Managing Bypasses Using Safety Lifecycle Manager (SLM®)

Safety Lifecycle Manager

Conformance to IEC61511

MANGAN Software Solutions

Managing Bypasses Using Safety Lifecycle Manager (SLM)

IEC-61508 & IEC 61511 Certified

SLM® Safety Lifecycle Manager

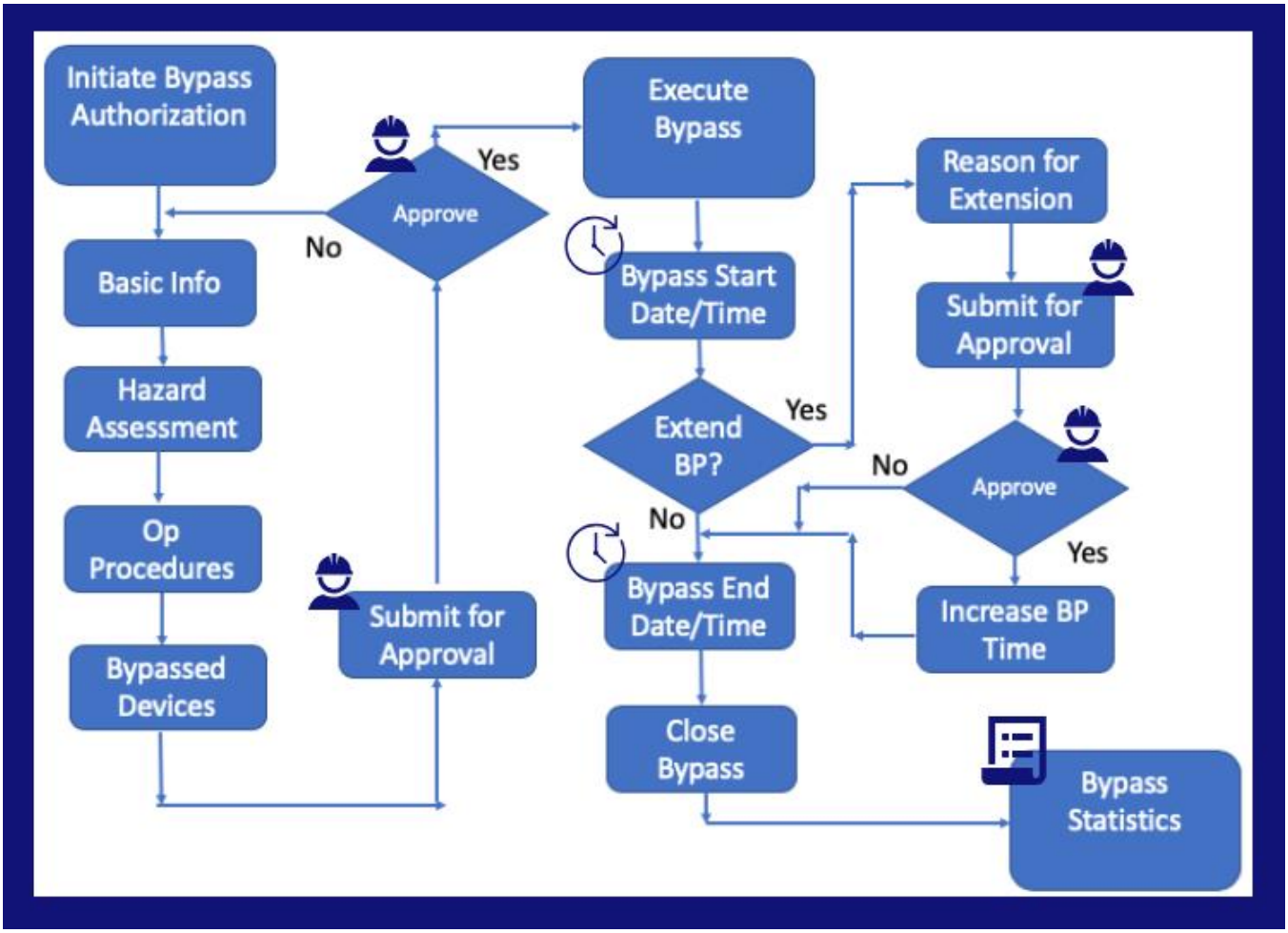
www.Mangansoftware.com

IEC 61511 Part 1, contains extensive discussions of the design and operating procedures for Safety Instrumented Function (SIF) bypasses. Clause 16.2 describes operational requirements such as:

- Performing a hazard analysis prior to initiating a bypass
- Having operational procedures in place for when a protective function has been bypassed
- Logging of all bypasses

SLM provides a robust Bypass management and logging function that meets all of the requirements of IEC-61511 and integrates with the performance analysis and reporting functions of the SLM Operate-Maintain Module. SLM Operate-Maintain Module uses the Bypass Authorization object and Work Flow to initiate, approve and record the execution of Protective Function Bypasses. SLM does not limit the use of Bypasses to just SIF's. In SLM, any protective function may have a Bypass Authorization associated with it.

The figure below illustrates how the Work Flow supports the tasks required:



A Bypass Authorization is initiated by any authorized SLM User. In practice this will usually be a member of the Operations Staff for a Unit, often a shift foreman or Operations Engineer. The originator is guided to enter the information required to support the Bypass Authorization. This includes:

- Basic Bypass Information such as the reason for the Bypass, the anticipated start date and time and the maximum time which the Protective Function is to be Bypassed
- Hazard Assessment information – this includes an identification and assessment of the potential severity of hazards that may occur while the Protective Function is Bypassed and the corrective measures that should be taken if the hazard occurs
- Operation Procedures that are required to be used to mitigate potential hazards that may occur while the Protective Function is Bypassed
- Identification of the Devices associated with the Protective Function that will be Bypassed

Once this information is provided, the User then may submit the Bypass Authorization for Approval. The Bypass Authorization is submitted to the designated Approver, typically an Operations Supervisor of Manager. The Approver reviews the Bypass Authorization and either Approves or Disapproves the request.

Once the Bypass Authorization is Approved, the Operations team may execute the Bypass as planned. The originator or other authorized User may then record the start date and time of the Bypass in the Bypass Authorization. If a Bypass is expected to exceed the time requested in the original Bypass Authorization submittal, the User may request approval for a Bypass Extension by filling in the data in the Bypass extension section of the Bypass Authorization object. When approved, this will update the authorized Bypass time and prevent the Bypass from being reported as exceeding its authorized time.

When the Bypass is completed, the originator or other authorized User then enters the date and time when the Protective Function is returned to service and then close the Bypass Authorization. Closing of the Bypass Authorization results in the Bypass data being added to the SLM Events that are used to analyze Protective Function and Device performance.

SLM contains performance views that capture all Bypasses for a Function, Unit and Site. The analysis functions include reporting on the number of bypasses, time in bypass and identification of Bypass Events that exceeded the authorized bypass time. SLM will also compute the effect of Bypasses on a Protective Function's in-service performance, such as computing the in-service reduction in the Functions' RRF or PFD. Functions that have excessive Bypasses will also show up on the Unit and Site bad actors lists.