Maximizing HAZOP/LOPA Quality

Steven T. Maher, PE CSP
Risk Management Professionals

TH-A2 - Part 3
March 23, 2023

25th California Unified Program
Annual Training Conference
March 20 – 23, 2023

Key Topics

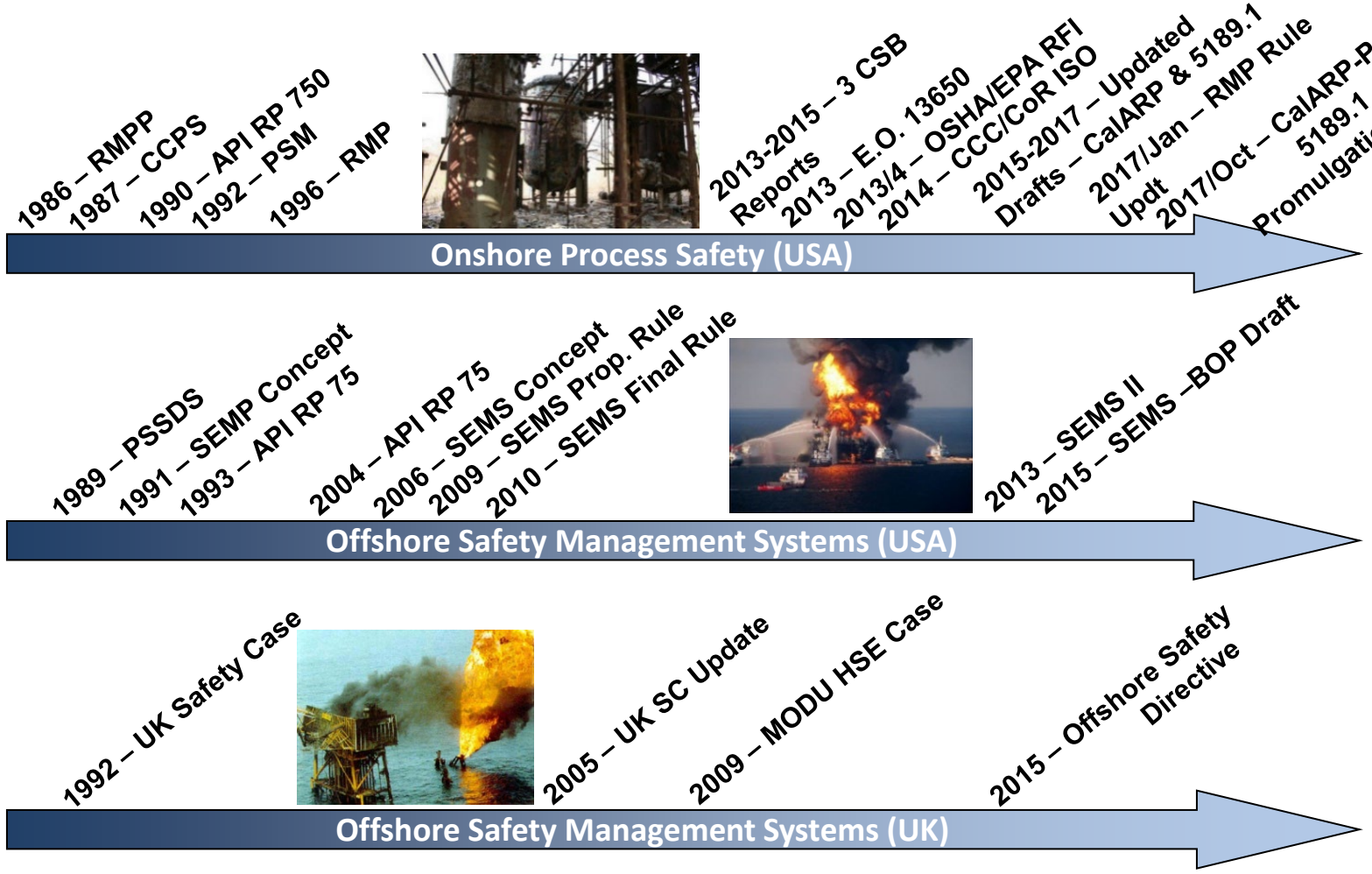
- Why Quality Process Hazard Analysis (PHA) is Important
- Brief History of Key PHA Techniques & Regulatory Requirements
- Resources & Preparation
- Tips for Conducting a Quality PHA
- PHA Documentation
- Common PHA Quality Challenges
- Maximizing the Future Usefulness of the PHA
- Questions?

Why Quality Process Hazard Analysis (PHA) is Important

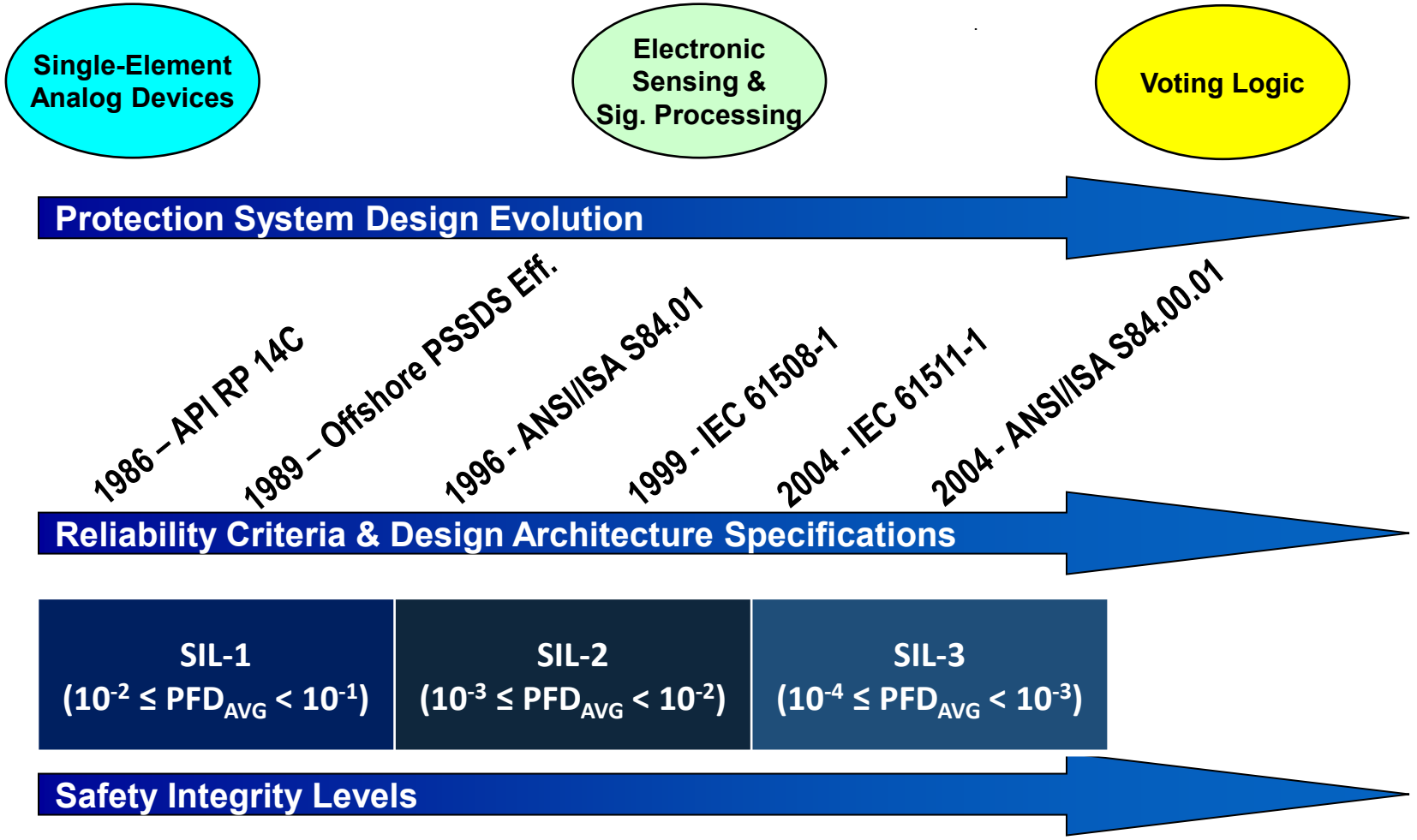
Tragedies to Avoid

Brief History of Key PHA Techniques and Regulatory Requirements

Evolution of SMS Guidelines & Regulations to Performance (Goal) – Based Standards

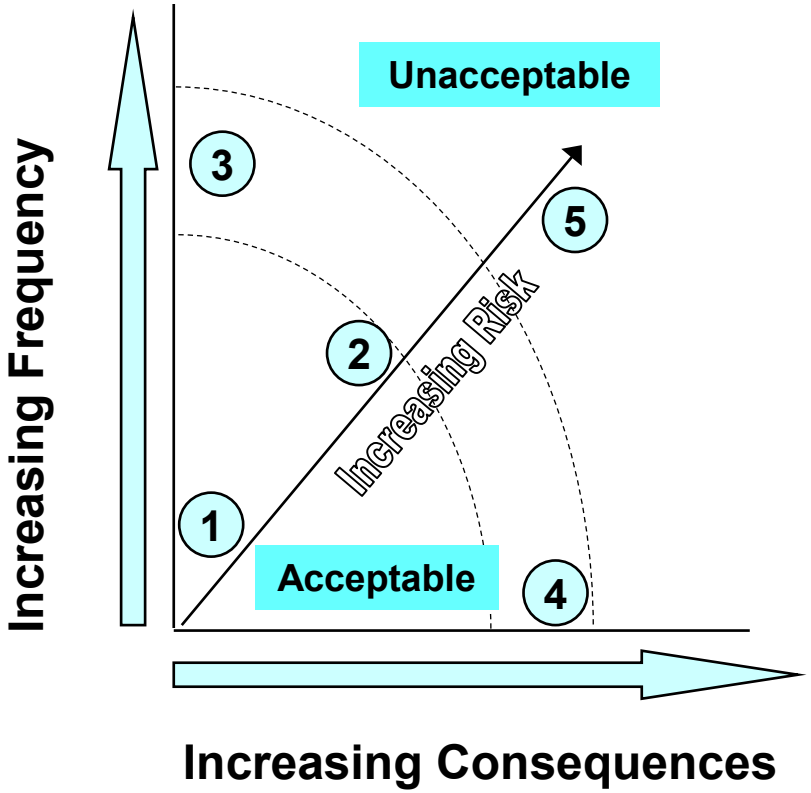


Tandem Advances in Protection System Design Architectures & Analysis

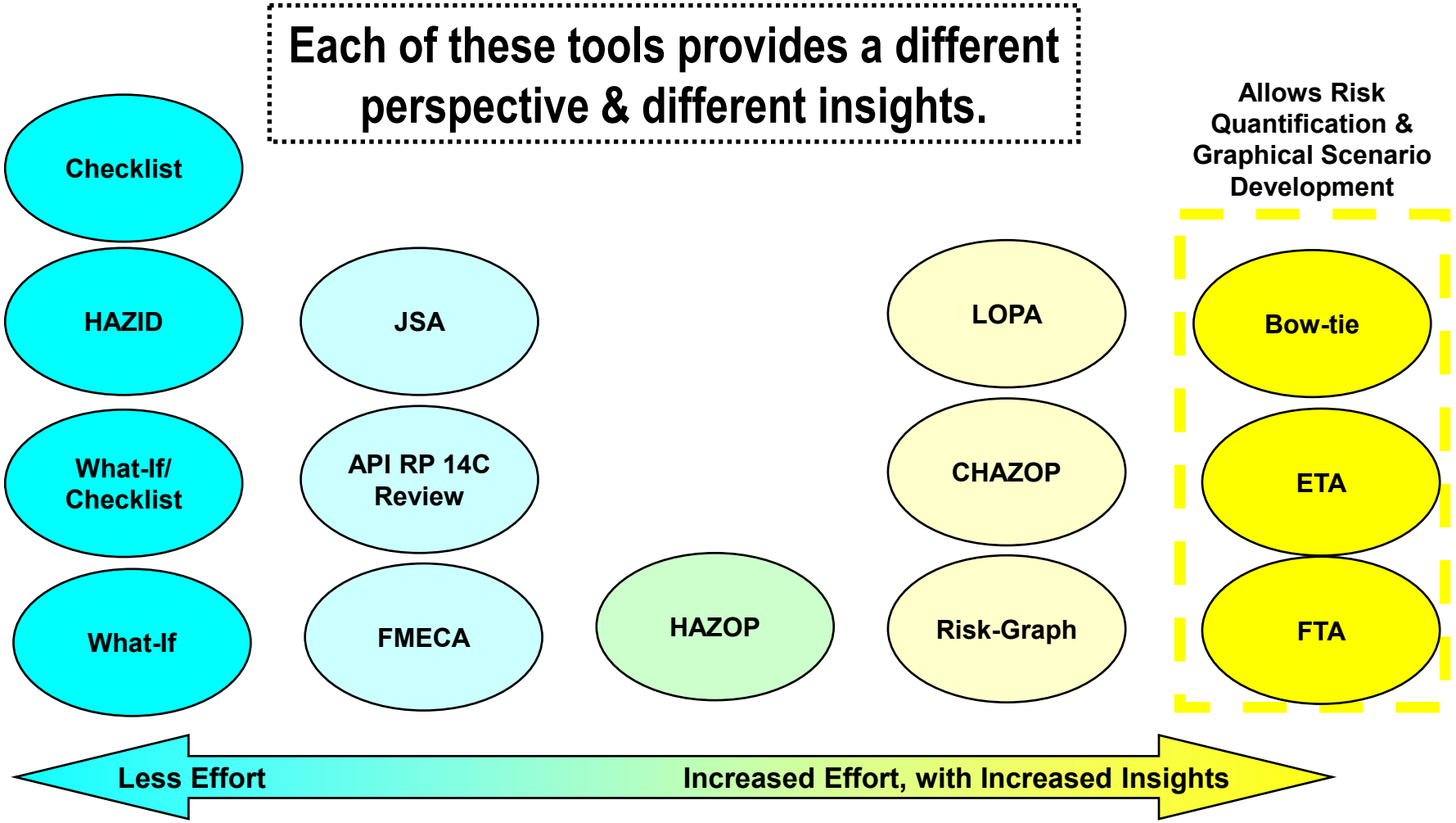


Focusing on the Objective (The "Big Picture")

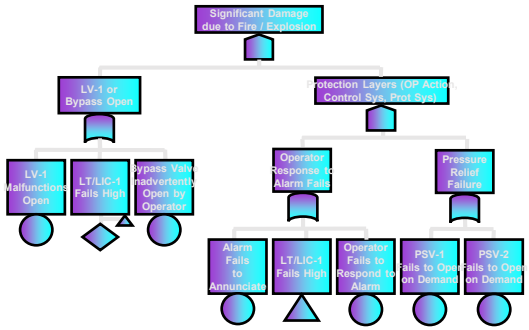
- **RISK = PROBABILITY * CONSEQUENCES**
  - **Probability = Likelihood of Occurrence**
  - **Consequences = Effects of Occurrence**
- For Engineered Systems:
  - **Risk = Σ $F_i * C_i$**

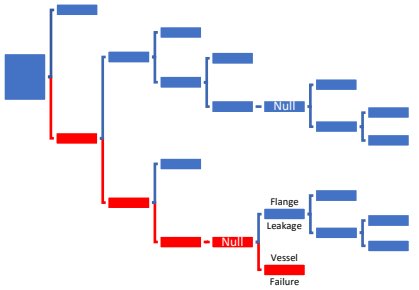


Hazard Analysis Tool Spectrum



HAZOP & LOPA are Core Elements of Hazard Evaluation





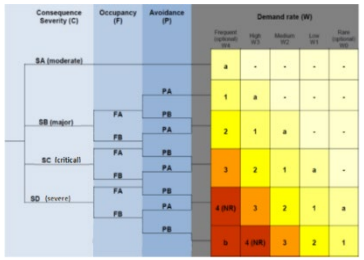
HAZOP ⟷ LOPA

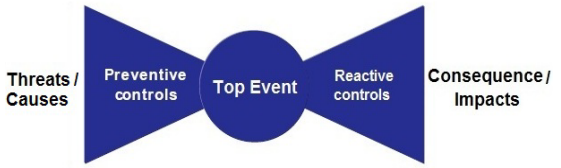
CHAZOP

What-If

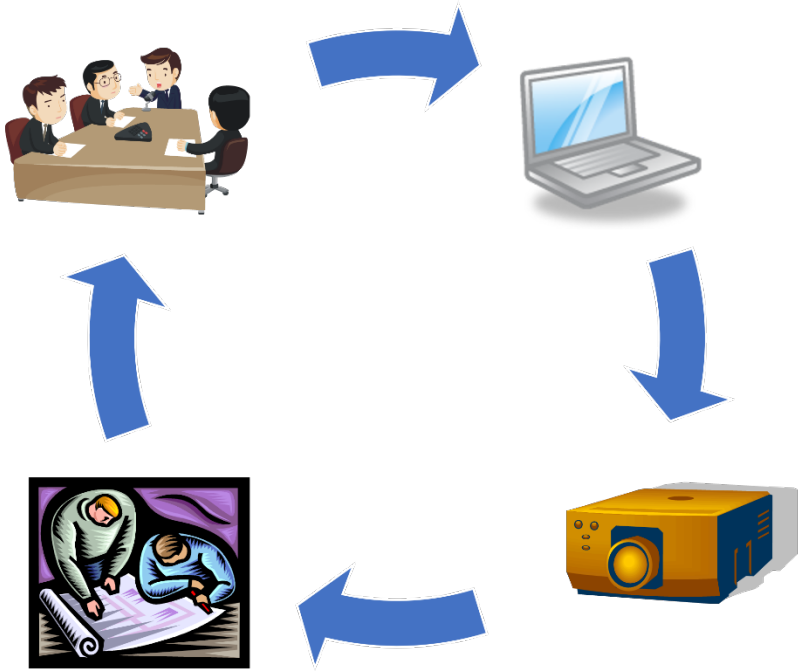
Checklist

FMECA

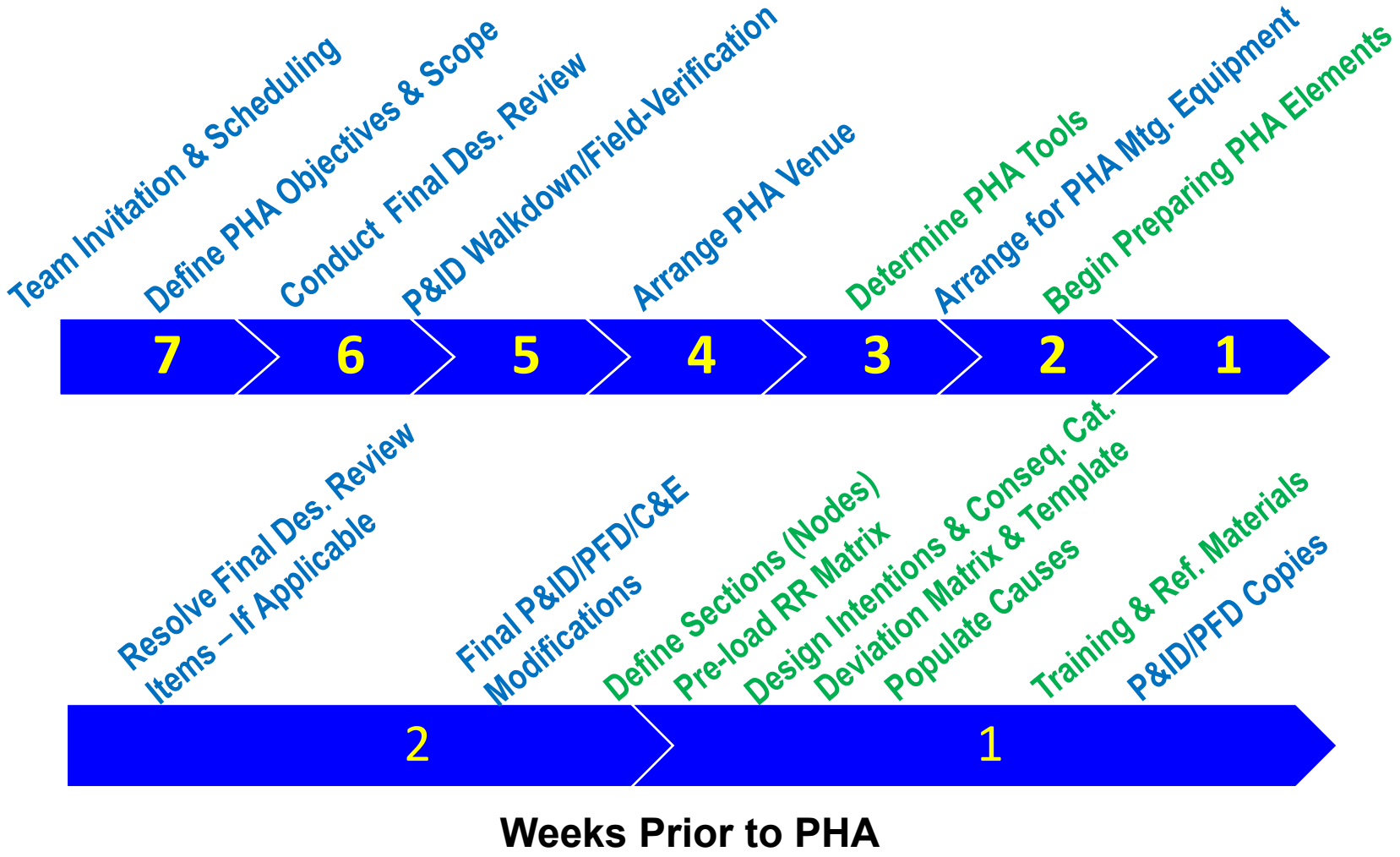




Resources & Preparation

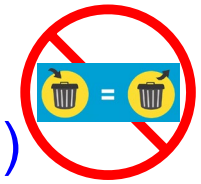


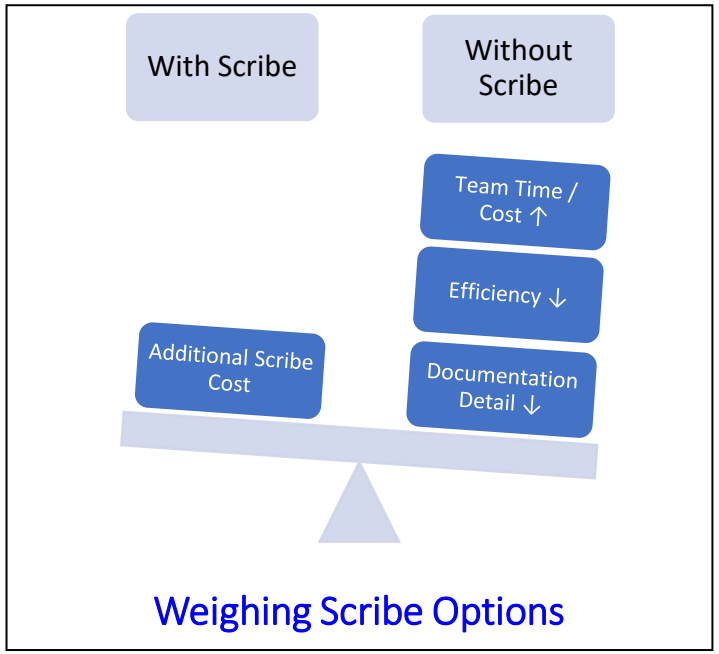
Timeline for PHA Preparation



Planning & Preparation Essentials

- Qualified, Experienced, & Prepared:
  - Technical Experts who Participate in all Phases of the PHA (Process Engineering, Operations, & Maintenance Disciplines Required by PSM/RMP)
  - Facilitator – Additional Skills Required for Remote PHAs
  - Scribe – Engineering, Software, PHA Skills Helpful
- Quality-Checked, Complete, & Field-Verified Engineering Drawings
- Access to Other Key Process Safety Information
- PHA & Revalidation Schedule
- Use of Appropriate PHA Technique
- Cause Pre-Population (Completeness, Grouping for Future-use, Easy Location During PHA)





Weighing Scribe Options

Tips for Conducting a Quality PHA

Tips for Conducting a Quality PHA

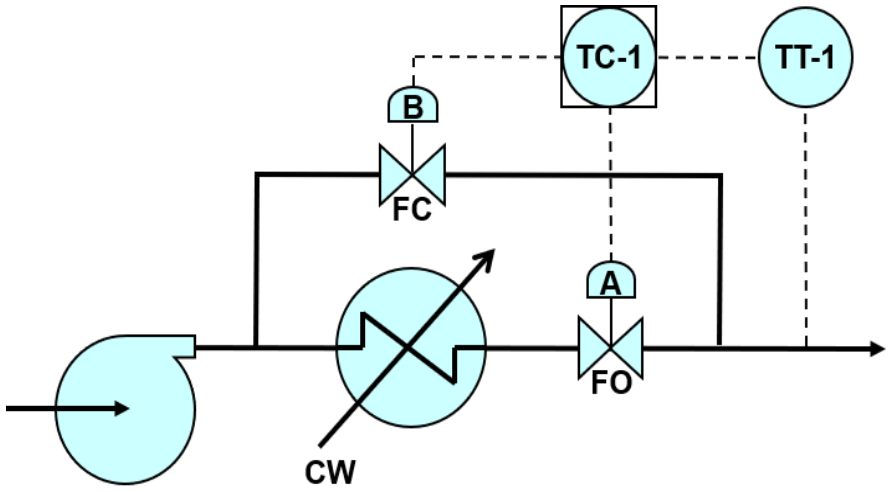
- Facilitator Support
  - Trains & Drives Team Synchronization
  - Encourages Participant Involvement/Cooperation
  - Pushes for Consistent Risk-Ranking
  - Uses Risk-Ranking to Drive Recommendations
  - Drives Team to Consistently Bin Probable Worst-Case Consequences & Apply Safeguards Associated with the Scenario
  - As Appropriate, Links:
    - HAZOP
    - LOPA
    - Quantitative Risk Assessment (QRA)
    - Other Tools/Perspectives

Tips for Conducting a Quality PHA

- Knowledge Base
  - Process Design/Limits & Response to Upset Conditions
  - Instrumentation & Setpoints
  - Control & Protection System Actions
  - Equipment Physical Configuration
  - Operations & Maintenance
  - Management Endorsement & Commitment of Resources
- Team Interaction & Professionalism
  - Consideration of All Salient Perspectives & Input
  - Maintaining Focus and Minimizing Interruptions During the PHA
  - Objectivity
  - Session Length Should Reflect Process Complexity

Tips for Conducting a Quality PHA

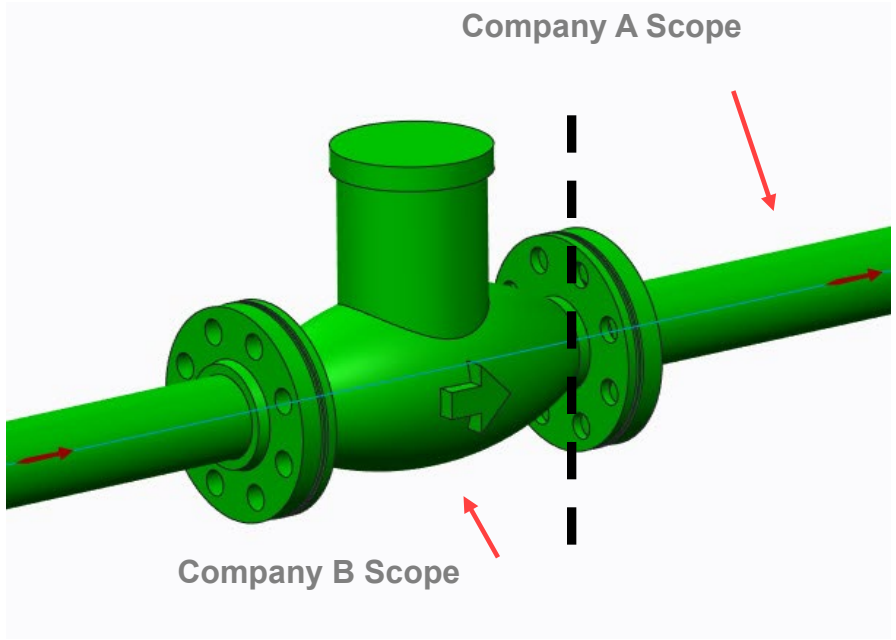
- Technical Details
  - Process Design/Limits & Response to Upset Conditions
  - Overpressure Ratios
  - Cause/Consequence Documentation
  - Instrumentation & Setpoints
  - Control & Protection System Actions
  - Valve Failure Mode Clarity
  - Crediting Alarms as Safeguards
  - Subcomponent Failure Modes



Common Temperature Control System
(control station block and bypass valves removed)

Tips for Conducting a Quality PHA

- PHA Sessions
  - Capital Projects vs. Operating Facilities
  - Session Length Reflecting Process Complexity
  - PHA Team Training
  - Node Completeness Checks
  - PHA Revalidation vs. Re-do
  - Node Boundaries
  - Avoid Repeating Scenarios



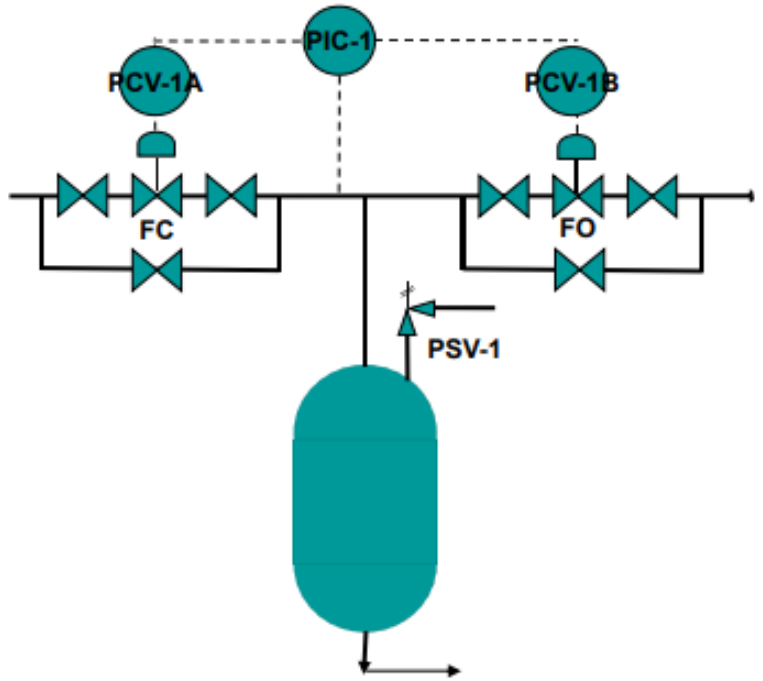
Node Boundaries to Avoid

Tips for Conducting a Quality PHA

- Information Dynamics
  - ➢Key Information Requirements
    - Process Flow Diagrams
    - Piping & Instrumentation Diagrams
    - Cause & Effect Diagrams
    - Alarm, Action, and PSV Setpoints – Relief Valve Design-basis Documentation
    - Equipment Layout Drawings
    - Access to Other Process Safety Information
  - ➢A "Parking Lot" for Resolvable PHA Issues to Streamline Efforts
  - ➢Manageable Drawing Updates – Knowing when to Stop
  - ➢Manageable Information Gaps

Example/Common Information Gaps

- General P&ID Content
  - Design Pressures/Temperatures/Metallurgy
  - Piping Specifications
- Control Valves
  - Failure Positions, Size, Setpoints
- Relief Valves
  - Setpoints, Size, Sizing Basis
- Pumps
  - Maximum Blocked-in Differential Pressure, Minimum Flow Requirements, Seal Design, Net Positive Suction Head (NPSH), Casing Design Pressure, Discharge Piping Specs
- Block Valves
  - "Normal" Positions



Documentation

PHA Documentation

- Analysis Completeness
  - Specific Causes, with Equipment Numbers Identified
  - Identify Probable Worst-Case Consequences
  - Focus on Reliable, Active, Tagged Safeguards with Sufficient Process Safety Time – Link to Cause/Consequence
  - Recommendations (or gap acceptance) Whenever Clearly-Defined Acceptable Risk Level is Not Achieved
  - Valid Operating Modes Addressed
  - Address Related Issues: Security, Siting, Human Factors, Training, Maintenance, Testing, Inspection, Start-up/Shutdown, Previous Incidents
- Consistency
  - Risk-Ranking – Consistent & Synchronized with Scenario
  - Level of Detail & Scenario Depth Pivoting on Importance

PHA Documentation

- Usability
  - Recommendations – Understandable, Self-standing, Logical, Complete
- Traceability
  - Scenarios – Logically-developed, Complete, Understandable
  - Block Valve Inadvertent Mispositioning
  - Liberal Use of Clarifying Comments
  - Team's Evaluation and Basis for Conclusions should be Readily Understood to Support Future Revalidation Efforts
  - Risk-Ranking – Consistent & Matched with Scenario
  - Clear Scope & System Boundaries
  - Document Team Composition and Experience
  - Sensible Recommendations Linked to the Scenario
  - Prolific Use of Equipment Tag Numbers & Cross-Referencing

Example – Causes (1)

- Bad
  - "Pump fails"
- Helpful
  - "Active Condensate Stabilizer Bottoms Pump (P-XXXX, P&ID YYYY) fails to operate, possibly due to a loss of power."
- Considerations
  - Use a 20-second rule for locating equipment.
  - Equipment names should exactly match the P&ID and be capitalized for easy spotting and specificity.
  - Vessel/Pump/Compressor/Activated Valve – First time usage in a scenario should have a tag number and P&ID reference.

Example – Causes (2)

- Bad
  - "Valve closed"
- Helpful
  - "LV-XXXX (P&ID YYYY) fails closed, possibly due to LT/LC-XXXX malfunctioning low, or block valve inadvertently closed."
- Considerations
  - Identify root transmitters for Causes & Safeguards.
  - Examples for when to split failure modes as Independent Causes – push-pull configuration, operational block valve, multiple controlled devices
  - Combine sub-failure-modes only when consequences are identical and LOPA results are not impacted.

Example – Causes (3)

- Bad
  - "ESD valve fails"
- Two Helpful Examples to Not Make a Safeguard into a Causal Event
  - "XSV-XXXX (P&ID YYYY) failing to close on demand, possibly due to an instrumentation malfunction, is implicit in the PFD associated with a safeguard credited in Scenario ZZ.AA.BB. No new issues were identified by the HAZOP/LOPA Team."
  - Inadvertent closure of overflow line manual valve is implicit in the PFD associated with a safeguard credited in Scenario ZZ.AA.BB. No new issues were identified by the HAZOP/LOPA Team."
- Considerations
  - HAZOP/LOPA are scenario-based analyses
  - If a safeguard's failure is already implicit in a scenario, treating its failure as a separate causal event is inappropriate

Example – Consequences (1)

- Bad
  - "Compressor goes into recycle"
- Helpful
  - "Potential overpressurization of equipment downstream of the operating Gas Export Compressor (C-XXXX, P&ID YYYY). Potential breach, release of flammable gas, fire, and personnel hazard."
- Considerations
  - Ensure ULTIMATE CONSEQUENCES are documented.
  - Illustrate event sequencing.
  - Cascading consequences (e.g., flammable gas release if a PSV opens to control overpressurization) may be handled with a separate consequence category.

Example – Safeguards (1)

- Bad
  - "Pressure control"
- Helpful
  - "PT/PC-XXXX (ZZ psig, P&ID YYYY) is designed to open PV-XXXX and prevent overpressurization of the Condensate Stabilizer Column (V-AAAA, P&ID BBBB)."
- Considerations
  - Use a 20-second rule for locating equipment.
  - Highlight the setpoint to the HAZOP/LOPA Team, especially to clarify/verify scenario progression.
  - Validate process safety time.

Example – Safeguards (2)

- Bad
  - "High pressure trip"
- Helpful
  - "PAHH-XXXX (AA barg, P&ID YYYY) is designed to trigger ESD-ZZZZ and trip any operating Gas Export Compressor on high-high discharge pressure."
- Considerations
  - Make good use of software type-ahead features.
  - Make it easy to spot common-mode failures.
  - Segue to LOPA.
  - Order safeguards by event sequence.
  - Partition safeguard as an Independent Protection Layer (IPL).

Example – Safeguards (3)

- Bad
  - "Temperature alarm"
- Helpful
  - "TAH-XXXX (180C, P&ID YYYY) is designed to trigger a Control Room alarm on high outlet temperature and provide the Operator with sufficient time for diagnosis and corrective action."
- Considerations
  - Typically group alarms as a single safeguard.
  - Reliability & timing of Operator response to alarm(s):
    - Present to hear the alarm
    - Alarm prioritization and diagnosis
    - Permission for corrective action
    - Initiating the corrective action
    - Time for the corrective action to mitigate the event
  - Only include "effective alarms."

Example – Safeguards (4)

- Example of Compound Safeguard
  - PSV-XXXX and PSV-YYYY (AA barg, P&ID ZZZZ) both working together are designed to provide overpressure protection for this scenario.
- Considerations
  - Segue to LOPA
  - Clear definition of IPL

Example – Recommendations (1)

- Bad
  - "Review high pressure protection."
- Helpful
  - "To minimize the potential for overpressurizing equipment downstream of the Gas Export Compressor (C-XXXX, P&ID YYYY), consider configuring a high discharge pressure trip of any active compressors."
- Considerations
  - Ensure action is clear and minimizes the need for the assignee to review the HAZOP/LOPA Report.
  - Briefly identify the concern.
  - Include P&ID references and equipment tag numbers.

Priorities for PHA QA Review

- **Completeness Check** – All Key Causal Events
- **Probable Worst-Case Consequences** – Clearly identified and used as the basis for risk-ranking
- **Safeguard/IPL Verification** – Especially Independence
- **Scenarios** – Interpretable – Should present an image of event
- **Risk-Ranking** – Consistent
- **Clear Action Items** – Complete with Focused Basis, Self-Standing
- **Same Initiating Event, but Different Deviation** – Increased potential for confusion and future misuse

Quality Program Control – PHA

- Leadership & Synchronization of Facilitation
- Patterned Examples
- Knowledge Base of Best Practices
- Knowledge Base of Owner/Facility Preferences

Common PHA Quality Challenges

Common PHA Quality Challenges (1)

- **Causal Event Completeness**
- **Incorrect Ultimate Consequences**
  - From a Major Oil & Gas Company's Guidelines: "Underestimating can lead to insufficient layers of protection being applied and risk being insufficiently managed."
  - Pre-crediting the mitigative effects of safeguards can result in underestimating the "challenges" to the IPL, leading to a potential for underestimating the needed SIL Assignment for the SIF.
- **Missing Safeguards and Overestimation of SIL because BPCS was not Credited as an IPL**
- **Incorrect Scenario Development Leading to Erroneous Conclusions** – E.g., failure of a safety feature used as an initiating event.

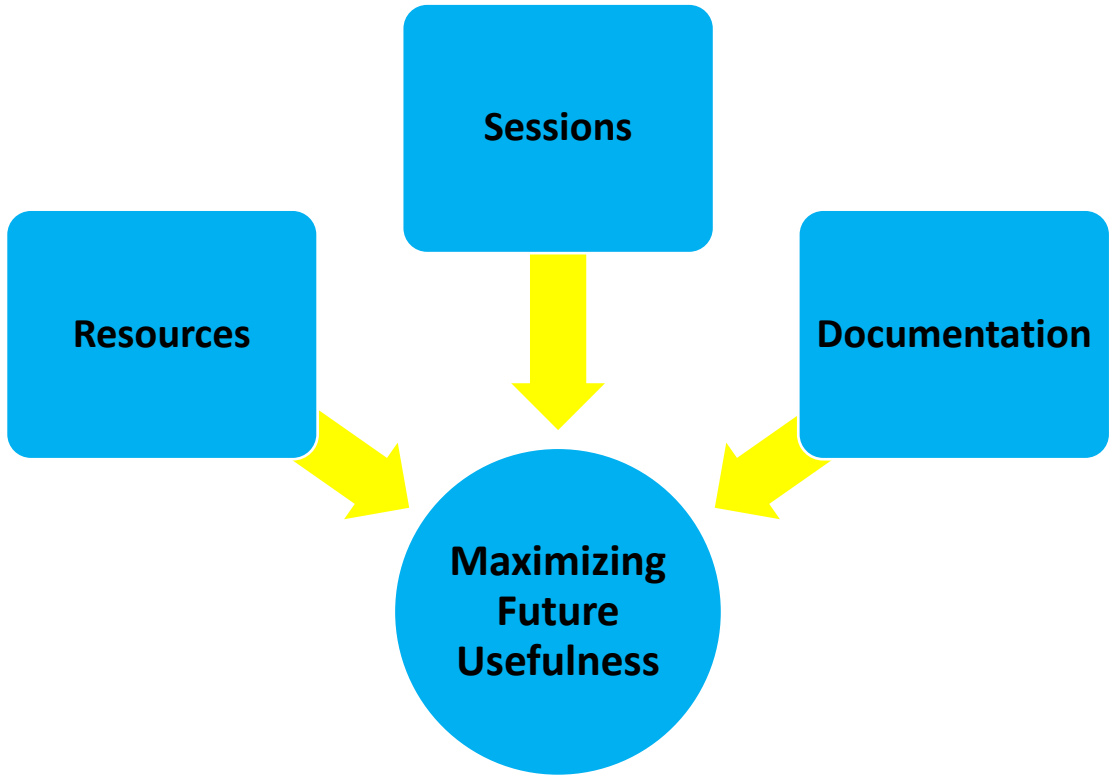
Common PHA Quality Challenges (2)

- **LOPA Not Done Properly** – E.g., IEF, Operator presence for vulnerability factor
- **Not Using Software Features to Streamline Effort and Drive Consistency** (e.g., careful and consistent application of safeguard patterning) – This can lead to SIL underestimation.
- **Duplication of Scenarios** – Apply the multiple consequence category format and implement discipline.
- **Evaluation of Vendor Packages as a Separate Process** – This is a project organization and discipline application issue.
- **Equipment Tag Numbers and P&ID References**

Common PHA Quality Challenges (3)

- Programmatic Issues
  - **Facilitation/Scribe Team** – Maintain consistency with a smaller, dedicated set of individuals.
  - **Assignment of a Lead Facilitator for Large, Multi-Team Projects**
  - **Facilitator Synchronization Training**
  - **Focus on Long-Term Objectives** – The best approach to HAZOP/LOPA documentation is to focus on long-term objectives and potential uses, e.g., Project-MOC, Plant Operations MOC, SIL Assignment, future revalidation, etc.
  - **Quality Assurance Reviews Earlier in the Project Cycle**

Maximizing the Future Usefulness of the PHA



Maximizing the Future Usefulness of the PHA

- Apply Documentation Traceability Tips
- Prolific Use of Equipment Tag Numbers, P&ID References, & Cross-Referencing
- Sensible and Consistent Grouping of Scenarios
- Use Standardized PHA Approach
- Large Nodes Can Allow for a More Holistic Approach
- Qualifications and Experience of Facilitator & Team
- Consider Long-term Use & Strive for “Evergreen” Approach
- Software Longevity & Compatibility

Questions?

Steven T. Maher, PE CSP

Steve.Maher@RMPCorp.com

949/282-0123

www.RMPCorp.com

Risk Management Professionals