



Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

TECHNICAL REPORT

ISA-TR84.00.04-2005 Part 2

Example Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)

Approved 1 December 2005

NOTICE OF COPYRIGHT

This is a copyright document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in ISA's license to that person.

It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.



Documents
Document Sharing Hub

ISA-TR84.00.04-2005 Part 2 --
Example Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)

ISBN: 1-55617-980-4

Copyright © 2005 by ISA. All rights reserved. Not for resale. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of the Publisher.

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, North Carolina 27709

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR84.00.04-2005 Part 2.

This document has been prepared as part of the service of ISA toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices, and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE DOCUMENT, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE DOCUMENT OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.

EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS DOCUMENT, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE DOCUMENT MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE DOCUMENT. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE DOCUMENT OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE DOCUMENT FOR THE USER'S INTENDED APPLICATION.

HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.

THE USER OF THIS DOCUMENT SHOULD BE AWARE THAT THIS DOCUMENT MAY BE IMPACTED BY ELECTRONIC SECURITY ISSUES. THE COMMITTEE HAS NOT YET ADDRESSED THE POTENTIAL ISSUES IN THIS VERSION.

This ISA technical report was prepared by ISA-SP84 Working Group 2, which included the following members:

NAME

A. Summers, *ISA-SP84 WG2 Leader*
 W. Johnson, *ISA-SP84 Chair*
 V. Maggioli, *ISA-SP84 Managing Director*
 R. Dunn, *ISA-SP84 Recorder*
 R. Adamski
 H. Bezecny
 D. Bolland
 K. Bond
 S. Brown
 N. Cammy
 J. Campbell
 W. Cohen
 A. Dowell, III
 K. Gandhi
 W. Goble
 D. Green
 P. Gruhn
 J. Harris
 W. Hearn
 T. Jackson
 K. Klein
 M. Lang
 T. Layer
 N. McLeod
 E. Marszal
 R. Nelson
 D. Novak
 T. Ostrowski
 W. Owen
 G. Ramachandran
 G. Robertson
 L. Robison
 S. Shah
 J. Siebert
 B. Smith
 C. Sossman
 P. Stavrianidis
 H. Storey
 R. Strube
 L. Suttinger
 K. Szafron
 R. Szanyi
 R. Taubert
 H. Thomas
 A. Woltman
 D. Zetterberg

COMPANY

SIS-TECH Solutions LLC
 E.I. Du Pont
 Feltronics Corp.
 DuPont Engineering
 Premier Consulting Services
 Dow Deutschland
 ExxonMobil Research & Engineering Co.
 Consultant
 Health & Safety Executive (HSE), UK
 UOP LLC
 ConocoPhillips
 KBR
 Rohm and Haas Co.
 KBR
 Exida Com LLC
 Rohm & Haas Company
 ICS Triplex
 UOP LLC
 Westinghouse Savannah River Co.
 Bechtel Corp.
 Solutia, Inc.
 CF Industries
 Emerson Process Management
 Arkema
 Kenexis
 Celanese Corp.
 BASF Corp.
 Oxychem
 Chevron Research & Technology Co.
 Motiva Enterprises LLC
 Oxy Information Technology
 BP Oil
 Exxon Mobil Chemical Co.
 Invista
 Nova Chemicals
 Washington Safety Management Solutions LLC
 FM Approvals
 Shell Global Solutions
 Intertek Testing Services NA, Inc.
 Westinghouse Savannah River Co.
 BP
 ExxonMobil Research Engineering
 BASF Corp
 Air Products & Chemicals Inc
 Shell Global Solutions
 Chevron Energy Technology Co.

This ISA technical report was approved for publication by the ISA Standards and Practices Board on 1 December 2005:

NAME	COMPANY
I. Verhappen, President	Syncrude Canada, Ltd.
F. Amir	E I Du Pont Co.
D. Bishop	Consultant
M. Coppler	Ametek Inc.
B. Dumortier	Schneider Electric
W. Holland	Consultant
E. Icayan	ACES Inc.
A. Iverson	Ivy Optiks
R. Jones	Consultant
K. P. Lindner	Endress + Hauser Process Solutions
V. Maggioli	Feltronics Corp.
T. McAviney	Jacobs Engineering Group
A. McCauley	Chagrin Valley Controls Inc.
G. McFarland	Emerson Process Management
R. Reimer	Rockwell Automation
J. Rennie	Consultant
N. Sands	E I Du Pont Co.
H. Sasajima	Yamatake Corp.
T. Schnaare	Rosemount Inc.
A. Summers	SIS-TECH Solutions LLC
J. Tatera	Tatera & Associates
R. Webb	Consultant
W. Weidman	Parsons Energy and Chemicals
J. Weiss	KEMA Inc.
M. Widmeyer	Stanford Linear Accelerator Center
C. Williams	Eastman Kodak Co.
M. Zielinski	Emerson Process Management

This page intentionally left blank.

CONTENTS

1	Introduction.....	9
2	Project Definition.....	9
2.1	Conceptual Planning	10
2.2	Process Hazards Analysis	10
3	Simplified Process Description	10
4	Preliminary Design	12
5	ISA-84.01-2004 Application	12
5.1	Step 1: Hazard & Risk Assessment	16
5.2	Step 2: Allocation of Safety Functions	28
5.3	Step 3: SIS Safety Requirements Specifications.....	32
5.4	Step 4: SIS Design and Engineering.....	52
5.5	Step 5: SIS Installation, Commissioning, Validation	63
5.6	Step 6: SIS Operation and Maintenance.....	78
5.7	Step 7: SIS Modification.....	80
5.8	Step 8: SIS Decommissioning	81
5.9	Step 9: SIS Verification	81
5.10	Step 10: Management of Functional Safety and SIS Functional Safety Assessment	82

This page intentionally left blank.

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.

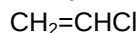
This example shows cradle-to-grave documentation for each SIF. This documentation pedigree gives auditors and plant personnel the means to track the SIF through the safety lifecycle phases back to the process hazards analysis (PHA) that created it. Each SIF is clearly identified in each document to facilitate 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.

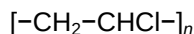
All references shown refer to information within this example unless otherwise noted.

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.

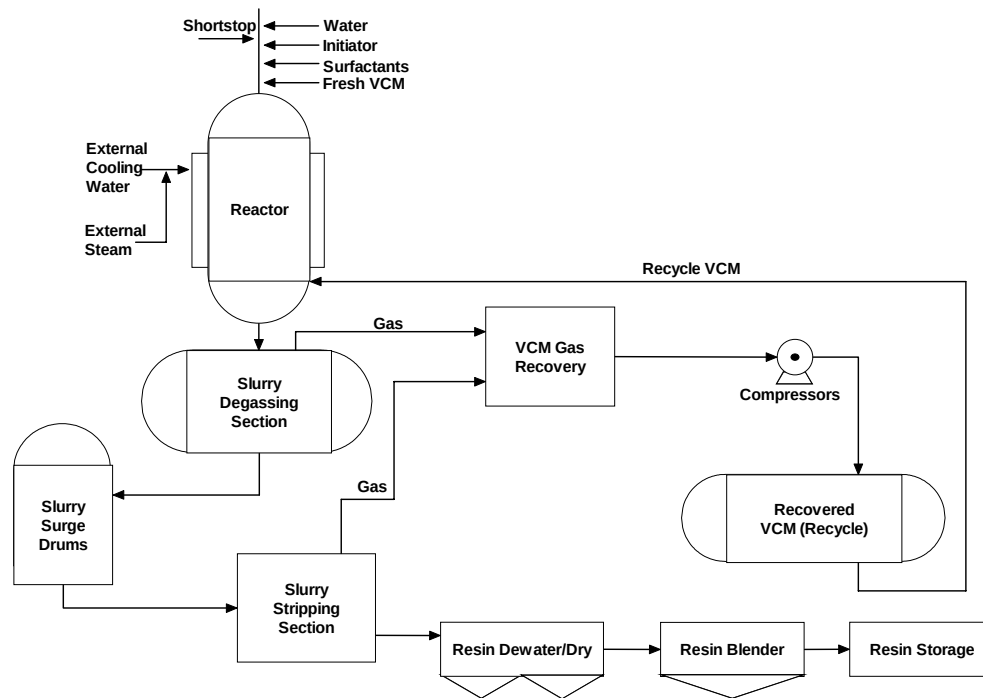


Figure 1– Simplified flow diagram: the PVC process

Figure 1 is a simplified process flow diagram for a typical PVC manufacturing facility. If the reactor vessel has been opened for maintenance after the last batch was processed and dumped, it must first be evacuated to remove any residual air (oxygen) in the vapor space, to minimize the oxidation reaction of monomer which produces HCl and may lead to stress corrosion damage to the reactor vessel as well as to poor product quality. Otherwise, the first step is to treat the reactor vessel with anti-foulant solution to prevent polymerization on the reactor walls. This is followed by charging the vessel with de-mineralized water and surfactants.

Then, the liquid vinyl chloride monomer (VCM) charge is added at its vapor pressure (about 56 psig at 70°F).

The reaction initiator is a peroxide that is dissolved in a solvent. Since it is fairly active, it is stored at cold temperatures in a special bunker. Small quantities are removed for daily use in the process and are kept in a freezer. It is first introduced into a small charge pot associated with the reactor to assure that only the correct quantity is added.

After the reaction initiator is introduced, steam-heated water is applied to the reactor jacket to raise the temperature to about 130 to 140 °F (depending on the batch recipe for the particular grade of product), where the reaction will proceed at a satisfactory rate. Agitation is necessary to suspend the VCM in the water (control particle size), improve heat transfer throughout the batch, and produce a uniform product. Since the reaction is exothermic, cooling water is then circulated through the vessel jacket to control the reactor temperature. Reactor conditions are controlled carefully during the approximately eight hours required for completion of the polymerization.

The reaction is completed when the reactor pressure decreases, signaling that most of the monomer has reacted. Reacted polymer is dumped from the reactor and sent to downstream process units for residual VCM recovery, stripping, dewatering, and drying.

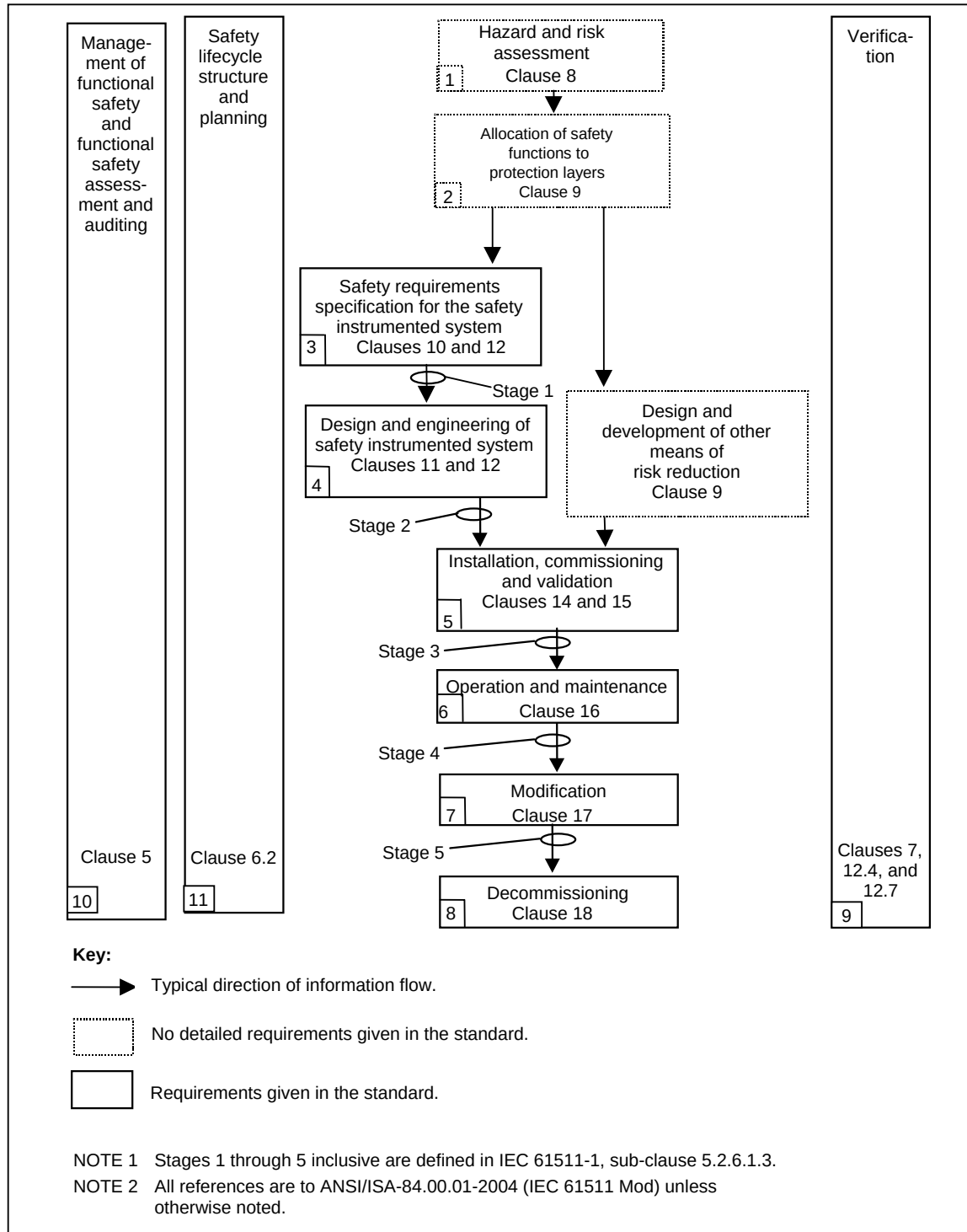
4 Preliminary Design

All special local requirements are reviewed, applicable regulations are identified, and general risk guidelines are established. Utility requirements (e.g., air, cooling water, electrical power) are reviewed and confirmed to be adequate for the application.

5 ISA-84.01-2004 Application

When the preliminary planning is complete (see clauses 1 through 3 inclusive), the implementation of ISA-84.01-2004 is begun.

For this example the design strategy is to initialize the lifecycle design (Figure 2) and break down the lifecycle phases into ten steps consistent with Figure 2 and Table 1 (safety lifecycle overview). At this point in the project, it may be beneficial to use the lifecycle table to assign responsibility for each lifecycle phase as shown in Table 1.



IEC 3247/02

Figure 2 – SIS safety lifecycle phases and functional safety assessment stages

Table 1 – SIS safety lifecycle overview

Safety lifecycle phase or activity		Objectives	Requirements Clause or Subclause of ISA-84.01-2004	Inputs	Outputs	Responsibility
Fig. 2 Box #	Title					
1	Hazard and risk assessment	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	8	Process design, layout, manning arrangements, safety targets	A description of the hazards, of the required safety function(s) and of the associated risk reduction	PHA Team Clause 2.2
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each safety instrumented function, the associated safety integrity level		A description of the required safety instrumented function(s) and associated safety integrity requirements	Description of allocation of safety requirements (see Clause 9 of ISA-84.01-2004)	PHA Team Clause 2.2
3	SIS safety requirements specification	To specify the requirements for each SIS, in terms of the required safety instrumented functions and their associated safety integrity, in order to achieve the required functional safety	10	Description of allocation of safety requirements (see clause 9 of ISA-84.01-2004)	SIS safety requirements; software safety requirements	E & I Team
4	SIS design and engineering	To design the SIS to meet the requirements for safety instrumented functions and safety integrity	11 and 12.4	SIS safety requirements; Software safety requirements	Design of the SIS in conformance with the SIS safety requirements; planning for the SIS integration test	E & I Team
5	SIS installation, commissioning and validation	To integrate and test the SIS; To validate that the SIS meets in all respects the requirements for safety in terms of the required safety instrumented functions and the required safety integrity	12.3, 14, 15	SIS design; SIS integration test plan; SIS safety requirements; Plan for the safety validation of the SIS	Fully functioning SIS in conformance with the SIS design results of SIS integration tests; Results of the installation, commissioning and validation activities	Construction
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	16	SIS requirements; SIS design; Plan for SIS operation and maintenance	Results of the operation and maintenance activities	Operations

Safety lifecycle phase or activity		Objectives	Requirements Clause or Subclause of ISA-84.01-2004	Inputs	Outputs	Responsibility
Fig. 2 Box #	Title					
7	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required safety integrity level is achieved and maintained	17	Revised SIS safety requirements	Results of SIS modification	Operations
8	Decommissioning	To ensure proper review, sector organization, and ensure SIF remain appropriate	18	As-built safety requirements and process information	SIF placed out of service	Operations
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	7, 12.7	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase	Operations
10	SIS functional safety assessment	To investigate and arrive at a judgment on the functional safety achieved by the SIS	5	Planning for SIS functional safety assessment; SIS safety requirement	Results of SIS functional safety assessment	Operations

5.1 Step 1: Hazard & Risk Assessment

Overview					
Safety lifecycle phase or activity		Objectives	Requirements Clause or Subclause of ISA-84.01-2004	Inputs	Outputs
Fig. 2, Box 1	Hazard and risk assessment	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	8	Process design, layout, manning arrangements, safety targets	A description of the hazards, of the required safety function(s) and of the associated risk reduction

5.1.1 Hazard Identification

The hazard identification process started during the business decision analysis (clauses 2.1 & 2.2). It is one of the most important functions of the PHA team, and is ongoing until the process is turned over to plant operations and becomes subject to operational safety review and audit programs.

5.1.1.1 Preliminary Hazard Evaluation

The first step in any process development planning is to identify the broad parameters of the production process, to define safety and environmental hazards (or hazardous events), and to seek opportunities for making the process inherently safer. To do this, information is required about the physical and hazardous properties of all the feedstock, intermediates, products and wastes involved in possible alternative processes. For this example, where a specific polymer is being made from its monomer, there is little choice about the basic reactant. The available alternative processes vary the polymerization medium—solution, suspension or emulsion. The significant properties of VCM are summarized in Table 2.

NOTE — This is an example only for educational purposes. Contact vendors for the latest VCM material safety data sheet.

However, the reaction conditions and the initiator (plus any additives) need to be carefully chosen to assure that the reaction rate can be safely controlled to prevent runaway reactions, while producing adequate quality and yield. The selected technology involves polymerization in water, but does require small quantities of a relatively dangerous liquid initiator. The hazards associated with the initiator also need careful attention, but are not included in this simplified example.

5.1.1.2 Accident History

Next, the potential hazards are identified. In this example, the primary hazards are associated with the flammability and toxicity of combustion products from VCM. In actual plant design, personnel exposure and environmental ambient VCM limits would also be major considerations; for simplicity, these are not covered in this example. As a first step, it is useful to review the past history of accidents associated with similar operations.

In the case of VCM, we find reference to an accident in a PVC plant, in which four lives were lost and ten people were injured. This accident was due to discharging a batch from the wrong reactor vessel, so that

monomer was released into a room containing the parallel reactors. VCM vapor was presumably ignited by a spark from electric machines or by static electricity and the building housing the reactors exploded.

In another accident, a worker mistakenly opened a manhole cover on a reactor that was in service, releasing a large quantity of vinyl chloride that ignited and caused a flash fire resulting in the death of the maintenance person and two laborers.

Another accident involved charging a reactor with 250 gallons of VCM with the bottom valve of the reactor open. Although a serious hazard was created by this release, ignition did not occur and no one was injured. Other incidents are noted, such as one in which an explosion occurred during maintenance work on a vinyl chloride pump (due to a poly-peroxide contaminant that was present as a result of three simultaneous, abnormal situations). VCM was also released from a scrubber in a VCM production plant due to maintenance problems with a plugged valve during periodic recharging. Ignition of VCM resulted in one death and several injuries.

There also have been VCM releases and fires associated with transportation. A derailment of 16 cars near Houston, TX, USA, led to the escape of VCM from a 48,000-gallon rail tanker with immediate ignition. After 45 minutes of exposure to the fire, a second rail car of VCM ruptured violently, producing a large fireball (BLEVE, see 5.1.1.4, below), killing a fireman and injuring 37 other people. Large sections of a tank car were found about 400 feet from the derailment site after the explosion.

There are probably numerous minor incidents for every major accident reported. These may have cost impacts or cause some small environmental impact, but are too minor to be noted in the published incident lists, even though the more likely causes of minor equipment failures or small releases will be known to those familiar with plant operations and maintenance. Nevertheless, attention must be paid to the potential for small releases since these may be partial pathways to major accidents. Particularly with a highly flammable pressurized material, ignited small releases may cause larger failures if they heat other system components. Thus, integrity of a VCM system needs to be at a high level.

Table 2 – Some Physical Properties of Vinyl Chloride

Formula: $\text{CH}_2=\text{CHCl}$ Synonyms : vinyl chloride monomer (VCM) Monochloroethylene Chlorethene vinyl chloride (VCl) Shipped as compressed liquefied gas; Reid Vap. press.=75 psia Gas, colorless, sweet odor; Mol wt. = 62.5; Sp. Grav. (vap) = 2.16 Normal boiling point = 7.1°F; Sp. Gr. (liqNBP) = 0.97; Floats and boils on water Critical T = 317°F; Critical P = 775 psia; Melting point = -245 °F Heat of Vaporization = 160 Btu / lb; Heat of Combustion = 8136 Btu/lb Heat of Polymerization = -729 Btu / lb; Normally stable at ambient conditions; polymerizes in presence of air, sunlight, moisture, heat, or free radical initiators unless stabilized by inhibitors.
FIRE HAZARDS: Flammable Limits in Air: 3.6-33% Flash Point: -108°F (o.c.); Autoignition T = 882 °F Spills flash, boil and produce heavier-than-air gas cloud that may be ignited with flashback. Poisonous gases (HCl, CO, etc.) produced in fire May explode if ignited in confined space External fire exposure to container may result in BLEVE
HEALTH HAZARDS: Irritating vapor to eyes, nose and throat. If inhaled, causes dizziness, difficult breathing, and may cause serious adverse effects, even death. Excessive exposure may cause lung, liver and kidney effects. Human carcinogen, listed by OSHA, IARC and NTP. Threshold Limit Value: 5 ppm OSHA PEL: 1 ppm TWA, 5 ppm excursion limit average over any period not exceeding 15 minutes. Odor Threshold: 260 ppm Liquid contact may cause frostbite.
WATER POLLUTION: Limit in process water: 10 ppm Limit in water discharged offsite: 1 ppm
AIR EMISSIONS: Limit in process discharge to atmosphere: 10 ppm (local standard) Limit for annual concentration at plant boundary: 0.2 $\mu\text{g}/\text{m}^3$ VCM in air
RESPONSE TO DISCHARGE: Issue Warning—High Flammability, remove ignition sources, ventilate Stop flow Evacuate area, allow entry only with proper protective gear Let large fires burn; extinguish small fires with dry chemical or CO_2 Cool exposed container with water Prevent entry into sewer systems to avoid potential explosions

5.1.1.3 Preliminary Process Design Safety Considerations

For this example, the desired production rate of PVC is 200 million pounds per year, or about 23,000 lb/hr. Based on known reaction kinetics, at a reaction temperature of about 140°F, the corresponding cycle time is about 8 hours. In setting the reactor inventory, judgment is usually used with some awareness of the fact that hazard magnitude for catastrophic vessel failure is related to the amount of hazardous material. At one extreme, a single reactor might be used, with a production batch of 180,000 lb of PVC in a 40% slurry mixture, requiring a reactor sized for about 50,000 gallons capacity. This would be unwise, since no redundancy is present and there is a very large, flammable, high-pressure inventory. Also since capacity is not distributed, production batches would be large and infrequent, and would require downstream equipment sized for large inventories. Furthermore, this reactor would require addition of a large quantity of the dangerous initiator solution—a large enough inventory to raise serious safety concerns.

At the other extreme, a large number, say ten, of small reactors, each designed for a 18,000-lb production batch (about 5,000 gallons), might be used. In the first extreme, inventories are large; in the second, batches are small, switching operations are much more frequent, and there are many more interconnecting lines, valves, and complexities. Tradeoffs would be considered, based on operational needs, availability of equipment, and cost, as well as safety.

Refinement of such analyses leads to selection of the number of reactors in parallel and the size of the reactor unit. At this point, it is well to provide for any potential for future expansion in capacity. In this example, it is decided to install three parallel reactors, each with a 17,000-gallon capacity. The 5 gallons of initiator solution required per batch is a manageable quantity for safe handling. The maximum inventory of VCM in a reactor is estimated to be 60,000 lb.

Reaction temperature is selected to achieve a desired molecular weight, which is end-use driven. Proper reactor cooling water temperature control for stable reactor operation is required to prevent runaway reaction. Stable control of the polymerization reaction temperature requires a low temperature difference between the cooling water and the reaction temperature. For this example, the tempered cooling water supply temperature is high enough to provide a low temperature difference, versus the 140°F reaction temperature, for safe operation. The tempered cooling water comes from an established, highly reliable source with sufficient quantity and pressure available.

For this example, it was assumed that relief valves and vent valves go to a scrubber so that discharges are not environmental incidents.

5.1.1.4 Recognized Process Hazards

The primary acute hazards associated with VCM release are fire and explosion, with generation of toxic combustion products. These types of hazard include the following:

Jetfires: A leak from a pressurized system ignites and forms a burning jet that might impinge on other equipment and cause damage. (In rough terms, jet length is about 150 times the jet orifice diameter—a jet from a 2-in. hole could produce a burning jet about 30 feet long.)

Flash fires: A pressurized liquid release flashes, producing flammable vapor that travels to an ignition source. Upon ignition, the flame travels back through the flammable vapor cloud. (The flammable plume in this case can be substantially larger than the flame jet.)

Poolfires: Residual liquid from a flashing release forms a pool which may ignite and burn with a flame height that is two or three times the width of the pool.

BLEVEs (Boiling Liquid Expanding Vapor Explosions): A pressurized tank of VCM or associated piping exposed to an external fire may fail due to metallurgical weakening. Such failure may result in a catastrophic tank failure, a fireball and the potential for rocketing fragments. Relief valve overpressure protection will not prevent a BLEVE.

Explosions: Leakage of flammable gas into a confined space with subsequent ignition may lead to explosions or detonations with substantial overpressures.

Hydraulic Failure: Overfilling of a tank with subsequent liquid expansion through heating may lead to collapse of any vapor space and rapid pressurization. Sudden tank failure may ensue.

Stress Corrosion Failure: Air (oxygen) in the system may increase the presence of chloride ions and may lead to loss of metallurgical integrity.

Toxic Combustion Products: The combustion products of VCM include phosgene, hydrogen chloride and carbon monoxide along with other toxics. (These will be present in the aftermath of a fire, particularly if the fire is within a confined space).

Runaway Polymerization Reaction: VCM polymerization has the potential to rupture the reactor, releasing the VCM with major damage possible.

In addition, VCM presents chronic exposure hazards, being a known human carcinogen, and is a regulated substance with regard to personnel exposures to its vapors, having an OSHA PEL (personnel exposure limit – time weighted average) of 1 ppm in air. Further, federal and local regulations limit its discharge levels from process vents and plant water treatment systems. There are also stringent limits set on the amount of residual VCM that may be present in the PVC product.

There are some lesser short-term hazards involved with inhalation of VCM vapor and the potential for auto-refrigeration of flashing fluid. Personnel require protection from both inhalation and possible freeze burns.

At this point, scoping hazard zone estimates are made to indicate the magnitude of major potential accidents. A 60,000-lb release of VCM could produce a flammable vapor cloud equivalent to a cubic volume that is about 400 feet on a side. Because VCM is a heavy gas and may contain aerosols from flashing, a major vapor cloud is much more likely to be pancake-shaped, but still might have a flammable footprint of 1,000-1,500 feet in diameter. This indicates that the maximum accident involving a single reactor might have offsite impacts, and could fill a substantial confined volume with flammable gas. In terms of the assessment criteria discussed in Table 6 below, this impact should be considered to be at least "severe," and probably "extensive," depending on specific data considerations. To be conservative, the PHA team considers it to be in the "extensive" impact category. (Note: The bulk storage of VCM on site is not considered in this limited example.)

5.1.2 Process Design Strategy

5.1.2.1 Process Definition

The details of the design require definition of the basic operating procedures and maintenance strategies for the facility. Figure 3, a preliminary P&I diagram, is provided to assist in this effort. The operational steps for the process are outlined below:

Pre-evacuation of air: If the reactors have been opened for maintenance, oxygen must be removed from the system for quality and metallurgical integrity reasons.

Reactor preparation: The empty reactor is rinsed with high-pressure water, leak tested if the hatch has been opened, and treated with antifoulant.

Demineralized water charging: A controlled charge of water is added. An overcharge might lead to a hydraulic overfill; an undercharge may cause quality problems and potential runaway reaction. Any surfactants or other additives are also introduced during this step.

VCM charging: An accurate charge of VCM is added to the reactor.

Reactor heat-up: The initiator is added from the charge pot to the batch, and steam is added to the cooling water circulated through the reactor jacket until the batch is at a temperature where the reaction will proceed (about 10°F below the steady-state reaction temperature).

Reaction: The steam system is isolated and cooling water is circulated through the reactor jacket to control temperature by removing the heat of polymerization while the reaction progresses.

Termination: When the reactor pressure starts to decrease because most of the VCM present has been consumed by the polymerization, the batch will be dumped.

Reactor Discharge: The reactor contents are dumped under pressure to a downstream holding facility where the system is degassed for subsequent stripping and drying. To prevent resin settling in the reactor, the agitator operates during the dumping procedure. Unreacted VCM is recovered for reuse.

There are two additional process systems that are provided for an emergency situation. In the event of an uncontrolled reaction or the potential for such an event, the polymerization can be stopped rapidly by addition of a Shortstop chemical (chain stopping agent) to the batch. However, agitation of the batch is necessary for good distribution of the Shortstop to rapidly terminate the polymerization. If the agitator has failed, the Shortstop must be added within a minute or two, to allow mixing before the liquid swirl in the reactor dissipates. As a back-up, the reactor contents can be mixed by “burping” the reactor—dropping pressure to generate rising bubbles within the bulk liquid mass. These are both operator-activated events.

The second emergency system is an automatic depressurization system. In the event of an uncontrolled reaction, the reaction can be safely limited by depressurizing the reactor to the vent system. The heat of vaporization of the boiling reaction mass safely removes heat from the reactor. The emergency vent system will be sized to handle the peak venting needs of the reactor system.

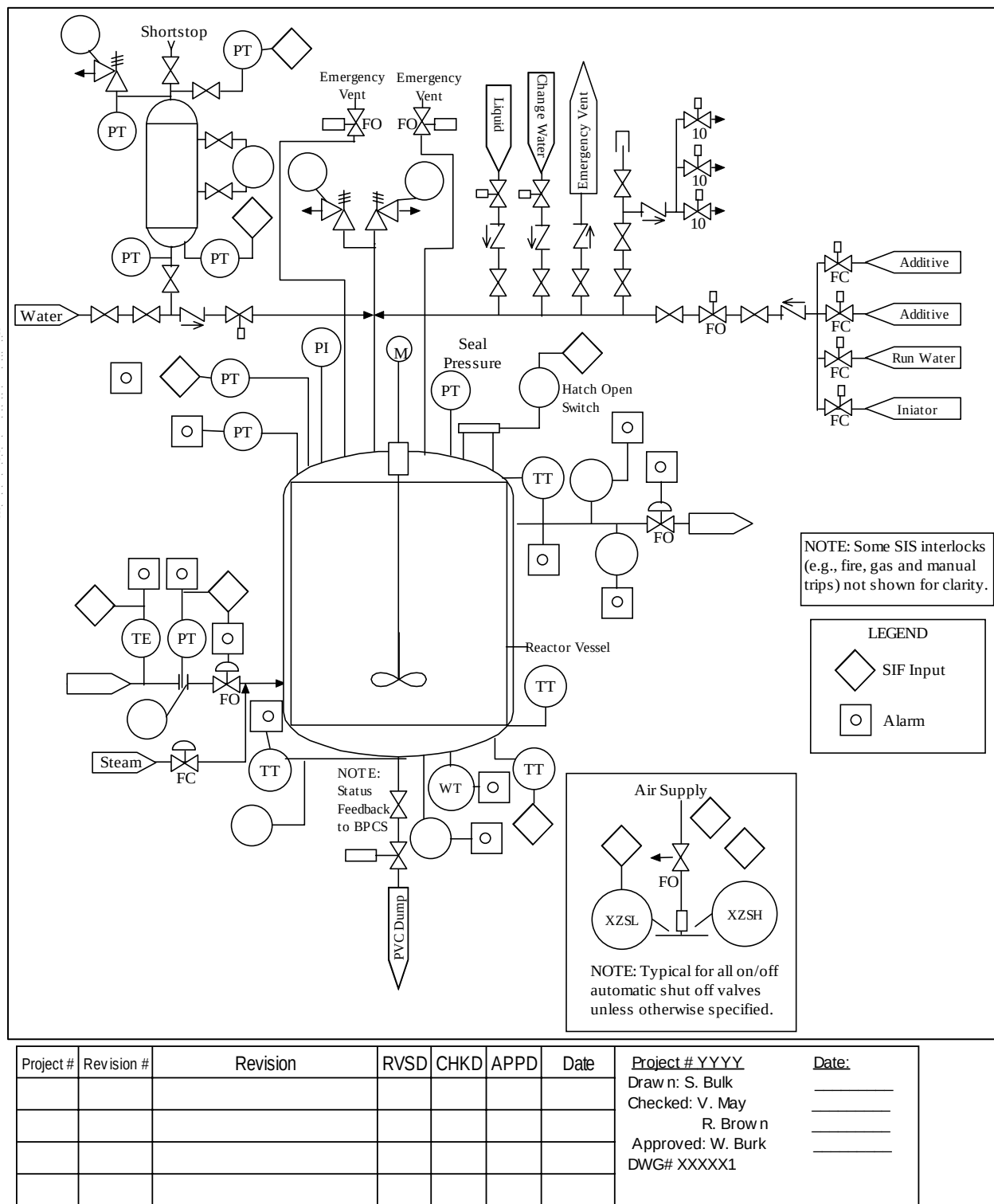


Figure 3 – Example of the preliminary P&ID for PVC reactor unit

NOTE — Piping headers are shown consolidated for clarity. See Figure 10 for header clarity.

5.1.3 Preliminary Hazard Assessment

Once the design was developed in some detail, the PHA team subjected the design to a preliminary hazard assessment. This assessment is considered preliminary because the design is not yet complete. The PHA team used a what-if/checklist review (Table 3) for the simpler portions of the process, and a HAZOP (Table 4) on the more complex portions of the process.

From the hazard identification process and from the past accident history, it seems that the example process reactor has the potential for “minor” through “extensive” events as defined in Table 6.

In addition, design integrity must consider the need to meet the strict containment requirements to prevent emissions of VCM that might endanger worker safety and health. The results of this hazard review need to be carefully documented, with particular regard to event sequences that might lead to uncontrolled releases.

NOTE — Table 3 and Table 4 show only partial lists of hazards pertinent to this example. A typical project would have a much more extensive list of What-If and HAZOP items.

Table 3 – What-If/Checklist
Prepared and Approved by the Process Hazards Analysis Team, see clause 2.2

WHAT IF...	HAZARD	CONSEQUENCES	SAFEGUARDS	REF #	RECOMMEN- DATIONS	BY
What if area wide electrical power fails. (UPS instrumentation power remains)	Runaway reaction through loss of agitation. Indicated by agitator motor off, low coolant flow, high reactor pressure, and high reactor temperature.	Runaway reaction causes reactor overpressure and loss of containment.	Add shortstop and burp reactor to stop runaway. Depressurize reactor - SIS (Pressure safety valve sized for this event).		Use LOPA to determine required SIL	
Batch recipe error - two charges of initiator are used.	High initiator concentration causes runaway reaction. Indicated by high reactor temperature and pressure.	Runaway reaction leads to reactor overpressure and loss of containment.	Add shortstop. Depressurize reactor - SIS (Pressure safety valve sized for this event).		Use LOPA to determine required SIL	
What if reactor agitator seal fails.	VCM fume release. Indicated by high pressure in the reactor seal and fume detector in the area.	VCM fumes are flammable.	Additional ventilation around reactor seal. Depressurize reactor on high seal pressure – SIS.		Use LOPA to determine required SIL	

NOTE — This is only a partial list of hazards.

Table 4 – HAZOP

Prepared and Approved by the Process Hazards Analysis Team, see clause 2.2

GW	DEVIATION	CAUSES	CONSEQUENCES	SAFEGUARDS	REF #	RECOMMENDATIONS	BY
No	No Flow	Cooling water control system failure	Eventual runaway reaction through reactor high temperature and/or high pressure	Add Shortstop. Depressurize reactor SIS (Pressure safety relief valve sized for this event)		Use LOPA to determine required SIL	
		Pump stops due to pump power failure	Eventual runaway reaction through reactor high temperature and/or high pressure	There is a Steam drive on the pump in addition to electric power. Add Shortstop. Depressurize reactor SIS (Pressure safety relief valve sized for this event).		Use LOPA to determine required SIL	
No	No Agitation	Agitator motor drive fails	Reduced cooling temperature, non-uniformity, leads to runaway reaction. As indicated by high reactor temperature, pressure, and low agitator motor amperage.	Add shortstop and burp reactor to stop runaway. Depressurize reactor SIS (Pressure safety relief valve, sized for this event.).		Use LOPA to determine required SIL	
More	Higher Temperature	Temperature control failure causes overheating during steam heating	High temperature leads to runaway reaction. Indicated by high reactor pressure and temperature.	Add Shortstop. Depressurize reactor SIS (Pressure safety relief valve sized for this event.).		Use LOPA to determine required SIL	
More	Higher Level	Level control failure allows the reactor to overfill	Reactor becomes liquid full as the temperature increases, possible hydraulic reactor damage and VCM release. Indicated by high charge level, high charge weight, or high reactor pressure.	Compare high level and weight with recipe. Depressurize reactor SIS (Pressure safety relief valve sized for this event).		Use LOPA to determine required SIL	

NOTE 1 — This is only a partial list of hazards.
NOTE 2 — GW stands for Guide Word.

Based on these results, a team of appropriate PHA process and instrumentation experts summarized a list of accident events where safety instrumented functions were proposed as mitigation of the hazard.

Table 5 is a partial list of accident events and the associated prevention strategy used to propose interlock strategy and actions to help further identify or create additional independent layers of protection.

Table 5 – Partial Summary of Hazard Assessment Information for Development of Safety Instrumented Function Strategy

Prepared and Approved by the Process Hazards Analysis Team, see clause 2.2

#	INITIATING EVENT	PROCESS UPSET	PROCESS VARIABLES AFFECTED	PREVENTIVE STRATEGY
1	Cooling water control fails	Loss of cooling leading to runaway reaction	- Low C.W. Flow - High Reactor Temp. - High Reactor Pressure	- Add Shortstop - Depressurize Reactor (SIS) - Pressure Safety Valves (IPL)
2	Agitator Motor Drive Fails	Reduced cooling, temperature non-uniformity leads to runaway reaction	- Low Agitator Motor Amperage - High Reactor Temp. - High Reactor Pressure	- Add Shortstop and Burp reactor to stop runaway. - Depressurize Reactor (SIS) - Pressure Safety Valves (IPL)
3	Area-wide loss of normal electrical power (UPS instrumentation power remains)	Loss of agitation leading to runaway reaction	- Agitation Motor off - Low Coolant Flow - High Reactor Pressure - High Reactor Temp.	- Add Shortstop and Burp reactor to stop runaway. - Depressurize Reactor (SIS) - Pressure Safety Valves (IPL)
4	Cooling water pumps stop, pump power failure	Loss of cooling leading to runaway reaction	- Low C.W. Flow - High Reactor Temp. - High Reactor Pressure	- Steam Drives on Pumps - Add Shortstop - Depressurize Reactor (SIS) - Pressure Safety Valves (IPL)
5	Batch recipe error; two charges of initiator are used	High initiator concentration causes runaway reaction	- High Reactor Pressure - High Reactor Temp.	- Add Shortstop - Depressurize Reactor (SIS) - Pressure Safety Valves (IPL)
6	Control system failure overfills reactor	Reactor becomes liquid full as the temperature increases, possible hydraulic reactor damage and VCM release.	- High Charge Level - High Charge Weight - High Reactor Pressure	- Compare level & weight with recipe - Depressurize Reactor (SIS) - Pressure Safety Valves (IPL)
7	Temperature control failure causes overheating during steam heat-up step	High temperature leads to runaway reaction.	- High Reactor Pressure - High Reactor Temp.	- Add Shortstop - Depressurize Reactor (SIS) - Pressure Safety Valves (IPL)
8	Reactor agitator seal fails	Seal failure can lead to dangerous VCM fume release	- High Pressure in Reactor Seal - Fume Detection in Reaction Area	- Additional ventilation around seal - Depressure reactor on high seal pressure (SIS)