MANGAN
Software Solutions

A Novice's Overview of Safety Lifecycle Manager (SLM®)

SLM®
Safety Lifecycle Manager

www.Mangansoftware.com

Table of Contents

1 Introduction

The Safety Lifecycle Manager® software suite (SLM®) is comprised of 16 software modules that encompass the entire IEC 61511/ISA 84 Safety Lifecycle. Developed and offered by Mangan Software Solutions (MSS), SLM is the foremost software application that provides an enterprise, manufacturing site, or engineering project with the capabilities to execute, manage and fully document Process Safety and the Safety Lifecycle in one integrated database solution. The application provides basic and comprehensive Safety Lifecycle functions as well as an extensive set of optional auxiliary functionalities.

No matter what level of functionality a user requires, SLM offers exceptional value in reducing costs and leveraging benefits for the Safety Lifecycle. While the Safety Lifecycle can be daunting if you are new to the process, or if you are managing what appears to be a difficult and expensive undertaking, SLM is designed as an intuitive, robust, and integrated suite of modules using work processes that provide a rapid path to success for every facet of Process Safety and the Safety Lifecycle.

This White Paper is intended to provide an overview of SLM for novices in the Safety Lifecycle or for managerial personnel who only need to understand the importance of the Safety Lifecycle and be aware of what really needs to be done for each phase of the Safety Lifecycle.

MSS offers a series of White Papers and other support material for those who need a more detailed understanding of the Safety Lifecycle and the usage and capabilities of SLM.

2 The Safety Lifecycle

The Safety Lifecycle grew out of several catastrophic events that happened across a number of industries. There was a realization that organizations around the world were not handling process hazards and their mitigations very well, and as a result calamitous events involving loss of life and massive economic and environmental impacts were occurring. Various industry-standards organizations started looking at what could be done, and a number of standards were developed. Among them are ISA 84, IEC 61508 and IEC 61511. These standards are extensive and complex, but they all come down to a few principals:

- Process hazards need to be identified in a formalized and consistent way.

- The severity and likelihood of process hazards need to be categorized in a formalized and consistent way.
- When the risk posed by a process hazard is deemed to be unacceptably high, mitigations must be identified that reduce the risk to acceptable levels. These may be design requirements for equipment (e.g., design pressure/temperature); instrumented functions,such as alarms, controls, interlocks, and safety shutdowns; or physical protections, such as overpressure protection, dikes and barriers, and mechanical interlocks.
- Mitigations identified must have specific functional requirements defined, which include the expectations that the mitigations will actually function when they are required.
- Mitigations that are installed must be tested and maintained to assure that the expectations for functioning when needed are met.
- Personnel that operate and maintain the processes must be properly trained on the mitigations that have been installed, including operation and maintenance requirements associated with them.
- Performance of mitigations must be monitored and where performance is not meeting expectations, corrective actions must be performed.
- All modifications must be managed through a formalized management of change process.
- Records must be kept of the performance and design expectations for mitigations, testing, demand, fault/failure and periods where the mitigations are disabled, non-functional or bypassed.

Compliance with the above items is not a simple task. It can involve crossing traditional organization boundaries, creating documentation that is hard to maintain and share, and adding operating and maintenance responsibilities on an already stretched staff. The SLM application is designed to eliminate most of this burden and allow Safety Lifecycle Management to be efficiently and effectively integrated into existing organizations.

3 SLM in a Few Words

SLM is based upon a set of ten modules that cover the entire Safety Lifecycle. These functional modules may be licensed together or separately, depending upon a particular users' needs. In conjunction with the functional modules, there are six platform modules that are common to all the SLM safety lifecycle modules and are provided with each SLM installation. Collectively, these six modules are identified as the SLM Atlas™ Platform Modules. The safety lifecycle functionality of these modules is comprehensive and extensive, so only the main functions and features are described in this White Paper. MSS has published a number of additional White Papers and other supporting material to provide more detailed descriptions of SLM modules' functions.

The ten SLM modules for Process Safety and the Safety Lifecycle are:

- **HAZOP Module** - Provides the all new "HAZOP Quick Workflow™" to perform and document results of Hazard and Operability (HAZOP) and other Process Hazard Analysis (PHA) studies. Users can import data from other applications or perform HAZOPs and other PHAs within SLM. This module replaces the former PHA/HAZOP Module.
- **LOPA Module** - Links to selected HAZOP and other PHA cases and documents Layer of Protection Analysis (LOPA) studies and identification of Independent Protection Layers (IPL). IPLs identified by LOPAs may be directly linked to actual site assets that are used to implement the functions.
- **Bowtie / Barrier Assurance Module** - Incorporates existing hazard analysis data to facilitate risk analysis and risk assessments on mitigation and prevention barriers.
- **Instrumented Systems Module** - Documents instrumented functions and devices used to implement IPLs.
- **Non-Instrumented Systems Module** - Documents non-instrument assets used to implement IPLs.
- **Relief Systems Modules** - Documents relief systems and devices used to implement overpressure prevention IPLs.
- **Operate and Maintain (O&M) Module** - Allows users to enter events for a wide number of types of IPL functions and their devices. Reports on Safety Lifecycle performance metrics such as Test History, Demands, Failures, Bypasses, and Service Status. The O&M Module presents performance data based upon entered events.
- **Functional Safety Assessment (FSA) Module** - Allows users to conduct and document Functional Safety Assessments required for Safety Instrumented Systems.
- **Action Item Tracker** - Provides a means for users to define and track action items within SLM. Action items created in other modules, such as the FSA and MOC modules, are linked to this module.
- **Management of Change (MOC) Module** - Provides a means for users to generate, approve and track MOCs within SLM. The module provides checklists for MOC generation and hazard assessments. Users may create action items within the MOC Module, which are then linked to the Action Item Tracker Module.

The six SLM Atlas™ Platform Modules are:

- **Home Dashboard Module** - Users can tailor their dashboard from over 150 reports, data views, and KPIs throughout SLM using drag and drop creation methods. Users can access recent items, quick links, bookmarks, and available modules, plus globally search the SLM database.
- **Global Module** - Allows users to define overall enterprise and site organization and Safety Lifecycle policies.
- **Personnel Module** - Allows administrators to document individual roles and qualifications and to define functions such as event approval scope for individual users.

- **Document Management System Module** - Every object in SLM can have associated documents. Document management tools provide searches of PDF documents, configurable mapping and ranking of documents, remote linking of documents via URLs, and tracking of document versions and external revisions.
- **System Configuration Module** - Allows administrators to manage SLM users and the data which they can view, change, create or delete and manage general system wide functions.
- **Import Adapter** - Allows users to define and store import templates for standard CSV data import files. Adapters are also available for common data import formats, as well as a data mapping tool to allow users to map data fields to object fields from an import file.

4 How SLM is Used

SLM is a web-based application. The application and its database are offered as 'software as a service' (SaaS) or installed on a host server at user organization's site or enterprise location. SLM SaaS may be a commercial server or virtual server, available through MSS or a third party. An important factor is that the SLM application can be available to authorized users without requiring any local installations. SLM contains cyber security functions that meet typical corporate requirements.

SLM is intended to be used by multiple organizations within an enterprise or facility. When SLM is set up, the organization is defined in terms of the enterprise, sites within the enterprise, and units within sites. Data is generally recorded at the unit level, which can include alarms, alarm groups, Basic Process Control Systems (BPCS), F&GF , interlocks, Safety Instrumented Functions (SIF), Safety Instrumented Systems (SIS), cause and effect (C&E) matrices, and high integrity protection system (HIPS) objects. MSS can customize the entire enterprise structure to meet a user organization's requirements.

Many portions of SLM are customizable. This includes setting up user roles, defining the contents of dropdown and pull-down lists, checklists, and other readily modified data. SLM may also be further customized to match a user's specific requirements. This level of customization requires modification of the SLM code and is available as a service from MSS. The White Paper *Getting Ready to Use SLM* describes the things that need to be considered when first setting up an SLM installation.

SLM is licensed by the module or in sets of modules, but modules not selected at the initial installation can be added at later dates. The decision to exclude some modules will not affect the functionality of other modules.

5 SLM for the Process Safety Management Organization

The primary SLM modules that a process safety management organization will use are the HAZOP and LOPA Modules. These modules may be used in a variety of ways depending on the organization's requirements, including:

- Importing of existing HAZOP and LOPA data into SLM from other applications, spreadsheets, etc.
- Performing HAZOPs and LOPAs directly in SLM. Once existing data has been imported, subsequent HAZOPs and LOPAs can be performed within SLM.
- Managing multiple parallel HAZOPs and LOPAs such as those originating from capital projects and Management of Change hazard assessments associated with site executed work.

SLM uses a Dynamic Risk Matrix to allow process safety management organizations to easily understand where in the enterprise that risk is concentrated. When used with the O&M Module, the current status of risk incurred by the performance and testing statuses of the protective functions implemented in each site and unit is recorded and viewable.

6 SLM for Engineering Organizations

The primary modules that an engineering organization will use are the Instrumented Systems, Non-Instrumented Systems, and Relief Systems Modules. Depending upon a particular organization's needs, the engineering organization may also use the SLM Functional Safety Assessment Module.

The first three modules are used to capture the existence of plant assets that are used to implement Safety Functions identified by PHAs, including HAZOPs and LOPAs. Examples of plant assets for Safety Functions include:

- Safety Instrumented Systems (SIS)
- Safety Instrumented Functions (SIF)
- Alarms associated with LOPA IPLs
- BPCS functions associated with LOPA IPLs
- Non-SIF interlocks, trips, etc. associated with LOPA IPLs
- Non-Instrumented IPLs such as mechanical stops, dikes, etc.
- Relief Systems and relief devices

Each function may then have Input and Output (I/O) assets associated with the function. These are organized to allow users to specify voting groups such as 2oo3, 2oo2, etc. SLM also uses the voting group definitions to compute the function's Probability of Failure on Demand (PFD) using a variety of failure rate sources. Basic functional requirements for I/O assets such as accuracy, response time, user defined failure rates, etc., may be captured in SLM. Detailed device data is specified under devices in the O&M Module.

SLM allows the user to link specific PHA, HAZOP, and LOPA scenarios with the plant assets identified in the engineering modules. This allows the user to easily access the process hazards that require the function to be in place and identify all of the plant assets associated with a specific scenario.

SLM also allows the user to easily specify Safety Requirements Specifications (SRS) for SISes. Each SIS object contains all the data fields required to develop an SRS that complies with IEC 61511 and ISA-84 requirements.

Once a set of functions and their I/O assets are defined, SLM allows authorized users to clone all or part of data sets to create a new object. Similar SISes, SIFs and I/O assets can be copied and then edited for the specific application. This minimizes the work required to create new SISes, SRSs, SIFs and IPLs and enforces consistency in format and content.

Engineering groups also will use the SLM O&M Module to monitor and report on the performance of SISes, SIFs and other IPLs. The O&M Module provides reports and displays that identify the following:

- Testing status, upcoming or overdue testing
- Demand, bypass, and fault/failure statistics for all functions and devices
- In-Service failure rate data for devices. This data is available by device ID, device type and device generic models. The In-Service failure rate data is also available to the Instrumented Systems Module to calculate SIF or other IPL In-Service PFD values.

During initial design and subsequent operation and/or modifications, the ISA and IEC standards require performance of FSAs. The SLM FSA Module allows users to create FSAs for SISes at each of the stages identified by the standards. The FSAs use a standardized set of checklists to assure completeness and consistency across an enterprise.

7 SLM for Operations

Operations groups may use SLM to better understand the protective functions for which they are responsible and to record operation related events in the O&M Module. They also use the O&M Module to understand the performance of the protective functions in their area and to record operations related events.

Operations personnel such as supervisors, process engineers and operators may be allowed to have view only rights to the process safety modules (HAZOP and LOPA) and engineering modules (Instrumented Systems, Non-Instrumented Systems, and Relief Systems). This allows operations personnel ready access to what the protective functions do, why they exist, and what equipment is associated with the protective functions. For example, an operator may view the data for a SIF and then be able to access the LOPA for that SIF in order to understand what a function does, what field devices are part of the function, and the hazards the function protects against.

The O&M Module allows operators and/or supervisors to directly enter operations related events. These events include:

- Demands upon SIFs or other IPLs, what devices were associated with the event, and whether the function responded to the demand as expected or not.
- Faults and failures associated with SIFs or other IPLs and their devices.
- SIF or other IPL bypasses. This includes requests for bypass approval including hazard assessments and supplementary operations procedures, the date and time the bypass was initiated and the date and time the bypass was removed, and the function restored to normal operation.

SLM provides operations personnel with performance data associated with protective functions.

Users are informed as testing becomes due or is overdue and of function performance, such as demands, failures, and bypass time.

The operating company was able to efficiently gather and analyze Tier 3 metrics for each IPL including:

8 SLM for Maintenance

Maintenance groups use SLM in a manner similar to operations groups. This includes having the same view level access to engineering and Process Safety information for the units and functions within their areas of responsibility. The maintenance groups will also use the O&M Module to monitor, schedule, and record maintenance activity. These functions include:

- Monitoring the test status for SIS, SIF and other IPL functions and identifying upcoming or overdue testing.
- Recording test results for functions and their devices.
- Recording maintenance events that occur between testing events.

- Recording replacement of devices, which may be an engineering activity depending upon an organization's practices.
- Recording changes in the Service Status of SISs, SIFs or other IPLs and their devices, which may be an engineering activity depending upon an organization's practices.

9 SLM for Management

SLM provides tools for management at various levels to monitor Process Safety at the unit, site, and enterprise levels. Among the reports and views available are:

- Dynamic Risk Matrix views that identify relative risk by unit, site and enterprise level.
- Protective function performance summaries that identify areas that have overdue testing, high demands or excessive bypassing.
- Tools that support identification of qualifications, roles, and responsibilities for individuals within an organization.

10 SLM Administration

SLM provides tools for overall user and application data management in the System Configuration and Global Modules. These include:

- Management of User IDs and the scope of view or modification of data. Users may be granted view or modification rights for specific units, one or more sites or the enterprise.
- Management of drop down and pull-down lists, checklist items, or other general data used by the modules.
- Management of approval policies for events including identification of approvers by event type, site, or unit.
- Management of enterprise-wide generic models and which sites use which generic models.

11 Conclusions

Mangan Software Solutions engineered SLM as a single platform solution for the complete Safety Lifecycle. SLM is the world's first and only TÜV certified process safety intelligence platform. It is comprised of a core set of modules used to configure and manage the system across the entire enterprise and a comprehensive set of interconnected application modules covering the entire Process Safety and Functional Safety Lifecycle.

Users can configure and manage custom user interface logos, font styling, units of measure, language translation, usage metrics, API interfaces, and data objects. The process and functional safety modules are designed and integrated to be extensible, so data can be stored and managed within a common framework, but which can be customized to suit any enterprise's requirements.

From HAZOP and LOPA studies, to SIS design, and through operations and maintenance, SLM has all the tools needed to successfully manage Process Safety and the Safety Lifecycle. Users can collect, record, and quickly access current and historical data used to manage the performance of Protective Functions. SLM is an enterprise ready solution that maximizes the effectiveness and minimizes costs for successfully performing Process Safety and the Safety Lifecycle.