How to Verify and Validate a Safety System Design
By: Wayne Solberg, Global OEM Technical Consultant, Certified Functional Safety Professional, Rockwell Automation

Using a rigorous safety LifeCycle™ approach, manufacturers and machine builders can harness the inherent value of intelligent safety system designs to help drive productivity, reduce labor costs and increase the bottom line.

The LifeCycle approach, as defined in standards IEC 61508 and IEC 62061, provides the foundation for this detailed, more systematic design process for machinery applications. It is based on integrating the safety and machine functions early in the design process.

Among the most important phases are the final ones – verifying and validating the performance of a safety system design. By this point, the designer already has completed the initial phases – that is, conducted a risk or hazard assessment, defined the functional requirements of the machine and begun designing the safety system.

Verifying the performance of the safety system design means to prove the circuit for the safety functions of the machine is working properly and meets the specified requirements. During verification, engineers and electricians test the safety system to make sure it is working while the machine is
running. For example, activating an emergency stop (e-stop) to test that the machine will indeed stop running completes the verification step for an e-stop application.

Next, completing the validation step means testing that the safety functions of the system do what they are designed to do. For example, in a dual-channel e-stop application using redundant control relays, a designer conducting the test might inject a human fault between the logic solver and output on channel one -- activating the e-stop -- to validate that the wiring is correct on channel one from the input to the logic solver. The designer would then repeat the process on the second channel to make sure it is functioning as planned.

To validate a light curtain application, for example, a designer conducting the test would validate the stop time by verifying the safe distance calculations to help ensure the light curtain is at the appropriate distance from the machine. Validation takes place at a machine builder's facility, and at an end user’s facility to help make sure the safety-related control system functions correctly during installation, start up and set up of that machine.

Ultimately, designers must remember that verification is different from validation. Validating the safety functions of a system requires a plan, must be documented and should include environmental, operational, and maintenance tasks and functions. Validation proves the safety circuit works correctly. It requires fault injection in all identified modes of operation. It also requires circuit evaluation using analytical tools to verify circuit design compliance, component selection verification and systematic analysis.

Verification and validation of a safety system must be in accordance with global functional safety standards. A designer must validate the safety system in accordance with IEC 61508, IEC 62061, EN ISO 13849-1 and 13849-2. Each standard provides a unique definition of validation, as follows:

Validation according to IEC 61508 and IEC 62061 means examining and testing the safety-related electrical control system, including hardware and software, to ensure it achieves the functional safety requirements of the specific application. The standards require the validation has a documented plan comprising the following:

- Details of when the validation shall take place
- Identification of the relevant modes of operation of the machine (e.g., normal operation, setting)
- Acceptance criteria (e.g., what is acceptable as a pass or fail form of validation)
- Corrective actions to be taken in the event of failure to meet the acceptance criteria to re-validate the system

Validation according to EN ISO 13849-1/2 also entails a planned, documented process. It uses static and dynamic testing, among other methodologies, to show that all safety-related parts of the control systems interact correctly to perform the intended safety function – and that unintended functions do not occur. Descriptions of safety functions and requirements of specified performance levels and categories are found in EN 954-1.

All safety functions, including any protection methods, circuits and components that mitigate identified hazards, need to be working correctly to be validated. This includes validation of software,
environmental and maintenance requirements, and general tools that can be used for mechanical, pneumatic, hydraulic and electrical systems. EN ISO 13849-2 also specifies the conditions under which the validation by testing of the safety-related parts of the control systems should be carried out.

In addition, validation must demonstrate that each safety-related part and control system meets the requirements of EN ISO 13849-1, including the specified performance level, category, and measures for control and avoidance of systematic failures.

Verifying and validating the safety-related control systems in accordance with the Safety LifeCycle approach helps a machine builder ensure a seamless installation, start up and set up of the machine at the end user’s facility. The end user can be confident it is receiving a machine with safety systems in compliance with today’s standards.

To learn more about this specific topic, please view our archived webinar at: http://discoverrockwellautomation.com/SA_EN_Functional_Safety_Webinar_Slides.aspx.

Learn more about contemporary, integrated safety configurations, global standards, and how users are employing safety automation in their organizations by contacting your local Allen-Bradley distributor, or by visiting the Rockwell Automation Safety portal. (http://discover.rockwellautomation.com/safety).

LifeCycle is a trademark of Rockwell Automation, Inc.