it:

- Can clutter the Performance/ Verification Standard.
- Can only cover a limited number of events.

This is not to say, of course, that some guidelines for how to cope with major impairments (such as non-availability of a fire pump) should not be available but that the detailed information should be held elsewhere in the Safety Management System and signposted from the Performance Standard. Typical examples might be:

- Actions to be taken in the event of Performance Standard failure.
- Procedures(s) for risk assessment on Performance Standard failure.

It is, incidentally, worth mentioning that the Performance Standards should not be cluttered with other information either, such as:

- Design information references in operational Performance Standards (as noted in section 2.1).
- The verification scheme policy and arrangements.
- The Safety Management System policy and arrangements.

Conclusion

We have found a wide range of approaches to the preparation of Safety Critical Element Performance Standards and their associated Verification Requirements. Some of these constitute very good practice whilst others have room for improvement.

The Step Change "Assurance & Verification Practitioner's Guide" provides excellent guidance.

Other related guidance is available via the Health and Safety Executive, The Energy Institute, the Commission for Energy Regulation (for those working under the similar Irish regime) and various other bodies.

A couple of final thoughts:

- Many Duty Holders use consultants such as Atkins to draft their Performance/ Verification Standards. It is our experience that this works best when established as a collaborative activity between the consultant and the Duty Holder. The Duty Holder needs to have a clear idea as to what they want to achieve and how it is to be done and provide management resources to co-ordinate the process internally, since access to a significant amount of Duty Holder resource (technical authorities, support

engineers, verification engineers and the ICP) is required. It is essential to take time up front to establish how the project is to be delivered and developing one Performance/ Verification Standard as a model for agreement before proceeding.

- Although Safety Critical Elements are defined as being hardware or software, the important of competence and competence assurance must not be under-estimated since all of the assurance and verification activities are crucially dependent on competent personnel.

Acknowledgements

We would like to acknowledge the many conversations with our colleagues and clients that have helped in the formulation of the ideas put forward in this paper.

References

1. Assurance and Practitioner's Guide, Step Change in Safety.
2. A Guide to the Offshore Installations (Safety Case) Regulations 2005, UK Health and Safety Executive.
3. Guidelines for the Management of Safety Critical Elements, Energy Institute, 2007.
4. Compliance Assurance System CER/13/254, The Commission for Energy Regulation, 2013.