Diagram 2. Initiating causes.
Diagram 4. Relief system with behaviors allocated to structures.
Diagram 6: Management system
Diagram 7. Asset integrity.
Diagram 8. Audits.
Diagram 11: Emergency planning and response.
**Diagram 12. Hazard analysis.**

HAZOP studies

Id = ""
Text = "Hazard and Operability studies shall be completed on the following:
1. Existing processes which have not been subjected to the HAZOP methodology.
2. Existing processes where an increase in the quantity/quality of available process information will enhance previously completed HAZOP(s).
3. New processes developed by and/or implemented into routine operations.
4. Ancillary operations which support bulk chemical manufacturing.
5. Major equipment installations or modifications.
7. Processes where there is a significant change in known or perceived hazards as demonstrated through process incidents, safety testing results and abnormalities.
8. Processes or operations as required by the legislation."

- Incident investigation
  - Management System: Management System
  - Major incidents follow-up practices
  - Near-miss reporting practices
    - Near-miss reports
      - Id: ""
      - Text: "Near misses reports of repeated operator errors or malfunctioning safety devices and alarms must include:
        - Where the incident occurred (e.g., part of plant).
        - What was being done, and when.
        - What system(s) failed (human, procedure, equipment, etc.).
        - What were the exact consequences of the incident.
        - What are the recommended actions or corrective actions.”
  - Incident and near miss investigation reports
Diagram 15. Management of change.
Prior to the introduction of a highly hazardous chemical to a process, the pre-startup safety review must confirm that the following:

- Construction and equipment are in accordance with design specifications;
- Safety, operating, maintenance, and emergency procedures are in place and are adequate;
- A process hazard analysis has been performed for new facilities and recommendations have been resolved or implemented before startup, and modified facilities meet the management of change requirements; and
- Training of each employee involved in operating a process has been completed.
Maintain info on hazardous materials.

For hazardous materials, the site should maintain maps and reference information on applicable chemicals, site locations, quantity of stored material that could be involved in reasonable accidental release scenarios, and the nature of the health hazards, property damage, and environmental harm most likely to accompany the release scenarios.

Diagram 20. Training.
Diagram 22: Inputs and outputs of MOC.

Inputs to MOC from Process safety information:
- Equipment specifications
- Safer operating limits
- Safety system definitions
- Drawings
- Chemical or process hazard information

Inputs to MOC from Training and performance:
- Job qualifications
- Staffing

Inputs to MOC from Contractor management:
- Qualification requirements
- Training requirements

Inputs to MOC from Hazard analysis:
- Indication of process or activity risk
- Risk tolerance criteria
- Recommendations needing to be managed as changes
- Safety systems
- Hazardous events descriptions
- Management of change
- Operating procedures
- Inspection and testing procedures

Inputs to MOC from Pre-startup review:
- Items discovered during a start-up review

Inputs to MOC from Operating procedures:
- Operating procedures descriptions
- Compensating measures
- Conditions to execute a safe shutdown
- Management of change
- Operating procedures
- Inspection and testing procedures

Inputs to MOC from Asset integrity:
- Maintenance procedures
- Personnel qualifications
- Inspection and testing procedures frequencies

Inputs to MOC from Safer work practices:
- Safer work practice procedures
- Criteria for applying procedures

Outputs from MOC to Contractor management:
- Changes to implementation timing

Outputs from MOC to Training and performance:
- Info on changes to inform or train personnel

Outputs from MOC to Process safety information:
- Updates to process safety information
- Updates to process knowledge
- Updates to records

Outputs from MOC to Pre-startup review:
- Changes to situations requiring start-up review

Outputs from MOC to Hazard analysis:
- Results of MOC hazard evaluation

Outputs from MOC to Operating procedures:
- Changes needed to affected operating procedures

Outputs from MOC to Asset integrity:
- Updates to maintenance procedures
- Updates to inspection and testing frequencies
- Updates to personnel qualifications

Outputs from MOC to Safer work practices:
- Updates to procedures
- Updates to personnel
- Updates to application criteria
Management commitment

Id = "MOC Mgmt 1"
Text = "Strong management commitment should include allocation of adequate resources for managing change and the willingness to modify existing management systems when necessary to accommodate MOC requirements."

Provide MOC training

Id = "MOC Mgmt 2"
Text = "Management should provide effective orientation and training for all personnel (including contract personnel) involved in activities that can result from or be affected by changes."

Allocate resources for managing change

Modify existing management systems to accommodate MOC requirements

Provide training for all personnel involved in activities derived from or affected by changes

Diagram 23. Management commitment MOC.
Diagram 24. Key principles and essential features MOC.
Diagram 26. MOC design and development.

Key issues:
- hazard evaluation communication of changes
- special approval of high-cost items not addressed by another system
- system documentation

Special situations: temporary repairs or installations, emergency changes, variance policy

«allocate»

Design

- Define MOC system scope
- Define system terminology
- Define roles
- Define interface considerations

Development

- Work within scope
- Use defined terms
- Enhance definitions as necessary
- Assign specific detailed tasks and responsibilities
- Develop interface or transition procedures between MOC and other process safety management systems
- Develop review and authorization procedures
- Develop guidelines for special situations
- Develop procedures for special situations
- Develop procedures, guidelines, forms, and documentation
Diagram 27. MOC system design specification.
Diagram 28. MOC system development.
Diagram 31. MOC system roles.
Diagram 32. Request for change review and approval procedure.
<table>
<thead>
<tr>
<th>#</th>
<th>Id</th>
<th>Name</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>C1</td>
<td>IPL Core Attribute: Independence</td>
<td>The performance of a layer should not be affected by the occurrence of the initiating cause, its consequences, or by the failure of another protective function used to reduce the risk of the same hazardous event.</td>
</tr>
<tr>
<td>2</td>
<td>C1a</td>
<td>Separation</td>
<td>The correct operation of the protection layer should not be conditional on any other layer and its separation from other layers should be unambiguous.</td>
</tr>
<tr>
<td>3</td>
<td>C1b</td>
<td>Demonstrate Independence</td>
<td>Independence within the management system should be demonstrated for any administrative process used for risk reduction or used for reduction of systematic error.</td>
</tr>
<tr>
<td>4</td>
<td>C1c</td>
<td>Consideration of Who</td>
<td>The independence assessment should consider who performs and manages the inspection, preventive maintenance, and maintenance activities for each protection layer.</td>
</tr>
<tr>
<td>5</td>
<td>C2</td>
<td>IPL Core Attribute: Functionality</td>
<td>The protection layer must be capable of operating as expected during actual service conditions and during all process operating modes where the hazardous event can occur.</td>
</tr>
<tr>
<td>6</td>
<td>C2a</td>
<td>Timely effective response</td>
<td>The protection layer must be capable of responding effectively within the time required by stopping the propagation of the initiating cause, even in the presence of other protection layer failures.</td>
</tr>
<tr>
<td>7</td>
<td>C2b</td>
<td>Examine potential interactions</td>
<td>The system should be examined holistically to understand the potential interactions between the hardware, software, and communication components of the system.</td>
</tr>
<tr>
<td>8</td>
<td>C2b1</td>
<td>Understand interactions</td>
<td>Personnel responsible for maintaining protective systems must understand how its components work within the complex system.</td>
</tr>
<tr>
<td>9</td>
<td>C2c</td>
<td>Impact assessment</td>
<td>Management of change processes must assess system impact, as well as impact to the function.</td>
</tr>
<tr>
<td>10</td>
<td>C3</td>
<td>IPL Core Attribute: Integrity</td>
<td>During the risk assessment phase, the required integrity has to be defined for each protective function using qualitative, semi-quantitative, or quantitative methods.</td>
</tr>
<tr>
<td>11</td>
<td>C4</td>
<td>IPL Core Attribute: Reliability</td>
<td>The equipment of a protection layer should operate as intended, under stated conditions, for a specified time period.</td>
</tr>
<tr>
<td>12</td>
<td>C5</td>
<td>IPL Core Attribute: Audibility</td>
<td>The protective management system must define the work processes used to develop and maintain the required information, documentation, and procedures, including assessments, verifications, inspections, and audits.</td>
</tr>
<tr>
<td>13</td>
<td>C5a</td>
<td>Audit trail traceability</td>
<td>The &quot;audit trail&quot; or &quot;paper trail&quot; should be traceable through the lifecycle from the hazard and risk analysis findings to reports on the installed and operational instrumented protective systems.</td>
</tr>
<tr>
<td>14</td>
<td>C6</td>
<td>IPL Core Attribute: Access Security</td>
<td>Access security should be implemented for any activity that potentially affects a core attribute of the system.</td>
</tr>
<tr>
<td>15</td>
<td>C6a</td>
<td>Administrative Access Security</td>
<td>The protective system should implement access security administratively with policies, practices and procedures to monitor, control, and audit.</td>
</tr>
<tr>
<td>16</td>
<td>C6b</td>
<td>Physical Access Security</td>
<td>The protective system should implement access security physically with independence equipment supported by barriers, such as keys, locks, and passwords.</td>
</tr>
<tr>
<td>17</td>
<td>C6c</td>
<td>Operations Activities Access Security</td>
<td>Access security should be implemented for operations activities, such as bypassing, set point changes, alarm response, event reporting, and documentation.</td>
</tr>
<tr>
<td>18</td>
<td>C6d</td>
<td>Isolate network information</td>
<td>Means additional to passwords, firewalls and encryption should be used to isolate and filter network information so that it cannot affect any protection layer.</td>
</tr>
<tr>
<td>19</td>
<td>C7</td>
<td>IPL Core Attribute: Management of</td>
<td>The management system should employ a management of change (MOC) or change management process to review, document and approve changes prior to implementation.</td>
</tr>
<tr>
<td></td>
<td>C7a</td>
<td>Assess impact of changes</td>
<td>The impact of changes such as staffing, reporting authority, site organization on work processes or the design basis must be assessed prior to their implementation.</td>
</tr>
</tbody>
</table>

Diagram 33. Requirement table.
Diagram 34. Policy.
Diagram 35. Laws and regulations.
<table>
<thead>
<tr>
<th>#</th>
<th>Id</th>
<th>Name</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15 USC 2601</td>
<td>TSCA</td>
<td>Toxic Substances Control Act I</td>
</tr>
<tr>
<td>2</td>
<td>29 CFR 1910.119</td>
<td>OSHA PSM</td>
<td>Process safety management of highly hazardous chemicals</td>
</tr>
<tr>
<td>3</td>
<td>29 USC 651</td>
<td>OSHA</td>
<td>Occupational Safety and Health Act</td>
</tr>
<tr>
<td>4</td>
<td>40 CFR 68.65</td>
<td>EPA RMP</td>
<td>Risk Management Program</td>
</tr>
<tr>
<td>5</td>
<td>42 USC 116</td>
<td>EPCRA</td>
<td>Emergency Planning and Community Right-to-Know Act</td>
</tr>
</tbody>
</table>

Diagram 36. Laws and regulations table.
Diagram 38. Lifecycle.

- Planning
- Risk assessment phase
- Design
- Development
- Installation
- Operation and Maintenance
- Improvement

For MOC:
- Process development
- Detailed design
- Construction and startup
- Operating lifetime
- Extended shutdowns
- Decommissioning
Diagram 42. Stakeholders.
Diagram 45b: Stakeholders' viewpoints.
Diagram 46. Planning.
Diagram 47. Risk assessment phase.
Diagram 52. Improvement.
Diagram 53. LOPA structure for simulation.
Diagram 54. Parametric diagram of LOPA for simulation.
Diagram 55. Instances of LOPA for simulation.