MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

20th Annual International Symposium
October 24-26, 2017 • College Station, Texas

Plan to Fail

Amit K Aglave, Shashi Shekhar

Fluor Daniel India Pvt. Ltd.,

New Delhi, India

Presenter E-mail: amit.k.aglave@fluor.com

Abstract

The process industry has widely adopted the Functional Safety Standards IEC61508 [1] and IEC61511 [2] for achieving the Functional Safety. These standards lay the framework for achieving functional safety by considering the entire life-cycle of the safety instrumented system (SIS). Typical SIS safety life-cycle phases and functional safety assessment stages are illustrated in Figure-7 of IEC61511-1 [2].

The design and engineering of the SIS are most often focused on achieving the required risk reduction for the safety instrumented functions (SIF). However, with this single minded focus, the design and engineering of the SIS frequently progresses without a well thought out safety plan.

"By failing to prepare, you are preparing to fail – Benjamin Franklin".

Taking cues from this quote, this paper, "***Plan to Fail?***" intends to draw attention to importance of having a well understood 'Safety Plan' in place. The standards provide guidance for the development of a safety plan. However it is imperative for the functional safety team to ensure that it is aligned with the particular project under consideration. This means establishing goals and concepts early in the project schedule. The plan would then be updated as more details are known and hence be more effectively deployed during each phase of the safety life-cycle.

Introduction

The common perception about functional safety and functional safety standards is that it's only related to defining the required SIL and whether it is achieved. This leads the functional safety engineers to mainly focus on the SIL assignment and SIL verifications tasks. This insular approach results in neglecting other important phases of the safety life-cycle as well as the activities done are 'not to a plan'.

The intent of this paper 'Plan to Fail' is to draw attention to the objectives, review the owners for the development and identify the key parameters which should be addressed in a functional safety plan. In an interview to US Chemical Safety Board, Dr. Trevor Kletz quoted: 'How can we improve the design so this (accident) can't happen, how we can remove the opportunity for errors' [4]. One way to remove the opportunity of errors is to have a proper plan in place. A proper plan in place would then mean, 'Plan to Succeed' (i.e., succeed in the goal of achieving the objectives of functional safety).

Objectives of Safety Plan

As prescribed in IEC 61511 [2], the management of functional safety requires safety planning to be done for all phases of the safety life-cycle. The objective of developing a safety plan is to define the activities to be carried out by persons, departments, organizations who are associated with the design, implementation and maintenance of the functional safety. The planning shall be updated as necessary throughout the entire SIS safety life-cycle. The planning should be carried to the detailed activity level for every role. This includes individual or organization activities related to the particular phase of the SIS safety life-cycle.

As per this definition, the objectives of the safety plan are:

- To identify the activities to be carried out related to functional safety,
- To identify the criteria the SIS design should meet,
- To identify the techniques, measures and procedures for carrying out the identified activities,
- To identify the persons, departments or organizations who would execute the identified activities and
- To ensure that planning exists or is developed to ensure that the SIS meets the safety requirements.

Timing to Develop the Safety Plan

The next question is for which phase and at what time, the safety plan should be drafted. Figure 1 below provides representation of the SIS safety life-cycle phases and functional safety assessment stages as defined in IEC 61511-1 [2]. This clearly indicates that the planning should happen for each phase. The plan for each phase should be in place and approved by all stakeholders before beginning the execution of the phase. This will help ensure that the activities proceed in a correct sequence and the expected outcome of each activity is defined. This will also help to ensure that the subsequent phases have the required inputs before starting the activities.

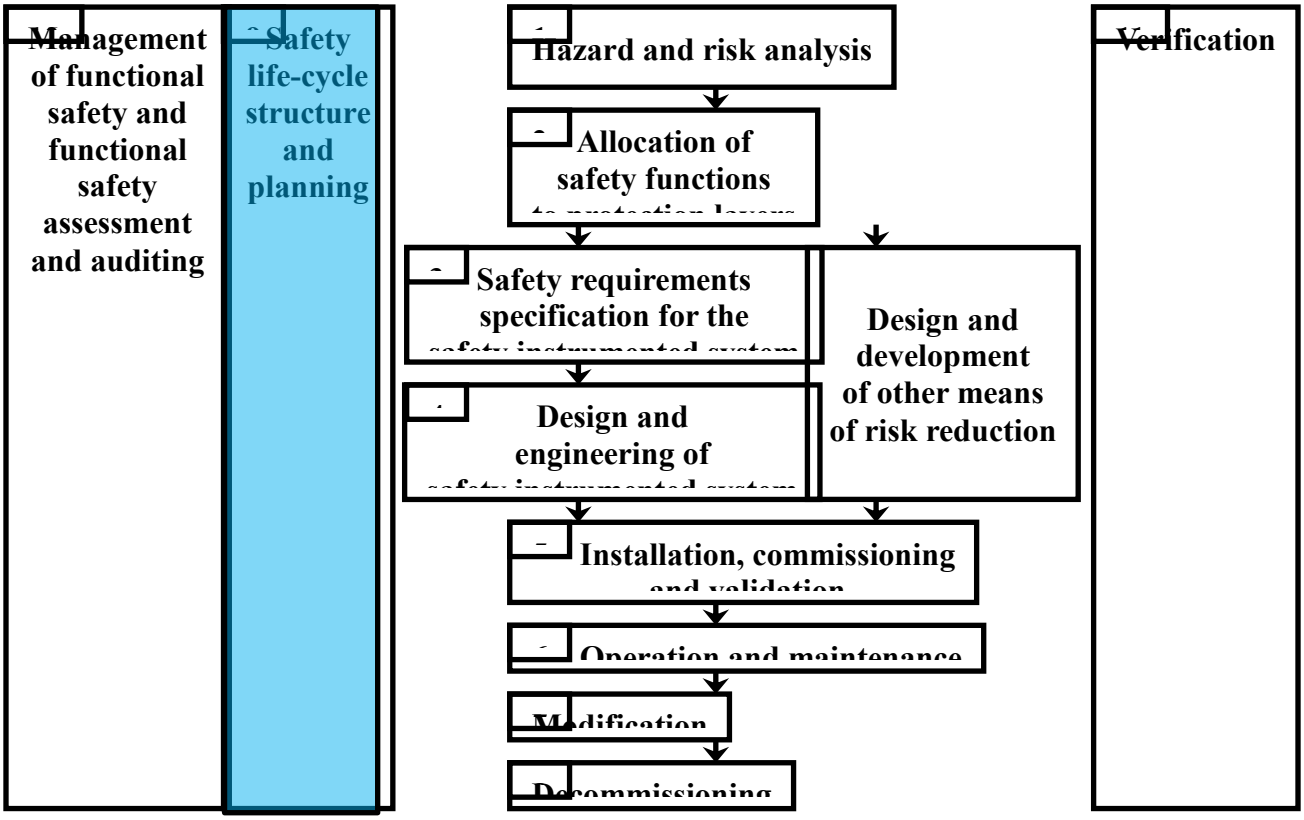

Figure 1. SIS safety life-cycle phases and FSA stages

Safety Life-Cycle Phase and Owners (Safety Plan Responsibility)

Since the plan undergoes a change in each phase with respect to the activities, persons, departments and organization, the safety plan is considered to be a live document. Figure 2 shows the responsible organizations which carry out the work related to the life-cycle phase. Within each organization, the departments and within the departments, responsible persons need to be identified. Assigning responsibilities for the development of the safety plan and identifying critical interfaces should be determined early in the project life-cycle.

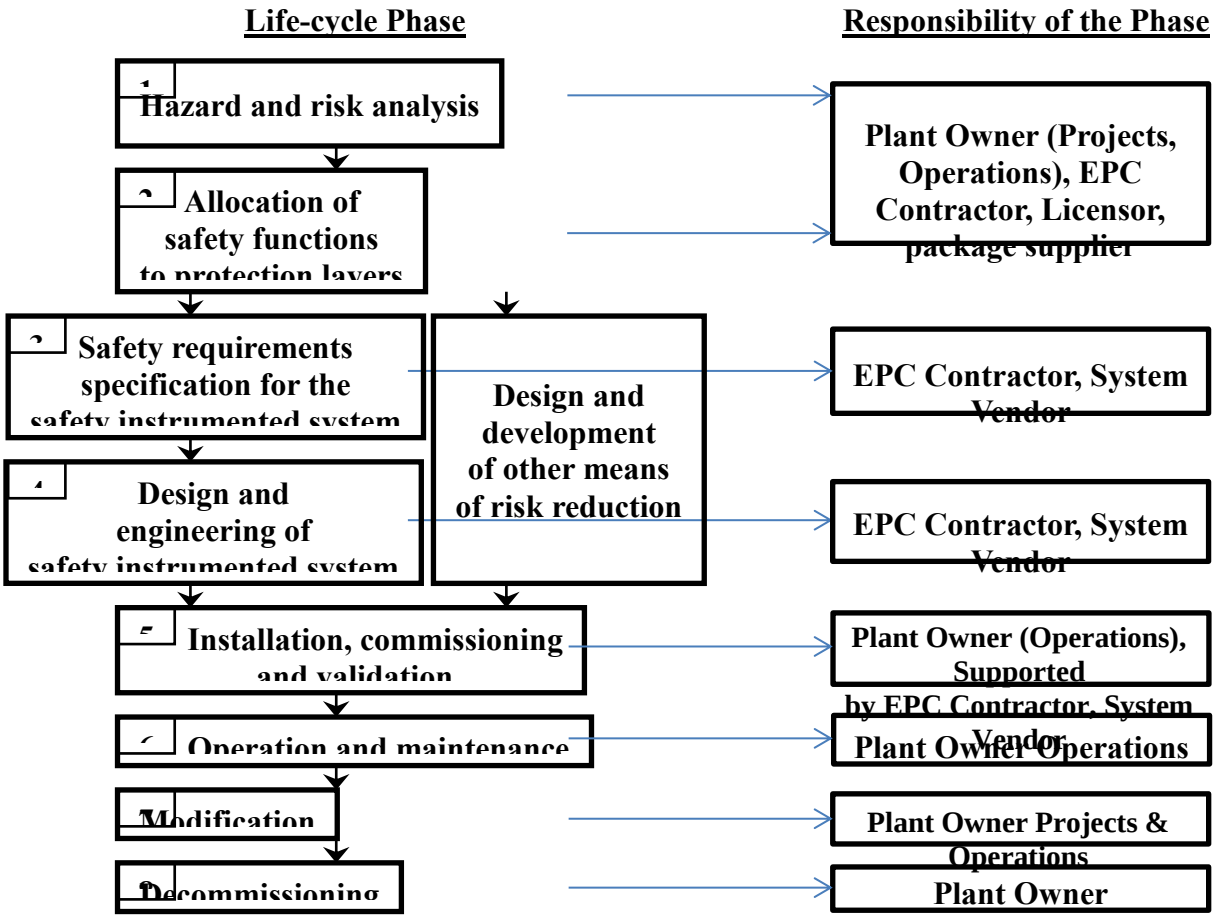

Figure 2. SIS safety life-cycle phases – Responsible Organizations

IEC 61511 [2] specifies that the periodic update or review of the safety plan should take place. However, the responsibility of making the update or undertaking review is not specified.

Due to the lack of clarity on the ownership, a project often progresses without a safety plan in place.

Structure of the Safety Plan

The IEC 61511 [2] does not specify any particular structure to be followed for the safety plan. The standard provides the flexibility of incorporating the safety plan as:

- part of quality plan; or
- a separate document titled ‘SIS Safety Life-cycle Plan’ or
- several documents which may include company procedures and practices.

Is this flexibility good? The main challenges with this flexibility with respect to above mentioned points are:

- If safety plan is part of quality plan, defining accountability of drafting the safety plan as part of the overall quality plan. Further, it poses challenge whether the appropriate stakeholder would be able to trace and use it.
- If safety plan is part of quality plan OR a separate dedicated document, who owns and transfers the document to the appropriate stakeholder of the phase under execution or subsequent phases?
- If safety plan is part of several documents and part of company procedures and practices, how to ensure that these documents are referred and applied for the phase under execution?

A suggested solution to this challenge is to prepare an 'Overall Safety Plan' and also develop a safety plan per phase.

The overall safety plan should be developed by the owner company and provide guidance on the minimum requirements as per the companies requirements and regulatory requirements of the place where the plant is being set up. The overall plan should also include the non-SIS based risk reduction applied in the design of the plant.

The per phase safety plan should be prepared by the respective responsible party. They should detail the requirements for the particular phase only. Where the phase is owned by more than one party, each party should develop the safety plan for their scope of work. For example, the phases 3 and 4 are executed normally by the EPC contractor and the system vendor. The EPC contractor should prepare the plan for the SRS and engineering inputs for SIS design which includes the design of sensors, final elements and functional requirements for logic solver. The system vendor should prepare the plan for the SRS covering the logic solver design which includes the design of its hardware and software.

The owner company should be responsible to ensure that the individual phase plans are aligned to the overall safety plan.

Contents of the Safety Plan

The content of the overall and safety plans per phase can be set up as per the following sections.

- **To identify the activities to be carried out related to Functional Safety.**
  Overall Safety Plan – Identify all phases which need to be carried out and requirements related to these phases which need to be considered in the safety plan. The plan should also include Non-SIS based risk reduction technologies design and criteria for considering those in the overall safety strategy. The overall safety plan should also set the target dates for each life-cycle phase by which activities of each phase should be completed.
  Safety Plan per phase – For each phase, define the objectives, inputs to the activities and the intended outputs of each phase. Further, it should also define whether a particular phase requires design review to be conducted and whether verification of the output needs to be done.
- **To identify the criteria the design should meet.**
  Overall Safety Plan – Identify the documents which are required to be prepared which will specify design criteria for meeting functional and integrity requirements for the SIS.
  Safety Plan per phase – Identify the engineering activities for design of the SIF including its sub-systems based on the SRS. This includes the design of the sensors and initiators,

logic solver and final elements. It also includes requirements for design reviews which should be conducted after completion of each important activity by system vendor such as hardware design, software prototypes and application software. Planning should also include requirements for SIL verification, hardware testing, software prototype testing and application software testing.

- **To identify the techniques, measures and procedures for carrying out the identified activities.**
  Overall Safety Plan – Identify the techniques, measures and procedures to be applied for each phase to conform the design against specified requirements. For example:
  - Specifying one of the technique for hazard analysis to be applied (e.g., safety reviews, HAZOP, FMEA etc)
  - Specifying which SIL assignment method will be used,
  - Specifying the techniques for avoiding random hardware failures, such as use of redundancy.

  Safety Plan per phase – This includes the plan for implementing the techniques and measure which are identified in the overall safety plan. This should include the availability of tools and resources, the personnel who should be involved, and the detailed procedures which would be applied for carrying the work.
- **To identify the persons, departments or organizations who would execute the identified activities.**
  Overall Safety Plan – Identify the requirements of personnel and the competence requirements to carry out each phase. This includes criteria for designers / engineers from the owner organization, EPC contractor, system vendor, third party consultants and assessing agencies.
  For example:
  - Participation from different disciplines (process, instrumentation, HSE, operations) for hazard analysis and SIL assignment.
  - Assigning a competent resource for carrying out SIL verification and design implementation.

  Safety Plan per phase – For each phase, implementation plan for each phase, roles (e.g. design review, testing, inspection etc) and responsibilities (e.g. HAZOP chairman / facilitator, scribe, application developer) of involved personnel, the requirements for their independence (e.g. the design review will be conducted by independent person within organization).

Impact of not having a safety plan or not following the safety plan

Each safety life-cycle phase is important with respect to functional safety. The SIS design builds upon the outcome of one phase as input for other. Hence the success of the project depends on execution of each phase based on a plan. Each facility and plant would be having different requirements based on its location, capacity, nature of process and the feed, owner requirements and risk tolerance criteria, regulatory requirements etc. Hence, the plan should be specifically developed for the plant and should not be a generic plan.

Each of the safety life-cycle activities and the examples of impact for not having a safety plan or not following the safety plan are listed below. This is also shown in the Figure 3.

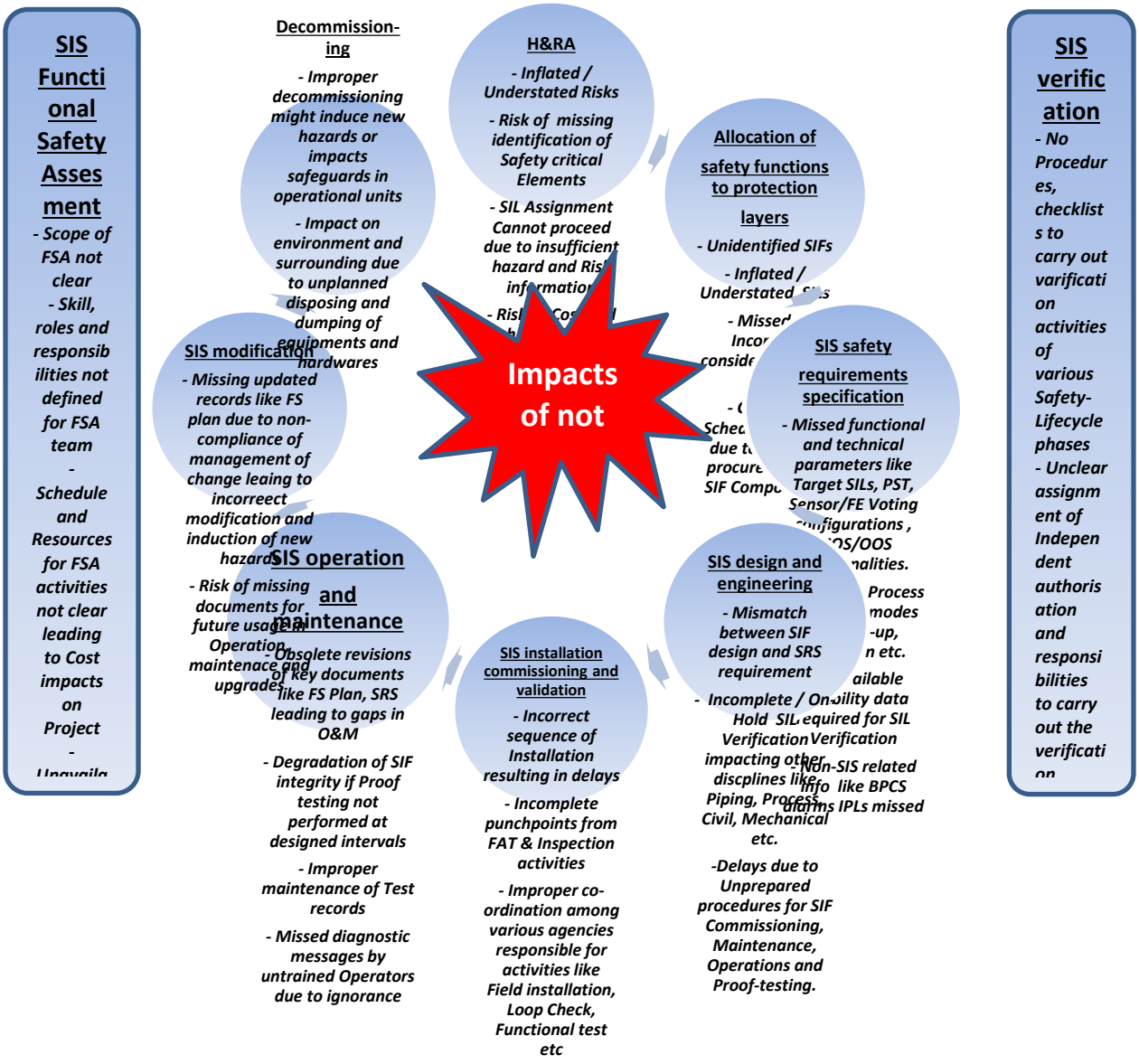

Figure 3. Impact of not having Safety Plan

- **Hazard and Risk Assessment.**
  - Incomplete / Incorrect assessment of hazards.
  - Safety critical elements not properly identified. This means the system design may have insufficient safeguards.
  - Next phase of SIL assignment cannot progress or progresses with insufficient data.
  - Risk to cost and schedule if the hazards surfaces in later stage of engineering.
- **Allocation of Safety Functions to Protection Layers**
  - Unidentified SIFs.
  - Missed / Incorrect credit of IPLs.
  - May delay the procurement of the SIF components impacting the cost and schedule.

- **Safety Requirements Specification for the SIS**
  - Key functional requirement and technical parameters may not be available for the design and engineering phase. For example, if the process safety time is not captured, the valve closing time cannot be determined and the procurement of the valve is delayed.
  - Incomplete SRS may result into failures of the SIS. Based upon the study by the UK Health & Safety Executive on 'Out of Control – Why Control Systems Go Wrong and How to Prevent Failures' [3] the main contributor to the failures is incorrect specification. It contributes to 44% of failures. The components 'Inadequate Functional Requirement Specifications' and 'Inadequate Safety Integrity Requirement Specifications' are 12% and 32% respectively. The result of the failures may be devastating for the plant safety. Further, if the failures reveal a systematic fault during operation phase, it may mean costly repair for modification of the SIS and probable stoppage to the operations.
  - Inputs for the logic solver design may not be complete resulting in delays of the design. For example, if the trip override philosophy is not defined, it would mean change in application software at a late stage in the project.
  - Important parameters for the SIL verification activity may not be adequately captured. This will result into the delays in completing the SIL verification. For e.g. definitions of β common cause failure factor, coverage criteria for proof tests.
  - Non-SIS related requirements may be missed. For example, the operator response to BPCS alarm is taken credit for in SIL assignment. However, if the requirements are not stated in SRS, it may be missed from the BPCS configuration.
- **Design and Engineering of the SIS**
  - SIF design may not completely meet the requirements of SRS.
  - The SIL verification may not be completed and there might be hold points on important aspects such as voting, proof testing etc. For example, if the voting requirements change resulting in increase of the final elements, it not only changes the design of SIS, but also impacts other disciplines such as piping, civil.
  - The procedures for SIF commissioning, maintenance, operations and proof testing may have deficiencies resulting in challenges during those phases. For example, if the proof testing time for meeting the SIL of the SIF is based on the testing at certain frequency, delays in testing means operations with degraded SIL.
- **Installation, Commissioning and Validation**
  - Incorrect sequence of installation may result in delayed commissioning.
  - Improper coordination of the agencies responsible for installation activities of SIF components such as field instruments, logic solver cabinets, field wiring and loop checks.
  - The non-compliances against design requirements are recorded as punch items during FAT or SAT. Some of these punch items may remain unaddressed due to the commissioning schedule pressures. Continuing commissioning with such open items means not having complete safeguarding in place. Further, the validation of the SIS after installation at site cannot be completed.
- **Operation and Maintenance**
  - Before the ownership of the system is transferred from the project to owner operator, key document, such as SRS, should be revised and up-to-date. If this

activity is not explicitly included in the overall safety plan, this step may not be completed. This may delay important operation and maintenance safety function activities from being completed.
    - If the maintenance activities like partial stroke tests or proof test activities are delayed or not performed, the integrity of the SIF may be degraded.
    - If the results of the findings are not compared against the criteria mentioned in SRS, defects/errors in the intended design cannot be ascertained.
    - Possible ignorance to the diagnostics messages generated by SIS means SIS repair is not done in time and may lead to increased spurious trips or no trips on demand.
- **Modification**
    - The SIS modification proceeds without an updated functional safety plan and SRS. This means the scope of the modification is not defined. This might result not only into incorrect execution of the modification, but may also induce newer hazards in to the SIS / process.
    - Risk of not having updated documents will affect the operations and maintenance or any future upgrades or modifications.
- **Decommissioning**
    - Improper decommissioning without complete analysis and effect may introduce new hazards or impact the safeguards for operational units and its SIS.
    - Risk of not having updated documents which affects the operations and maintenance of operational units and any future upgrades / modifications.

Other activities which are conducted in the safety life-cycle which also has impact of not having a safety plan / not following the safety plan are reviewed below:

- **Verification** – A plan for verification of outcome of each phase or important milestones within a phase should be prepared. This plan is necessary to ensure that verification activities are performed to demonstrate that the intended outcome of the activity or phase meets the objectives of the phase. This will also help to ensure that the subsequent phase has the sufficient required information. The verification plan should address the requirements for completing the task in terms of:
    - Required Checklists
    - Personnel who should carry the verification and independence required.
    - How the records of verification will be maintained and who will be responsible for carrying out actions on the findings.
- **Functional Safety Assessment** – The overall functional safety plan should include the requirements for completing Functional Safety Assessment (FSA). The FSA is performed to investigate and arrive at a judgement based on evidence on functionally safety achieved by one or more SIS and protection layers. The requirements of FSA should include:
    - Scope of FSA
    - Skills, responsibilities and authorities of FSA team
    - Personnel who should carry the FSA and independence required.
    - Resources required and
    - Methods for revalidation post modifications.
- **Competence of personnel** – Though part of management of functional safety, a plan should be in place for ensuring the requirements of competence. The requirements of

competence apply to persons, departments and organizations associated with execution of one or more phases of the safety life-cycle.

Conclusions

The effects of failure due to incorrect planning and resultant improper execution may be devastating when it comes to matters of functional safety. The deficiencies in the design may remain hidden for years until an incident happens. The incidents may have serious effects on health, safety and environment as well as production and revenue. There should be a safety plan in place for meeting the functional safety objectives and to demonstrate the compliance to the requirements and standards. Having the approach of having an overall safety plan and safety plan per phase will mitigate the challenges with respect to ownership and the quality of the safety plan.

Not having a safety plan or not executing as per the safety plan means 'Plan to fail'. But to ensure safe operations and to do justice to the investment on functional safety, one of the key deciding factors is to execute all phases as per a properly developed safety plan. This approach would then mean a 'Plan to succeed'; succeed in the goal of achieving the objectives of functional safety.

References

[1] IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.

[2] IEC, IEC 61511, Functional Safety of Instrumented Systems for the Process Industry Sector.

[3] UK Health & Safety Executive – Out of Control – Why Control Systems Go Wrong and How to Prevent Failures [http://www.hse.gov.uk/pubns/books/hsg238.htm].

[4] U.S. Chemical Safety Board [http://www.csb.gov/videos/]

Acknowledgements

We would like to thank P.K. Midha, Control System & Electrical Head of Department, Fluor Daniel India Pvt. Ltd. for his continuous support and motivation in completion of this paper.

We would also like to thank Simon Lucchini, Senior 'fellow', Fluor Canada for his valued guidance on the matter of Functional Safety and being our mentor.