

**NOTE** — This example is used with permission from AIChE, CCPS, *Guidelines for Safe Automation of Chemical Processes*, New York, 1993, available from: AIChE, 345 East 47th Street, New York, NY 10017, Tel: (212) 705-7657; and Process Industry Practices (PIP), *Safety Instrumented Systems Guidelines*, available from: Process Industry Practices (PIP), 3925 West Braker Lane (R4500), Austin, TX 78759, Tel: (512) 232-3041, www.PIP.org. The example is modified to meet ANSI/ISA 84.00.01-2004 (IEC 61511 Mod) requirements. This example was chosen to facilitate understanding of SIS application as it progressed from CCPS Guidelines dated 1993 to ANSI/ISA S84.01-1996, to ANSI/ISA 84.00.00.01-2004 (IEC 61511 Mod). This example was also used in Appendix B of AIChE, CCPS, *Layer of Protection Analysis, Simplified Process Risk Assessment*, 2001.

## 1 Introduction

Used in conjunction with ISA-TR84.00.04-2005 Part 1, the example set forth in this technical report is provided to illustrate how to apply ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511Mod). It is intended to demonstrate one method to meet the requirements of the standards. The reader should be aware that ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Mod) is performance based, and that many approaches can be used to achieve compliance. Some of the methods applied in this example include: what-if and HAZOP techniques for hazard and risk analysis, LOPA for allocation of safety functions to protection layers, fault tree analysis for SIL verification, and ladder logic to document the application software requirements. Other techniques and tools could be utilized at each of these steps in the safety lifecycle to meet the requirements of the standards.

**NOTE** — Throughout this technical report, the term “ISA-84.01-2004” is used to refer to ANSI/ISA-84.00.01-2004 Parts 1-3 (IEC 61511 Mod).

The example utilizes the similar chemical process presented in AIChE CCPS, *Guidelines for Safe Automation of Process Applications*, 1993, and in PIP PCESS001 1999, *Safety Instrumented Systems Guidelines*.

The safety lifecycle application in the CCPS version was based on the initial version of IEC 61508. The safety lifecycle application in the PIP version was based on ANSI/ISA-S84.01-1996. The safety lifecycle example herein is based on ISA-84.01-2004. As a result, the evolution of new design requirements can be assessed by comparing this example with previous versions.

This example selects a subsystem of a process and applies to it the design philosophy, procedures, techniques, and verification methodology discussed in ISA-84.01-2004.

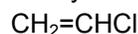
This example shows cradle-to-grave documentation for each SIF. This documentation pedigree gives auditors and plant personnel the means to track the SIF through the safety lifecycle phases back to the process hazards analysis (PHA) that created it. Each SIF is clearly identified in each document to facilitate tracking between lifecycle phases. A vital part of safety is the ability to demonstrate to others (e.g., auditors, regulators, insurance companies) that the risk reduction provided by each SIF is adequate.

*This example does not represent a complete design for a polymerization process because of the extensive detail that is required to achieve a high-integrity, safely automated design. As a result, this example includes a number of simplifications.*

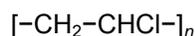
All references shown refer to information within this example unless otherwise noted.

## 2 Project Definition

The process is the polymerization of vinyl chloride monomer (VCM),



to make polyvinyl chloride (PVC),



The example involves a hazardous reactant, VCM, which is flammable and has toxic combustion products, as well as being a known carcinogen. The process also illustrates a larger-scale batch operation that operates in a semi-continuous manner during an approximately 10-hour period while the polymerization progresses. A simplified description of the process steps is also provided.

## 2.1 Conceptual Planning

Once a business decision is made to consider producing a certain product—in this example, polyvinyl chloride—the initial project team is assembled. This team will start by evaluating potential process routes to identify a technology that will satisfy production needs while meeting responsibilities for health, safety, and protection of the environment.

## 2.2 Process Hazards Analysis

In the very early stages of process evaluation and project definition, a process hazards analysis team (in this example, P.H.A. Smith, Process Jones, S. Bulk, V. May, R. Brown, W. Burk, A.C. Green) starts to interact closely with the designers. For projects handling hazardous materials, the team will include not only process design engineers but also health and safety specialists. The team will often need to have access to other specialists—such as chemists, operating personnel, consultants or engineering contractors having experience with the same or similar processes, and process licensors. In this example, a well-proven process is available as a starting point. Therefore, we will proceed with the business decision to produce this product, and concentrate on the aspects of the design process that influence or directly involve the design of the process control systems and safety interlock systems. More detailed information on related aspects of the design process can be found in the following list of texts from the Center for Chemical Process Safety, American Institute of Chemical Engineers:

- *Guidelines for Hazard Evaluation Procedures*
- *Guidelines for Chemical Process Quantitative Risk Analysis*
- *Guidelines for Safe Storage and Handling of High Toxic Hazard Material*
- *Guidelines for Vapor Release Mitigation*
- *Guidelines for the Technical Management of Chemical Process Safety.*

## 3 Simplified Process Description

The manufacture of PVC from the monomer is relatively straightforward. The heart of the process is the reactor vessel in which the polymerization takes place over a period of about ten hours, while the reactor contents are agitated mechanically and the heat of reaction is removed by the circulation of cooling water through the reactor jacket. Because the process involves the charging of a batch to the reactor, process systems are designed with multiple reactor units in parallel, so that the process can operate on a semi-continuous basis. For simplicity, this example will focus on one of the units, recognizing that a real production facility will typically have several parallel units operating in sequence.