



The Roadmap To Functional Safety

Q1: Setting the Stage for Project Success

The successful partnering of the risk management process to a control and safety system project can have a very positive impact on a company's earnings. Good corporate practices can reduce business risk and improve process reliability and process operability, leading to improved plant uptime, reduced operating expenses and the virtual elimination of emergencies and their associated capital and reputational costs.

Good risk management programs will optimize critical and non-critical safeguards to maximize safety. Yet the benefit of risk management goes beyond safety, it is an integral part of operational excellence. In a March 2009 speech to the World Refinery and Fuels Conference, Chevron Corp.'s president of global manufacturing stated that "we found that if you operate your refinery reliably and safely, you can produce as much as one new Greenfield refinery". He added "we think the technology is available today to react to upset conditions without human interaction". That's quite a statement, backed up by the fact that Chevron's 2.2 million barrel per day refining system has been able to improve operational reliability equivalent to a 5 to 7 % capacity gain of between 100,000 and 150,000 barrels.

In today's economic environment, where scarce capital is expected to quickly produce an attractive return on investment, implementing proven Process Safety Management (PSM) practices pays off, both in terms of productivity and accident prevention. You may recall that cost cutting in equipment maintenance was determined to be a contributing factor in the 2005 BP Texas City refinery explosion.

Many companies declare that the safety and control systems within their facilities are expected to comply with the latest corporate standards and international best practices. To make this a reality, the first step is to review the internal corporate procedures concerning the design and engineering of the various classes of instrumented systems, such as basic process control systems, critical alarm with operator response and protective instrumented systems, especially Safety In-

strumented Systems (SIS). During the review, procedures and standards pertaining to the SIS systems may be confusing or missing entirely. This remind us of a famous passage from Lewis Carol's Alice in Wonderland where the Cheshire cat addresses this same issue by saying to Alice, "if you don't know where you are going, any road will take you there".

The other reality is that project and operations management may be resistant to changing the firm's engineering process to incorporate the risk reduction principles outlined within the ANSI/ISA S84.00.01 / IEC 61511 Functional safety - Safety instrumented system for the process industry sector standard. As companies have few internal resources to

tives may be politically sensitive during this time of cost avoidance. Everyone wants the road to safety but isn't there some other way? At least until the profits of yesteryear return.

To address this standard confusion and management reluctance, over time we evolved a "roadmap to Functional Safety", using a simple story and model that makes project and operations managers understand quickly how this will work to benefit them. Technically grounded to ANSI/ISA S84.00.01 / IEC 61511, it has been proven in board rooms to quickly get management on side.

The ACM roadmap to Functional Safety addresses the questions: "how can I engineer my plant's safety and control systems to comply with the latest standards and practices" and "how can I make sure my plant is safe during the 25-50 years of operation?" The ACM Quad Model, introduced in earlier articles, enables managers, technicians and non-practitioners to understand Functional Safety and how the goal of complying with the latest corporate standards and international best practices can be achieved. The steps in the road to safety a corporation decides to build and maintain can be justified and phased in as the project can afford them or as mandated by the corporation. Some organizations taking this first step will use a smaller project as a learning opportunity to validate the benefits. The important thing is that all stakeholders understand the basic principles of Functional Safety and have been exposed to the roadmap to implement them.

The balance of this article is about Quadrant 1 of the ACM Quad Model (Figure 1), which we refer to as the Concept quadrant. The Safety Life Cycle begins at the Concept quadrant. As an idea moves from inspiration to concept, then through feasibility, it matures into a full blown project and needs to be managed through its life cycle within a company's Risk Management policy or philosophy. This quadrant sets out the Functional Safety roadmap for the project. The intent of Q1 is to integrate the prin-

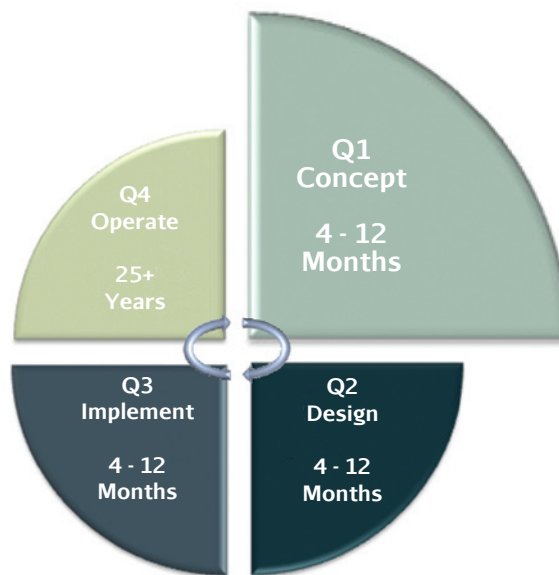


Figure 1: The Q1 Concept Quadrant of the ACM Quad Model

turn to for guidance and direction and (rightfully so) don't see vendors or engineering companies as interested in their well being as they are, they can end up questioning the entire approach and looking for justification and reassurance on their decision. They see the whole initiative as confusing, likely high cost and managers don't know how they can justify the cost and effort involved. New initia-

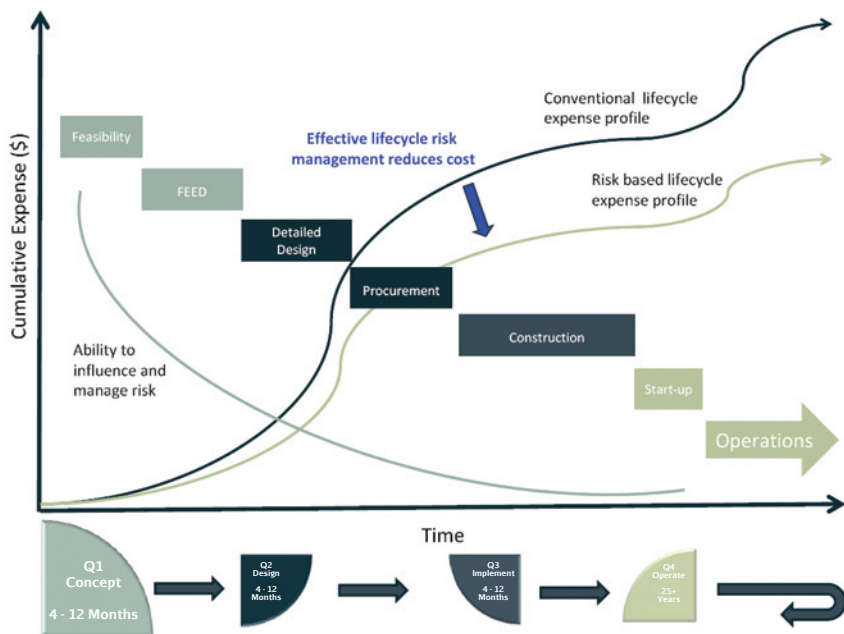


Figure 2: Project Lifecycle Cost / Ability to Influence Risk Comparison

principles of Risk Management with the specific Functional Safety requirements of safety and controls systems projects. After 15 years in business, experience tells us that Q1 is the fuzziest or least definitive quadrant. It relies on a combination of hard, quantitative engineering and less definitive, qualitative risk analysis and judgement. Companies that understand and execute this quadrant well will be repaid handsomely.

Risk Management

Risk Management is defined as a planned and systematic process of identifying, assessing, monitoring and controlling risk which adds value to the business. Its main goal is to help management maximize business value. This is achieved by improving the odds of meeting objectives by making good decisions and by taking appropriate actions with limited and imperfect information. This planned and systematic process does not replace the need for management judgement or leadership. Rather, it seeks to maximize the use of collective wisdom and experience through an established process.

The risk management process has the most impact and value during the early days of a project and at the start of each phase of a project. Starting off right is far easier and more cost effective than trying to correct adverse trends on a project whose momentum has already got going. As such, Risk Management is subject to the law of diminishing returns over time. Figure 2 shows how the project team's ability to influence becomes rapidly smaller as a project gets locked into its strategy.

In the ACM Quad Model, Q1 is roughly

equivalent to the Feasibility and FEED phases. The other matches are: Q2 to Detailed Design and Procurement; Q3 to Construction; and Q4 to Start-up and Operations.

The risk reduction process outlined within ANSI/ISA S84.00.01 / IEC 61511 parallels the traditional way of looking at Risk Management, which has five key pillars and when simplified are:

- 1) Risk identification – brainstorm hazards and causes of risk;
- 2) Risk Assessment – qualify or quantify consequences;
- 3) Response planning – optimize the response based on corporate priorities and preferences;
- 4) Action – make decisions and execute the risk reduction plan;
- 5) Continuous improvement – measure and strive to reach stretch goals.

The first two activities are concerned with the identification of uncertainty, and its associated risk to project budgets, schedules and value. Risk identification is a qualitative assessment via recognized techniques such as HAZID and brainstorming. In Risk Assessment, a stronger and more valuable outcome is possible if the risks and uncertainties are modeled semi-quantitatively or quantitatively if appropriate. Consistently using well defined risk models for facilities from an early stage enables a more rigorous and scientific approach to ranking and quantifying risk.

Common challenges we encounter is the risk assessment area include:

- struggling with the concepts of defining acceptable or tolerable corporate and/or individual risk;
- realizing the suite of risk “tools” is not

either complete or “fit for purpose” to their business;

- weak, incomplete or outdated internal corporate standards and procedures, often leading to confusion over technical terms and acronyms.

Team Competence

Another important activity that begins in Q1 is ensuring that staff working directly on the control and safety systems project are competent. That means they must have the fundamental education and experience necessary to perform their assigned tasks. They need to be trained in the steps involved in keeping the protective management system operating as designed. However, a major challenge within today's owner/ operators is that they have fewer experienced technical specialists in the company. The most senior plant operators have retired. The most knowledgeable corporate experts may have been downsized or their function replaced entirely by the reliance on engineering firms or vendors to supply this expertise. Consequently, owner / operator's project managers may feel vulnerable.

Training and education can address the need for competent staff, not just during Q1 but throughout the Safety Lifecycle. This is particularly true for owner/ operators of existing plants with SIS systems or what we refer to as during Q4 on the ACM Quad Model. They often need help through training or mentoring programs. Increasingly, this also means that individuals require certification from an accredited training program, such as the TÜV Rheinland Functional Safety Program for Safety Instrumented Systems. ACM is Canada's only course provider in this program, which has trained nearly 1,800 professionals from over 25 countries since 2004.

Operating Procedures

The importance of well written procedures cannot be overstated. They are used to retain essential information, which is often kept informally by key individuals within the organization. Due to the reality of staff turnover and multiple EPC firms working on an owner/ operator's project, procedures are often the only means of communicating the requirements and activities. Operating procedures are needed for all four quadrants of the Safety Lifecycle.

SRS Specification

The output of Q1 is the Safety Requirement Specification or SRS. It contains the performance and functional requirements of the SIS. The SRS forms the key measure by which the SIS design is compared and judged throughout the remainder of its lifecycle. It is not a document generated once, but is instead a living and evolving document that changes

throughout the entire design. It is much more than just the specification for the SIS design. It is the fundamental validation tool for the SIS design and is the basis for management of change activities through the SIS's lifecycle. Considering that OSHA's PSM program requires companies to maintain up-to-date and accurate "process safety information", it is not a stretch to say that a comprehensive SRS is as important a document to a SIS as a P&ID is to performing a HAZOP study. It is critical process safety information.

Verification

To round out Q1 activities is to ask if everything has been done completely and per specification. Again, without a roadmap to follow and a way of measuring accomplishment, how is this possible?

Verification activities are comprehensive quality checks on documentation typically conducted by members of a project team or company who are not directly involved in the execution of the work. The documentation should be comprehensible and detailed such that all parties understand its contents. Verification is part of the overall Functional Safety

Assessment which is a high level review of the overall risk management approach being executed in each of the quadrants to determine whether it is consistent with the project's risk analysis findings and its' operational requirements.


Q1 Benefits

As a company starts this journey, it is vital to the whole process that benefits are seen almost immediately by those involved to keep the momentum going. Benefits realized by some of our clients in Q1 of the ACM quad model include:

- Eliminating 30 - 50% of the Safety Instrumented Functions (SIF) in the proposed design of a new sour gas plant, saving upwards of \$100,000 per SIF in hardware costs and maintenance savings (based on a 25 year lifecycle including capital purchase, installation, hardware, maintenance, replacement every 10 years, spare parts, training, related loss production time due to failures, etc.);
- Cutting 20 - 40% from the proposed testing and maintenance budget of a new facility because only those critical or safety related functions would receive intense atten-

tion and resources;

- Obtaining approval from regulatory authorities to stretch testing interval of subsea valves from every month to every 3 - 6 months by using the LOPA process to demonstrate that safety integrity was not compromised.

The activities in Q1 are objective and subjective, scientific and gut based. By executing this phase of a control and safety systems project well, the pay off is huge. Risks have been managed, the process is auditable and the operating asset is set up for a successful life. Consider a recent quote by Trevor Kletz on the BP Texas City follow up: "If you think safety is expensive, try an accident!" 



About the Author: Readers can contact the author, Ken Bingham of ACM Facility Safety, a division of ACM Automation Inc. for more information by email: ken.bingham@acm.ab.ca and by telephone at 403.264.9637