Session Twelve

A generally accepted good practice approach to functional safety management

David Nassehi
Senior Functional Safety Engineer/CFSE, PMP- Plexal Group Pty. Ltd. www.plexalgroup.com

Abstract

The Project Management Institute (PMI) Project Management Body of Knowledge (PMBOK) GUIDE (ANSI/PMI99-001-2008/IEEE1490-2011) presents a set of standard guidelines for project management and identifies the project management body of knowledge that is generally recognized as good practice. It is process-based and the approach is consistent with ISO 9000. It describes the project management life cycle and the project life cycle.

This paper compares AS IEC-61511 lifecycle and Functional Safety Management requirements with the PMBOK guidelines, identifies the approaches which are in line with both and suggests strategies to embed in the project lifecycle which improves Functional Safety (FS) objectives throughout the safety lifecycle to achieve integrated functional safety and project management.

Introduction

AS IEC 61511-1 clause 5 requires that a safety management system must be in place so as to ensure that where safety instrumented systems are used, they have the ability to place and/or maintain the process in a safe state. The requirements are:

- Persons, departments, organizations or other units which are responsible for carrying out and reviewing each of the safety life-cycle phases shall be identified and be informed of the responsibilities assigned to them (including where relevant, licensing authorities or safety regulatory bodies).
- Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable.
- Hazards shall be identified, risks evaluated and the necessary risk reduction determined as defined in Clause 8.
- Safety planning shall take place to define the activities that are required to be carried out along with the persons, department, organization or other units responsible to carry out these activities. This planning shall be updated as necessary throughout the entire safety life cycle.
- Procedures shall be implemented to ensure prompt follow-up and satisfactory resolution of recommendations pertaining to the safety instrumented system arising from hazard analysis and risk assessment, assessment and auditing activities (verification activities; validation activities; post-incident and post-accident activities).
- Any supplier, providing products or services to an organization, having overall responsibility for one or more phases of the safety life cycle, shall

deliver products or services as specified by that organization and shall have a quality management system. Procedures shall be in place to establish the adequacy of the quality management system.

To cover these requirements a target oriented management system is essential, which examines the safety case, plans and manages activities, and monitors and controls performance and quality. The Project Management Body of Knowledge (PMBOK) offers tools and techniques to reduce management threats.

PMBOK is a collection of processes and knowledge areas generally recognized as best practice within the project management discipline. “Generally recognized” means the knowledge and practices described are applicable to most projects most of the time, and there is consensus about their value and usefulness. “Good practice” means there is general agreement that the application of the knowledge, skills, tools, and techniques can enhance the chances of success over many projects. As an internationally recognized standard (IEEE 1490-2011), it provides the fundamentals of the project management, applicable to the most of industries such as construction, software, engineering, and automotive. PMBOK recognizes five basic process groups (initiating, planning, executing, monitoring and control, and closing) and ten knowledge areas (scope, schedule, cost, quality, human resource, communications, risk, procurement and stakeholder management).

Similar to almost all projects, processes overlap and interact throughout a project or phase. Processes are described in terms of Inputs (such as documents, plans, and designs), tools and techniques (mechanisms applied to inputs) and Outputs (such as documents and products).

Functional Safety Management Threats

Most of the researches in functional safety subject examine its lifecycle activities with the aim of identifying failure causes of incidents. However, there are few researches to identify functional safety management threats. Risks of an unsuccessful functional safety management could be caused by the customer, lack of control over suppliers, sellers and contractors, lack of project management effort or knowledge of the project manager and stakeholders, the customer's customers, suppliers, resistance to change, or cultural differences.

Functional safety projects in general, share the common causes of project failures such as poor problem definition, indefinable scope, lack of support, undesignated individual in charge, lack of project plan, structure and detail, under-funded, insufficient resources, poor tracking, poor communication, straying from goals, unrealistic time frames, gold plating, Scope creep or changing deliverables.

Scope Creep

Functional safety projects are vulnerable to scope creep. The scope may not be properly defined from the beginning as the requirements are unknown until after hazard & risk analysis and allocation of protective layers. The scope could be impacted as a result of integrated change management, new identified risks, updated quality measures, recently discovered stakeholders or other constraints such as time, cost, resources and quality. Large projects need to be

divided into phases or sub-projects. The scope creep will in turn impact other project constraints.

Schedule Creep

The project could be subject to inadequate time frame due to late identification of the requirements, unexpected delays, changes to project priorities and critical path, and changes to other project constraints.

Unmanaged Stakeholders

Many project managers fail to consider the span of potential stakeholders. Stakeholders are any people or organizations whose interests may be positively or negatively impacted by the project or its product, as well as anyone who can exert positive or negative influence over the project. Any stakeholders who are missed will likely be found later. When they are discovered, they will probably request changes, which may cause increased scope of work, reworks and delays. Changes made later in the project are much more costly and harder to integrate than those made earlier.

Poor Communication

Project managers spend up to 90 percent of their time for communicating. Poor communications are the most frequent cause of problems on projects, resulting in increased conflicts, and obstructed requirements collection and information flow. It can have a negative impact on scope management, controlling and monitoring efforts.

PMBOK Approach to Mitigate FS Management Threats

While AS IEC 61511 depicts a lifecycle for project lifecycle phases, PMBOK suggests project management processes and identifies what need to do to manage the project lifecycle activities.

PMBOK covers all of the functional safety management topics of AS IEC 61511 and offers tools and techniques for the project management knowledge areas to fulfil those requirements. The choices of response strategies for “THREATS” include Avoid**,** Mitigate, Transfer (Deflect, Allocate) or Accept.

Managing Stakeholders

Identifying the stakeholders, their requirements, interests, concerns, influences and impacts is a key activity in initiation of the projects. Stakeholders include more than the project manager, customer, sponsor and team. Stakeholders are any people or organizations whose interests may be positively or negatively impacted by the project or its product. They can include individuals and groups such as the performing organization, the project management staff, the project management office, portfolio and program managers, and other departments within the organization (e.g., marketing, legal, and customer service), functional or operational managers, and sellers. External to the organization, including government regulators, consultants, end users, customers, taxpayers, and banks and other financial institutions, people or groups who could exert positive or negative influence over the project but would not otherwise be considered

part of the project are also considered stakeholders. A project manager should analyse and manage stakeholders' needs and levels of their influence throughout the project. A project manager should identify all of them as early as possible, determine their requirements, expectations, interest and level of influence, and then plan how to manage them, communicate with them, manage their expectations, influence, and engagement, communicate with them, and control communications. Planning communication with stakeholders is also critical and is related to stakeholder management.

Effective Communications

Good communication and relationships with stakeholders are critical to success, so it's essential to monitor these two areas on the project. Reports help the team members know where they need to recommend and implement corrective actions. Reporting performance includes looking into the future. Stakeholders are included in project presentations and receive project information, including progress reports, updates, changes to the project management plan, and changes to the project documents, when appropriate. The team and sponsor can use forecasts to determine what preventive actions are needed. Feedback from the people who receive the reports is essential to ensure the project still meets the business needs and aligns with the project charter.

Adopt Enterprise Environmental Factors

Projects have mutual impacts on cultural norms, management policies, and procedures of the organizations of which they are a part. Functional, projectized, and matrix organizational structures will dictate who the project manager goes to for help with resources, how communications must be handled, and many other aspects of project management. An organization's project management information system is part of its enterprise environmental factors. This includes automated tools, such as scheduling software, a configuration management system, shared workspaces for file storage or distribution, work authorization software, time-tracking software, procurement management software and repositories for historical information. Project managers deal with existing processes, procedures, and historical information or "organizational process assets". They are inputs to the majority of processes in all the project management process groups. They provide direction and guidance in planning and help the project benefit from past company experience. These include processes and policies for quality assurance, continuous improvement, procurement, human resource management, change control, safety, and more. Such information are key part of organizational process assets. Historical information (or data) is a record of past projects which is used to plan and manage future projects, thereby improving the process of project management. Historical information can include activities, lessons learned, WBSs, benchmarks, reports, risks, risk response plans, estimates, resources and project management plans and correspondence.

The Role of Project Manager’s Skills

PMBOK emphasizes some key attributes for the project managers. The project manager should be assigned during project initiating, be well skilled, put the interests of the project first, and have authority and power to plan before acting.

They understand the value of the tools and techniques and adapt them to a project, ensure that organizational policies are followed; spend time on such activities as team building and ensuring high team performance; are proactive to finds problems early; look for changes, and focus on preventing problems.
Before the project work starts, the project manager should assess whether the project can meet the project constraints and objectives and resolve any differences with management.

Project Management Frameworks

PMBOK assumes some key attributes for the project. A project should have project charter, which authorizes the project and the role of the project manager, A work breakdown structure (WBS) and a project management plan is in place; Stakeholders are involved throughout the project. Their needs are taken into account while planning the project and creating the communications management plan and stakeholder management plan. They may also help identify and manage risks. Project cost and schedule cannot be finalized without completing risk management. PMBOK assumes the project management plan is realistic, justifiable and achievable. Projects are re-estimated throughout the life of the project to make sure the end date and cost objectives will be met. Delays must be made up by adjusting future work, rather than extending delivery deadlines. A change in scope must be evaluated for its impacts to time, cost, quality, risk, resources, and customer satisfaction. The project manager should have enough data about the project to do this analysis.
Most problems that occur have a risk response plan already created to deal with them. Risks are a major topic at every team meeting. Team meetings do not focus on status. They can be collected by other means. All changes to the project management plan flow through the change management process and integrated change control. Quality is considered in performing changes to any component of the project and verified before an activity or work package is completed. No project is complete unless there has been final acceptance from the customer.

Scope Management

A requirements management plan should be developed which describes the methods to identify requirements, analyse, prioritize and manage them, and track changes. Some methods of collecting the requirements are interview, focus groups, facilitated workshops, brainstorming, multi-criteria decision analysis, affinity diagrams, mind maps, questionaries and surveys, observation, prototypes, and collecting historical records. Scope management plan is a plan which identifies in advance how the scope will be determined, managed and controlled. The Scope must be clearly defined and formally approved before work starts. Requirements are gathered from all the stakeholders, not just the person who assigned the project. Requirements gathering can take a considerable amount of time, especially on large projects that may involve obtaining requirements from hundreds of people. Requirements must be evaluated against the business case, and prioritized to determine what is in and out of scope. While the project is being executed, the project manager ensures that only the approved scope of work is being done. “Gold plating” a project is not acceptable.

Schedule Management

Project managers have a professional responsibility to amend unpredicted schedule impacts imposed by an unrealistic timeframe, management requests or integrated change control. They need to present options and ensure the project is achievable by properly planning the project and using schedule network analysis techniques like schedule compression to compress the schedule without changing project scope. Another method is “Fast Tracking” which involves taking critical path activities that were originally planned in a series and doing them in parallel for some or all of their duration. “Crashing**”** which suggests adding or adjusting resources in order to compress the schedule may also be employed.

Quality Management

Quality controls, and quality assurance is emphasized by the AS IEC 61511. The project manager should recommend improvements to performing organization's standards, policies, and processes. Quality should be considered whenever there is a change to any of the project constraints. Quality should be checked before an activity or work package is completed. Poor quality may result in increased costs, decreased profits, low morale, low customer satisfaction, increased risk, rework and schedule delays. Quality Management plan focuses on defining quality for the project, the product, project management, and planning how it is supposed to be achieved. Performing “Quality Assurance” is an executing process. Its focus is on the work being done on the project to ensure the team is following organizational policies, standards, and processes as planned to produce the project's deliverables. Quality control, in contrast is a monitoring and controlling process which examines the actual deliverables produced on the project. Its purpose is to ensure the deliverables are correct, meet the planned level of quality and to find the source of problems and recommend ways to address them.
Quality Audits are specifically requested in AS IEC 61511. Quality Audits and Process Analysis are among many other tools commonly used to perform quality assurance.

Human Resource Management

The competency requirements of the AS IEC 61511 have a strong link to human resource management. Human resource management includes determining the resource requirements, availability, project team directory, assigning roles and responsibilities, training, and recognition and reward systems.

The project manager is responsible for team building and improving the team members' competencies. The project team could be consulted to identify and involve stakeholders, identify requirements, constraints and assumptions, create the WBS, decompose the work packages for which they are responsible into schedule activities, help identify dependencies between activities, provide time and cost estimates, participate in the risk management process, comply with quality and communications plans, execute the project management plan to accomplish the work defined in the project scope statement ,conduct process improvement, and recommend changes to the project, including corrective actions.

Procurement Management

Project managers are responsible for maintaining project integrity and overall quality of the deliverables irrespective to being outsourced or internal to the project team. Therefore, they play an important role in procurement process. This role is highlighted when a contractor or supplier is involved in a safety lifecycle activity. Project manager involvement includes understanding contract terms and conditions, specifying scope of work and all the project management requirements(such as attendance at meetings, reports, actions, and communications), identifying risks and incorporating mitigation and allocation of risks into the contract to decrease project risk, tailoring the contract to the unique needs of the project, determining the time required to complete the procurement process, and identifying communication channels and completing the monitoring and controlling activities.

How PMBOK Helps Manage FS Lifecycle Phases

FS lifecycle phases are hazard and risk identification, allocating protective layer, safety requirements specification, design and engineering, installation and commissioning, operation and maintenance, modifications, and decommissioning. To manage each of these phases, some specific PMBOK process groups and associated knowledge areas and activities should be focused and require specific consideration.

Project Initiating

Project initiating process group and its activities come into focus when dealing with the identifying hazards and risks. It is a key success factor to Select functional safety project manager, determine company culture and existing systems, collect processes, procedures, and historical information, divide large projects into phases, uncover initial requirements, assumptions, risks, constraints, and existing agreements, assess project and product feasibility within the given constraints, create measurable Objectives, and identify stakeholders and determine their expectations, influence, and impact.

There might be occasions of major re-works on projects due to not involving operations department as the end-user stakeholders in communicating design specifications. Unclear assumptions or unspecified standards to comply can broadly impact the project scope and cost. Imagine the yawning gap between the 0.999 and 0.9999 safety availability requirement. Imagine how a SIS logic solver design project that environmental conditions are not fully specified and the vendor has completed his design and integration based on their default conditions and the product fails to function in the field.

Project Planning

IEC AS 61511-1 clause 6.2.3 requires a plan for all safety life-cycle phases to define the criteria, techniques, measures and procedures to ensure that the requirements are being met and maintained during the lifecycle. Also, the sequential nature of functional safety related projects mandates accurate work break down and network diagram.

A plan without considering the project constraints will never end up with on-time and on-schedule delivery of the safety related system outputs. Imagine how a delayed PHA report can lead to the whole project delay. Imagine how

desperate situation may arise if cost, resource or schedule contingency plans are not in place and some gaps are identified during stage 3 functional safety assessment. Unplanned communication management can lead to uncontrolled changes to the safety system. Incomplete procurement documents may end up with failed safety system targets. How the safety could be achieved or maintained if there is no contingency plan in place for a cyber-security risks to the control and safeguarding system? What is the plan if operating plant loses the Alarm IPLs because of a malfunctioning alarm management system?

PMBOK suggests that the project planning activities shall be performed once the basis requirements are identified and the project is initiated. For successful planning, the project managers should determine how they will plan for each knowledge area, determine detailed requirements, create project scope statement, assess what to purchase and create procurement documents, determine planning team, create WBS and WBS dictionary, create activity list, create network diagram, estimate resource requirements, estimate time and cost, determine critical path, develop schedule, develop budget, determine quality standards, processes, and metrics, create Process improvement plan, determine all roles and responsibilities, plan communications and stakeholder engagement, perform risk identification, qualitative and quantitative risk analysis, and risk response planning, iterate when necessary, finalize procurement documents, create change management plan, finalize the "how to execute and control" parts of all management plans, develop realistic and final PM plan and performance measurement baseline, gain formal approval of the plan, and finally hold kick-off meetings.

Project Execution

Each phase of the safety life-cycle incorporates project execution activities. There might be other suppliers, sellers, teams and departments involved in the activities. IEC AS 61511 requires that the lifecycle activities be performed as per the relevant phase plan. This in turn mandates to follow procedures, and carefully execute the activities to avoid deviations from the plan, react or pro-act accordingly to findings from monitoring and controlling measures and improve the performance wherever possible.

Functional Safety Assessment and auditing (IEC AS 61511, clause 5.2.6) requirements are all fit into the PMBOK “execution” process group and quality management knowledge area. Auditing is a quality assurance means to determine if procedures are being followed, efficient and effective. Process analysis is a part of the continuous improvement effort on a project and focuses on identifying improvements that might be needed in processes.

Through a process analysis, as well as other QA/QC analysis, a functional safety manager may notice that the hazard identification, risk assessment and SIL study as discrete activities are less effective or involves more repeated activities and decide to integrate and combine one or more activities to obtain quicker or more accurate results. By performing a causal analysis on spurious trips in an operating plant, one may realize that impulse line plugging is the root cause and suggest alternative hook-up arrangement or a higher redundancy for future designs. A review of punch items from a process unit’s safety application software, one may find that inefficient project communication or incomplete change management has led to uncontrolled ranges and setpoint data communicated to the software supplier. And as a result should recommend

review of communication procedures, impact analysis methods in their management of change, or their configuration management system.

In the “execution” phase, the project managers should execute the work according to the PM plan, produce product deliverables (product scope), gather work performance data, request changes, implement only approved changes , continuously improve, follow processes, determine whether processes are correct and effective (quality assurance), perform quality audits, acquire final team, manage people, evaluate team and individual performance, hold team-building activities, give recognition and rewards, use issue logs, facilitate conflict resolution, release resources as work is completed , send and receive information, and solicit feedback, report on project performance, manage stakeholder engagement and expectations, hold meetings and select sellers.

Monitoring and Controlling

IEC AS 61511, Clause 7 requires verification to be planned and performed as planned, tools and supporting analysis identified and non-conformances handled. PMBOK monitoring and controlling tools and techniques are supportive to analyse and identify non-conformances of product (i.e. SIS lifecycle activities and deliverables) and project performance (e.g. KPIs, SPIs, CPIs). Similar to IEC AS 61511 clause 17, which requires procedures for authorizing and controlling changes, PMBOK suggests “change requests” wherever a corrective or preventive action or a defect repair required.

Imagine what cost and schedule impacts could be expected if you find out that the SIL verification at the conceptual design phase was based on some wrong assumptions and your SIF fails to meet the targets just because of poor QC procedures. You may need to re-evaluate the design, add or modify sensors, process connections and expensive final elements, and update documents which will impede the project progress. Well-defined quality control procedure, as well as quality people which feed the findings back to the respective disciplines can extensively prevent such headaches.

The integrity of a SIF can be voided and the safeguard could fail dangerously and remain undetected if changes to hardware or software modules are not being kept under a controlled configuration management system, an important requirement of IEC AS 61511 clause 5.2.7 and one of the PMBOK emphasised topics.

The PMBOK requires that the manager should take action to control the project, measure performance against the performance measurement baseline and other metrics in the management plan, analyse and evaluate performance, determine if variances warrant a corrective action or other change request, influence the factors that cause changes, request changes, perform integrated change control, approve or reject changes, update the PM plan and project documents, inform stakeholders of the results of change requests, monitor stakeholder engagement, manage configuration, create forecasts, gain acceptance of interim deliverables from the customer , perform quality control , perform risk reassessments and audit, manage reserves, and control procurements. Cause and effect diagrams, flowcharts, check sheets, pareto diagrams, histograms, control charts, scatter diagrams are examples of the basic tools for quality controls which may assist in analysing performance data and correct or improve procedures.

Project or Phase Closing

The ultimate purpose of a functional safety project is to ensure that where safety instrumented systems are used, they have the ability to place and/or maintain the process in a safe state. No product of project or phase is finalized unless it is accepted by the customer with no exception and meets safety requirements. In order to close a phase of project and enter the next phase or close the whole project and deliver the final product, the project management should confirm that work is done to requirements. Finally, the project manager should complete procurement closure, gain final acceptance of the product, complete financial closure, and hand off completed product. It is important to solicit feedback from the customer about the project, complete final performance reporting, index and archive records, gather final lessons learned and update knowledge base.

References

AS IEC 61511-1: 2004, (2004) Functional safety—Safety instrumented systems for the process industry sector.

Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Fifth Edition (2013), Project Management Institute.