Assessing Meticulous Verification Effectiveness Utilizing HAZOP and LOPA

Mr. John T. Perez, P.E.
Cognascents Consulting Group, Inc.
1519 Vander Wilt Lane, Bldg. 4
Katy, TX 77449
john.perez@cognascents.com

Mr. William Wimberly, CSP
Cognascents Consulting Group, Inc.
billy.wimberly@cognascents.com

Prepared for Presentation at
American Institute of Chemical Engineers
2016 Spring Meeting
12th Global Congress on Process Safety
Houston, Texas
April 11-23, 2016

Assessing Meticulous Verification Effectiveness Utilizing HAZOP and LOPA

Mr. John T. Perez, P.E.
Cognascents Consulting Group, Inc.
1519 Vander Wilt Lane, Bldg. 4
Katy, TX 77449
john.perez@cognascents.com

Mr. William Wimberly, CSP
Cognascents Consulting Group, Inc.
billy.wimberly@cognascents.com

Keywords: AIChE, CCPS, Hazard and Operability Study (HAZOP), hazard identification, Independent Protection Layer (IPL), Layer of Protection Analysis (LOPA), meticulous verification (MV), Process Hazard Analysis (PHA), Process Safety Information (PSI), IPL integrity, Process Safety Management (PSM), Vision 20/20.

Abstract

In 2011, the Center for Chemical Process Safety initiated work on Vision 20/20. The goal of Vision 20/20 is to demonstrate what perfect process safety will look like when it is championed by industry; driven by five tenets of culture, standards, competency, management systems, and lessons learned; and enhanced by community passion and four global societal themes. The five tenets serve as a framework of what constitutes high-integrity, effective, and successful process safety management. The four global societal themes represent critical supporting efforts to the overarching five tenets.

One of the four global societal themes is meticulous verification. Meticulous verification provides the perpetual assurance of integrity for an organization's dynamic process safety management program. Meticulous verification specifically calls for collaboration between companies and third-party entities to ensure comprehensive and ongoing assessment of process safety management's effectiveness.

Based on the authors' experiences as HAZOP and LOPA facilitators, meticulous verification serves as the mission critical Vision 20/20 element for long-term sustainability. A HAZOP is a nexus of process safety information and process safety management systems' effectiveness and serves as a bellwether of an organization's overall PSM integrity. The integrity of a management system is only as strong as the discipline of its keepers to do the right thing irrespective of the consequences. This discipline is tested over and over again every day in HAZOP, as the HAZOP

team is relied upon to verify information for accuracy and applicability regarding a wide range of technical subject matter.

In this paper, the authors provide a detailed map of HAZOP and LOPA meticulous verification tasks and interactions. Specific examples of MV vulnerabilities and safeguards are provided to enhance the effectiveness of PHA teams. These vulnerabilities and safeguards address issues such as operating procedures and operator response, enabling and conditional modifiers, management of change, mechanical integrity and testing of safeguards and IPLs.

The target audience for this paper is anyone whose responsibilities include (1) leading within an organization required to comply with OSHA 1910.119, (2) establishing effective HAZOP and LOPA guidance documents, (3) developing high-integrity meticulous verification protocols and checklists, and (4) performing meticulous verification tasks such as technical assurance reviews.

1 Background and Purpose

CCPS's Vision 20/20 was developed to provide a picture of what perfect process safety may look like in the future when process safety is "championed by industry; driven by five tenets of culture, standards, competency, management systems and lessons learned; and enhanced by community passion and four global societal themes."[1] The five tenets serve as a framework of what constitutes high-integrity, effective, and successful process safety management. The four global societal themes represent critical supporting efforts to the overarching five tenets. One of the global societal themes is called Meticulous Verification (MV). CCPS's intentions regarding MV are described as:

- "Companies use various assessment techniques to assure their process safety management systems are working as intended.
- It will become standard practice for companies to supplement internal audits with competent third-party verification of their engineered systems and process safety management systems.
- Third-party technical experts verify specific technical details.
- Public and non-governmental organizations evaluate implementation of company process safety programs.
- Third-party assessments may identify additional opportunities for improvement in company process safety management and can enhance stakeholder relationships.
- Meticulous Verification supports a partnership to challenge each other to deliver great process safety performance."

Based on a recent conversation with the primary author of Vision 20/20, Mr. Jack McCavit, the authors of the Vision 20/20 MV material were focused on (1) enhancing collaboration between industry and third-party entities and (2) ensuring high-integrity compliance audits are performed by competent auditors.

The purpose of this paper is (1) to raise the awareness of MV's importance to process safety management sustainability and (2) to provide a practical approach to MV for enhanced and sustained process safety management integrity.

2 Current 1910.119 Verbiage

The current language in 1910.119(o) is as follows:

"Employers shall certify that they have evaluated compliance with the provisions of this section at least every three years to verify that the procedures and practices developed under the standard are adequate and are being followed.

The compliance audit shall be conducted by at least one person knowledgeable in the process.

A report of the findings of the audit shall be developed.

The employer shall promptly determine and document an appropriate response to each of the findings of the compliance audit, and document that deficiencies have been corrected.

Employers shall retain the two (2) most recent compliance audit reports."[2]

The PSM mandate as it stands today does not require third-party involvement for compliance auditing. 1910.119 also does not specify a required sample size. Aside from the Contractors element, third-party involvement is not required for any PSM element – not even for Process Hazards Analysis (PHA).

3 How Do Most Companies Meet Compliance Audit Requirement?

Companies achieve compliance with the Compliance Audit element by way of first, second, and/or third-party compliance audits of representative processing units, specific PSM elements, and/or PSM management systems.[3] A sample selection is reviewed for compliance against company policies, selected RAGAGEP, and 1910.119 (which can be supplemented by Letters of Interpretation (LOIs)). Sampling is an accepted method of auditing and a 100% review is not the norm. The three types of audits referenced above are defined as follows:

- First-party - organization internal auditors;
- Second-party - independent auditors outside of the organization; and
- Third-party - independent external auditors.[3]

4 So What's the Problem with Vision 20/20's End-Goal?

There is nothing wrong with the Vision 20/20 end-goal as intended by the original set of authors. Despite rumors and speculation, the authors of Vision 20/20 did not craft the MV language to imply more frequent audits and a larger sample size requirement. OSHA and other process safety advocates have expressed a desire for formal third-party audits and increased audit frequencies. More specifically, Executive Order 13650 is currently seeking comment on increasing the frequency of audits and mandating third-party audits as part of an overhaul of 29 CFR 1910.119.[4] In addition, it has come to the authors' attention via confidential sources that OSHA is evaluating a mandate that all information be reviewed during an audit rather than a

sample selection. However, the rhetoric being espoused and superimposed atop the Vision 20/20 program by regulatory entities and other PSM advocates is not realistic or achievable.

The major problems with increased audits and larger sample sizes are the time and money required to complete such audits. Should the vision become the reality, then compliance would become difficult as the resources required to complete future compliance audits would be impractical with respect to available competency and financial constraints. The benefit of increased sample sizes quickly reaches a point of diminishing returns.

Competency is not a problem. There are plenty of competent people capable of conducting PSM compliance audits. Availability is the problem. Take a minute and imagine the cost associated with an audit where 100% of the documents that can be audited are included in the scope. For a large refinery, a team of six people work long hours for an entire week and are still not able to guarantee a 10% sample size review. It would take months for the team of six auditors to perform an ***effective*** compliance audit consisting of a 100% review. Do we have enough competent people to complete audits of 100% of the information and personnel? Yes. But, are they available for the time necessary to complete the effective audits?

5 What Role Can HAZOP and LOPA Play Regarding MV?

As an alternative to increasing the compliance audit burden, we propose new HAZOPs and LOPAs as well as HAZOP and LOPA five-year revalidations be used as tools to assess a company's MV effectiveness. This would support CCPS's Vision 20/20 without significant modification to current compliance audit protocols or PHA practices.

A HAZOP is a nexus of process safety information, technical expertise, and process safety management systems' overall effectiveness; and serves as a bellwether of an organization's overall PSM integrity. The integrity of a management system is only as strong as the discipline of its keepers to do the right thing irrespective of the consequences. This discipline is tested over and over again every day in HAZOP and LOPA, as the PHA team is relied upon to verify information for accuracy and applicability regarding a wide range of technical subject matter. Figure 1 below depicts the various PSM elements that provide inputs and information to a PHA.

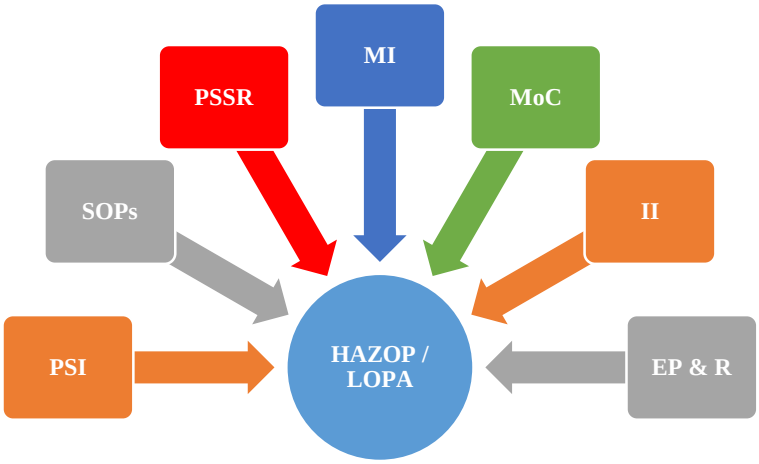

Figure 1: PSM Inputs to HAZOP/LOPA

As the previous figure depicts, one of the PSM elements feeding a HAZOP/LOPA exercise is Process Safety Information. A HAZOP should not be performed without first generating/obtaining and ensuring the integrity of the PSI. This effort ***is*** a compliance audit. It may not be documented as one or treated as one regarding formal team assignment and make-up, but it is a compliance audit. A team of experts is assessing the process safety information to determine whether it can be used to effectively identify, assess, and manage hazards. Figure 2 below depicts examples of process safety information used as inputs to a HAZOP/LOPA exercise.

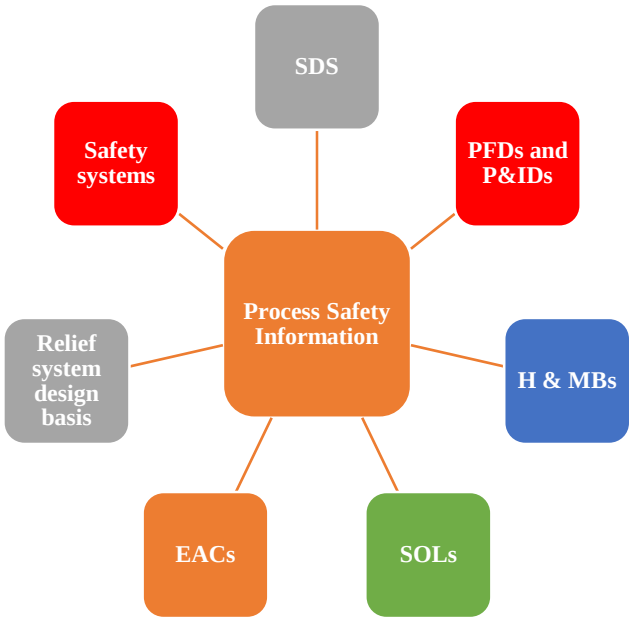

Figure 2: PSI Inputs to HAZOP/LOPA

Third-party facilitators are often used to manage the completion of HAZOP/LOPA exercises. Regardless of whether the facilitator is first-party, second-party, or third-party, their scope should already include the technical assessment of PSI prior to starting HAZOP/LOPA sessions; hence, adding formal MV assessment activity is more of a name change than anything else.

A company already performing PHAs similar to what is described above may leave current PSM compliance audit systems and protocols in place. If PSI is not being checked for technical accuracy before or during the HAZOP or LOPA, then it is not the compliance audit protocol that needs to change. In the authors' opinion, one of the major vulnerabilities with HAZOPs and LOPAs is the failure to ensure and assure the integrity of the PSI, which may result in the inability to adequately define a hazard or the associated risk. Identical to PSM compliance audits, questions need to be specific and comprehensive when assessing the technical accuracy of PSI. Questions may resemble the following:

1. Are the P&IDs accurate? When were they last walked down?
2. Have all MOCs been tracked? Have all impacted PSI been updated?
3. Have throughputs changed? If so, has the necessary information been updated?

4. If the PSI has changed due to an MOC, has a PSSR been performed?
5. How were the safe upper and lower operating limits set? Were process safety times calculated? Do SOPs, instrumented systems, alarms, and credit for operator response take process safety times into account?
6. Have safeguards been identified and documented? Are they robust enough to afford credit in a HAZOP?
7. Have IPLs been identified and documented? Do they meet all IPL criteria? How is their integrity maintained and assured? What kind of testing is performed?
8. Are relief devices sized for all potential overpressure scenarios? Do the technical assumptions match up with current design and operations? Does the field input data match the data used in the calculation files?

In the HAZOP, the facilitator should not take "Yes" at face value all of the time. The facilitator must drive and establish a culture of integrity through assurance. Take the time to check the information. "Checking" does not mean finding the information and verifying its existence. "Checking" means opening the file, looking at the assumptions, ensuring the technical basis matches current design and operation, cross-checking PSI across different data repositories, cross-checking PSI against SOPs, and doing anything else to assure the technical integrity of the PSI and other supporting information to the HAZOP/LOPA.

MV assurance proceeds from PSI assessment prior to conducting a HAZOP/LOPA through node definition, initiating event identification, consequence development, safeguard assignment, and risk-ranking. Each step of a HAZOP/LOPA can address MV assurance. Node definition requires rigorous scrutiny of the P&IDs and node boundaries. Node definition also includes checking/documenting design codes and standards. Equipment, piping, and instrumentation information is thoroughly reviewed to establish operating and design limits to determine appropriate deviations for analysis. Materials of construction, MAWPs, and MAWTs should all be checked.

As you move from node definition to the actual HAZOP/LOPA analyses, information regarding initiating events and consequence development move under the microscope. Once again, questions may resemble:

1. What can fail mechanically? Electrically? Hydraulically? Administratively?
2. What do the SOPs say specifically?
3. Are dispersion models completed? Are fire and blast studies complete and available? Does all of the information reflect current design and operating conditions?
4. How do the EACs impact consequences?
5. How does ventilation system design impact consequences with respect to emergency response and planning?
6. How do we handle check valves and restriction orifices? How do we ensure their integrity? Does it matter if a pressure relief device is sized assuming a check valve or RO is available?

Figure 3 depicts operating procedure inputs to HAZOP/LOPA exercises. Oftentimes, operating procedures are written by engineers and operators prior to commissioning and then updated after

commissioning to reflect final design and operating conditions. A HAZOP/LOPA is supposed to assess the hazards associated with all modes of operation. Hence, a valve being closed during one mode of operation may not be a problem, but may pose a serious threat during another mode of operation. It is common for alarms and interlocks to be disabled during temporary or abnormal modes of operation to facilitate non-routine maintenance or temporary operations. SOPs for non-routine modes of operation should be available, validated, and risk-assessed during the course of the HAZOP and LOPA.

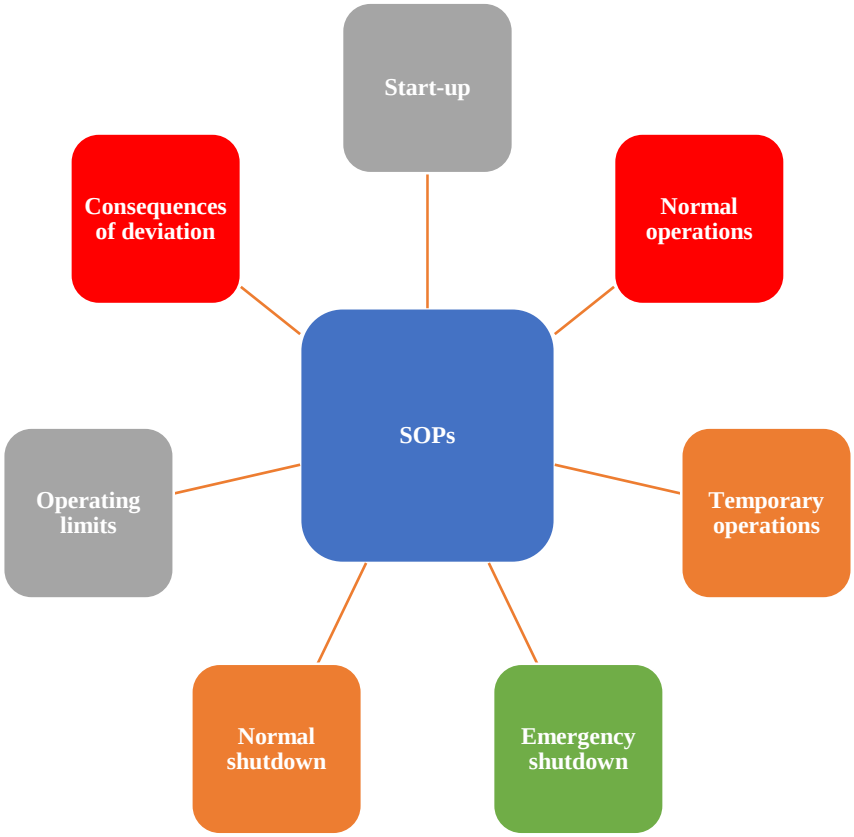

Figure 3: SOP Inputs to HAZOP/LOPA

An organization's mechanical integrity program can also be assessed during a HAZOP/LOPA. Mechanical integrity is sometimes cited as a safeguard. The authors agree that MI can be a safeguard, but only if the program is comprehensive, effective, and specific to the hazard identified. Credit for an MI program should only be taken after verification that the Inspection, Testing, and Preventative Maintenance (ITPM) methods and frequency are appropriate to the potential damage mechanisms identified by the HAZOP team. Likewise, a HAZOP/LOPA team should not take credit for any element whose function and availability is not assured by a high-integrity MI program.

For example, a pressure relief device can be sized correctly; however, if it has not been inspected and tested on a frequency fitting to its service, then it is not a reliable and effective IPL and safeguard. The same applies to safety-instrumented functions (SIFs) or high-integrity pressure protection systems (HIPPS).

6 What Role Can HAZOP and LOPA Play Regarding MV?

In an effort to provide the reader with an effective MV assessment tool, the authors have compiled a checklist of the various activities they perform before and/or during a HAZOP and LOPA. The following checklist serves as a sample MV assessment guidance document for a HAZOP/LOPA effort:

Table 1: Meticulous Verification Assessment Checklist for HAZOP/LOPA

HAZOP Phase	Specific Element	Meticulous Verification Checkpoint	OSHA CFR Reference
Data Collection:	MOC	☐ Current P&IDs reflect MOC changes ☐ Current operating procedures reflect MOC changes ☐ Current SIF safe charts reflect MOC changes ☐ Current relief valve calculations reflect MOC changes	1910.119(f)(3) 1910.119(d)(3)(i)(B) 1910.119(l)(4) 1910.119(l)(5)
	Field Walkdown Efforts	☐ Field walkdown and red line efforts have been captured on HAZOP P&IDs	1910.119(d)(3)(i)(B)
	Recommendation Close-out Identification	☐ Closure of recommendations from previous hazard assessments/audit findings are identified in tracking system	1910.119(e)(5) 1910.119(e)(7) 1910.119(o)(4)
	Previous Recommendations	☐ PSI reflects actions associated with recommendation closure from previous hazard assessments/audit findings	1910.119(e)(5) 1910.119(d) 1910.119(o)(4)
	Process System Selection	☐ Systems approaching 5 year hazard assessment revalidation deadline is on upcoming PHA schedule	1910.119(e)(6)
	Risk Communication	☐ Hazards identified in previous hazard assessments have been communicated to employees	1910.119(d)
Node Definition	Process Parameters	☐ Mechanical design limit documentation (U1, Pipe spec, etc.) is consistent with limits on P&IDs and operating procedures safe operating envelope	1910.119(d)(2)(i)(D)
		☐ Process equipment parameters are available to properly evaluate excursions from safe operating limits (pump curves, heater/exchanger spec sheets, etc.)	1910.119(d)(2)(i)(E)
		☐ Heat and material balance reflects current throughputs	1910.119(d)(3)(i)(G)
		☐ Heat & Material Balance reviewed and is within mechanical limits. (relief valve set points, U1 MAWP, etc.)	1910.119(d)(3)(i)(G)
		☐ Material chemical properties such as toxicity, corrosivity, reactivity, mixing, etc are available (chemical compatibility matrix, corrosion table, etc.)	1910.119(d)(1)(i-vii)
		☐ Materials of construction and compatibility with process is documented (corrosion tables, etc.)	1910.119(d)(1)(v)
		☐ Out of service equipment and piping is depicted accurately	1910.119(d)(2)
		☐ Operating modes are documented for all design intents of the process	1910.119(f)(1)(i)
Initiating Event Development	Operator error	☐ Operator refresher training is up to date and documented	1910.119(g)(2) 1910.119(g)(3)
		Managed valve system/log is adequate. ☐ Up to date ☐ Documented via a procedure ☐ Audited for accuracy and is consistent with initating event likelihood developed by team	1910.119(d) 1910.119(f)(1)(iii)(B) 1910.119(o)(1)

HAZOP Phase	Specific Element	Meticulous Verification Checkpoint	OSHA CFR Reference
		The operator error rate assumptions are defensible for the scenario developed ☐ Number of opportunities for the operator to make mistake is defensible ☐ Personnel that may be involved is included in training regimen ☐ Procedure details the operation and is clear ☐ Operator stress level is consistent with scenario developed by team ☐ Error rate accounts for similar valves/controls or confusing layout that may facilitate a higher rate	1910.119(f)(1) 1910.119(g)(3) 1910.119(3)(vi)
	Credibility	If a scenario has been determined to be "not credible" ☐ Documentation is available demonstrating defensibility ☐ Scenario meets threshold for establishing credibility	1910.119(e)(3)(i)
	Mechanical Failure	☐ Repair logs associated with the scenario developed by the team are consistent with initiating event likelihood developed	1910.119(j)(5) 1910.119(j)(4)(iii)
		Equipment addressed by scenario developed by team is captured by Inspection Test Preventative Maintenance (ITPM) Plan. Verify: ☐ Inspections up to date ☐ Testing is current ☐ Maintenance activities up to date ☐ Deficiencies have been corrected ☐ MOC changes were incorporated	1910.119(j)(2) 1910.119(j)(4) 1910.119(l)(1)
		☐ PMI records are available for piping/equipment associated with alloys	1910.119(j)(6)
	Previous Incidents	☐ Previous incidents and near misses are identified, investigated, and documented	1910.119(e)(3)(ii) 1910.119(m)(1) 1910.119 Appendix C (12)
		☐ Previous incidents recommendations/corrective actions are addressed/implemented and documented	1910.119(m)(5)
Severity Development	Safety	☐ Personnel Distribution is accurate and is reflective of scenario developed by team. (Specific operations should document personnel required and their exposure level for the operation)	1910.119(e)(3)(v) 1910.119(n)
		☐ Dispersion analysis is based on flow rate developed by scenario	1910.119(e)(3)(iv) 1910.119(e)(3)(v)
		☐ Process Safety Time is documented for the specific scenario developed by team.	1910.119(j)(6)(i)
		☐ Excursion rate/release volume calculations available or understood for the specific scenario developed by team	1910.119(e)(3)(iv-v) 1910.119(n)
		☐ Blast/Radiation Study is reflective of specific scenario developed by team (release volumes, congested volume calculations, released material properties)	1910.119(e)(3)(iv-v) 1910.119(n)
Likelihood Development	Conditional modifiers	☐ Ignition probability is based on congestion of equipment where flammable cloud may exist	1910.119(e)(3)(v) 1910.119(n)
		☐ Plot plan is reviewed to verify that ignition probability encompasses impact of surrounding equipment (fired equipment, open flames, etc.)	1910.119(e)(3)(v) 1910.119(n)

HAZOP Phase	Specific Element	Meticulous Verification Checkpoint	OSHA CFR Reference
		Enabling condition modifiers: ☐ Justification documented (historical performance, published industry data, previous experience, internal defined criteria) ☐ Applicable to hazard scenario developed by team	
		Time at risk factors☐ Justification is documented (historical performance, published industry data, previous experience, internal defined criteria)☐ Applicable to hazard scenario developed by team	1910.119(f)(1)
		Occupancy factors ☐ Justification is documented (historical performance, published industry data, previous experience, internal defined criteria) ☐ Applicable to hazard scenario developed by team ☐ Reviewed against facility personnel distribution ☐ Hazard Scenario occupancy factor accounts for foreseen action by operator on upset/alarm or automated response from a safety system	1910.119(e)(3)(v)
	Emergency Response	☐ Emergency response plan is documented and is adequate for the scenario developed by the team	1910.119(n)
		☐ Emergency response personnel are trained and training is up to date	1910.119(f)(1)(i)(E)
	Dikes/Bunds	☐ Volume of dike/bund meets design code requirements and documentation is available	1910.119(d)(3)(i)(F)
		☐ Dikes/Bunds ITPM is documented and adequate	1910.119(j)(4)
	Deluge Systems	☐ Deluge system coverage and operation is adequate for system and scenario developed by team	1910.119(f)(1)(iv) 1910.119(d)(3)(i)(H)
		☐ Deluge ITPM is documented and adequate	1910.119(j)(4)
	Hazardous Area Classification	☐ Electrical Area Classification drawings are up to date	1910.119(d)(3)(i)(C)
	Flow Restriction Orifices	☐ Orifice ITPM is documented and up to date	
		☐ Orifice calculations are available and document acceptable flow reduction for scenario developed by team	
	Pressure Relief Devices	☐ Selected relief device calculation files are up to date and are adequately sized for specific scenario identified by team	1910.119(d)(3)(i)(D)
		☐ Relief Valve / Effluent System ITPM is documented and up to date	1910.119(j)(4)
		☐ Hazards associated with discharge of the relief valve for the specific scenario are reviewed	1910.119(e)(3)(iv)
	Gas Detection Systems	☐ Gas Detection System ITPM is documented and up to date	1910.119(j)(4)
		☐ Gas detection alarms sound at or prior to reaching concentration of interest for the specific gas of interest depicted by the HAZOP scenario (STEL, PEL, LEL%)	1910.119(d)(3)(i)(H) 1910.119(d)(3)(ii) 1910.119(d)(1)(ii)
		☐ Gas detection systems cover area in question and are depicted appropriately on drawings	1910.119(e)(3)(v)
	Pump/Compressor Seals	☐ Seal systems vent to safe location and are depicted accurately on P&IDs	1910.119(d)(3)(i)(D) 1910.119(d)(3)(i)(H)
		☐ ITPM is documented and up to date	1910.119(j)(4)
	Redundant Equipment	☐ ITPM is documented and up to date	1910.119(j)(4)

HAZOP Phase	Specific Element	Meticulous Verification Checkpoint	OSHA CFR Reference
		☐ Operating procedures are available detailing redundant equipment and training is provided for its use	1910.119(f)(1)(i)(C) 1910.119(f)(1)(iii)(B) 1910.119(g)(1) 1910.119(j)(6)(iii)
		☐ Redundant equipment is documented to have capacity to meet 100% of demand (lead/lag systems may not provide full redundancy)	1910.119(j)(6)(iii)
	Spare Equipment	☐ ITPM is documented and up to date for spare	1910.119(j)(4)
		☐ Spares meet design specification	1910.119(j)(6)(iii)
		☐ PMI is confirmed for spares prior to use	1910.119(j)(6)(iii)
		☐ Inventory list confirms that spares are available	1910.119(j)(6)(iii)
		☐ Redundant equipment is documented to have capacity to meet 100% of demand (lead/lag systems may not provide full redundancy)	1910.119(j)(6)(iii)
	Ventilation Systems	☐ Ventilation systems is documented to be adequate for scenario developed by team	1910.119(d)(3)(i)€
		☐ Ventilation systems ITPM is documented and up to date	1910.119(j)(4)
	Check Valves	☐ ITPM is documented and up to date	1910.119(j)(4)
		☐ Check valve is designed for process service (vibration, clean/dirty, temperature, etc.)	
		☐ Repair, testing, and operating history demonstrates acceptable performance	1910.119(j)(5) 1910.119(j)(4)(iii)
	Cathodic Protection Systems	☐ ITPM is documented and up to date	1910.119(j)(4)
	Exclusion Zones	☐ Exclusion zones are enforced	1910.119(f)(1)(iii)(B)
		☐ Exclusion zones are readily identifiable	1910.119(f)(1)(iii)(B)
		☐ Exclusion zone boundaries are effective (cover radiation limit, dispersion limit, etc.)	1910.119(f)(1)(iii)(B)
		☐ Adequate procedures exist for operation within an exclusion zone	1910.119(f)(1)(iii)(B)
	Independent Monitoring / Third Party Monitoring	☐ Procedure exists detailing independent activity monitoring and procedure documents independence from person/equipment performing the task identified by the hazard scenario	1910.119(e)(3)(iii) 1910.119(f)(1)(iii)(B)
		☐ Training is documented for personnel involved	1910.119(e)(3)(iii) 1910.119(f)(1)(iii)(B)
		☐ Procedure has been reviewed by operations	1910.119(e)(3)(iii) 1910.119(f)(1)(iii)(B)
	Safety Showers/Eye Wash Stations	☐ ITPM is documented and up to date	1910.119(j)(4)
		☐ Operating procedures and operator training identifies the locations	1910.119(f)(1)(iii)(B)
	Process Alarms	☐ ITPM is documented and up to date	1910.119(j)(4)
		☐ Independence of alarm is verified and found to be adequate ☐ Separate controller from failure identified in hazard scenario ☐ Separate sensor from failure identified in hazard scenario ☐ Separate I/O card from failure identified in hazard scenario ☐ Separate final element from failure identified in hazard scenario	

HAZOP Phase	Specific Element	Meticulous Verification Checkpoint	OSHA CFR Reference
		☐ Process safety time is adequate to allow for response and correction to safe condition	1910.119(e)(3)(iii)
		☐ Alarms are consistent across PSI (P&ID, DCS, Cause and Effects, Human-Machine Interface)	1910.119(d)(3)(i)(H)
	Safety Critical Alarms	☐ Specific alarm response is documented within a procedure	1910.119(f)(1)(i)(C/E)
		☐ Alarm is confirmed to be unique (identifiable amongst multiple alarms)	
		Independence of alarm is verified and found to be adequate: ☐ Separate controller from failure identified in hazard scenario ☐ Separate sensor from failure identified in hazard scenario ☐ Separate I/O card from failure identified in hazard scenario ☐ Separate final element from failure identified in hazard scenario	
		☐ ITPM is documented and up to date	1910.119(j)(4)
		☐ Access security for set points / bypass of alarm is verified to be limited to required personnel only	
		☐ Process safety time is documented to be adequate to allow for response and correction to safe condition	1910.119(e)(3)(iii)
		☐ Alarms are consistent across PSI (P&ID, DCS, Cause and Effects, Human-Machine Interface)	1910.119(d)(3)(i)(H)
		☐ Specific Response is detailed in operator training	1910.119(g)(1)(i)
	BPCS functions	☐ Response time is documented to be fast enough to meet Process Safety time	1910.119(e)(3)(iii) 1910.119(d)(3)(ii)
		Independence of function is verified and found to be adequate ☐ Separate controller from failure identified in hazard scenario ☐ Separate sensor from failure identified in hazard scenario ☐ Separate I/O card from failure identified in hazard scenario ☐ Separate final element from failure identified in hazard scenario	
		☐ ITPM is documented and up to date	1910.119(j)(4)
		☐ PSI documentation is consistent and accurate (P&ID, DCS, Cause and Effects, Human-Machine Interface)	1910.119(d)(3)(i)(H)
		☐ BPCS function has adequate capacity to mitigate scenario developed by team (e.g. minimum flow recirculation line has adequate recycle flow to prevent deadhead)	1910.119(e)(3)(iii) 1910.119(d)(3)(ii)
	Safety Instrumented Systems	☐ SIS/SIF calculations are documented for SIL	1910.119(d)(3)(ii) 1910.119(d)(3)(i)(H)
		Independence of function is verified and found to be adequate: ☐ Separate controller from failure identified in hazard scenario ☐ Separate sensor from failure identified in hazard scenario ☐ Separate I/O card from failure identified in hazard scenario ☐ Separate final element from failure identified in hazard scenario	
		☐ ITPM is documented and adequate for SIL	1910.119(j)(4)

HAZOP Phase	Specific Element	Meticulous Verification Checkpoint	OSHA CFR Reference
		☐ Actual SIS/SIF set points match documentation	
		☐ Access security is verified to be limited to required personnel only	
		☐ Operating procedures for activities involving safety systems and functions are available	1910.119(f)(1)(iv)
		☐ Any manual over-rides of SIS/SIF are documented and risk assessed	1910.119(f)(1)(iv) 1910.119(f)(4)

7 MV Assurance Deliverables

Efforts utilizing HAZOP and LOPA for MV assurance should produce a formal deliverable to serve as a document of record. This deliverable should be separate from the PHA report as the actions may not be driven by a specific hazard scenario and subsequent risk-ranking designation. The report does not have to be burdensome on the PHA team, but it should include the following elements:

1. Executive summary;
2. Details of MV assurance team (name, title, role, years of experience, contact information);
3. Details of MV assurance activity and protocols (checklists incorporated, information reviewed, sample size, personnel interviewed, observations made);
4. Part of 1910.119 where potential non-compliance may exist;
5. Proposed actions specific to the MV assurance scope; and
6. Description of management review process to approve or reject proposed actions.

8 Supporting Cast and Criteria

For effective use of HAZOP and LOPA to assess the integrity of a company's MV efforts, the following elements must be in place:

1. The right culture/mindset/attitude to facilitate an effort focused on making facilities safer and better.
2. Authentic management support and understanding of what MV means and requires regarding time, money, and competence.
3. A HAZOP/LOPA team of competence and accountability dedicated to the discipline required to check information with relentless vigilance.
4. PSM documentation control systems in place to generate, maintain, and facilitate MV integrity.
5. Humility to recognize third-party entities may bring valuable expertise and value to MV exercises.

Without the above elements in place, the team will not devote the time required to support the MV assurance tenet of CCPS's Vision 20/20 because the value will not be enough to break through the obstacles.

9 Conclusion

Based on the authors' experience as HAZOP and LOPA facilitators, MV serves as the mission critical Vision 20/20 element for long-term sustainability. There is nothing wrong with the Vision 20/20 end-goal as intended by the original set of authors. Despite rumors and speculation, the authors of Vision 20/20 did not craft the MV language to imply more frequent audits and a larger sample size requirement.

Adding more burdensome PSM compliance audit requirements is not a problem of competency – it is a problem of availability. The authors posit the use of HAZOPs and LOPAs to help organizations achieve the intent of CCPS's Vision 20/20 MV challenge of using third-parties and enhanced collaboration between public, regulatory, and non-governmental organizations to increase the integrity of process safety management systems and information.

Increasing the integrity of HAZOPs and LOPAs requires meticulous verification, which should already be occurring more than observed. The authors have provided a comprehensive checklist to assist organizations in improving their MV efforts by raising the standard of excellence regarding facilitator and PHA team expertise and discipline.

MV is not a one-time task that is done every other day or week. MV is perpetual vigilance performed by available competence.

10 References

[1] CCPS, "Vision 20/20," Available at www.aiche.org/ccps/resources/vision-2020 (accessed January 2016).

[2] OSHA, "1910.119 Process Safety Management of Highly Hazardous Chemical," Available at www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9760 (accessed January 2016).

[3] B.D. Rains, "Process Safety Management What Is the Right Audit Approach for You?", DuPont, Copyright © 2009.

[4] B. Obama, "Executive Order – Improving Chemical Facility Safety and Security," Available at www.whitehouse.gov/the-press-office/2013/08/01/executive-order-improving-chemical-facility-safety-and-security (accessed January 2016).