The Use of Inherent Layers of Protection to Create Line-of-Sight Between Individual Activities and Process Safety Performance

Fred Henselwood
CSChE 2017 - Edmonton
Overview

How we are putting the pieces together

• About NOVA Chemicals
• Layer of Protection Model
• CCPS Vision 2020 Model
• The Role of Culture
• Lagging Metrics
• Conclusions
About NOVA Chemicals
When Responsible Care was developed in 1985, it was an expression of the chemistry industry’s commitment to safety. Over the years it has evolved into the industry’s commitment to sustainability – the betterment of society, the environment and the economy.

• NOVA Chemicals is committed to being a leader in achieving superior Responsible Care performance
• We value the safety and well-being of our co-workers, communities and the environment.
• Each of us is responsible for our own personal safety and the safety of the people and environment around us.
• We are committed to a zero-injury workplace.
Locations & Fast Facts

- **Number of Employees**: 2,800 worldwide
- **Annual Sales, 2016 (U.S.$)**: $3.5 billion
- **Leadership**
  - Todd Karran
  - CEO
- **Products**
  - Ethylene and Polyethylene Chemical Co-Products
  - Expandable Styrenic Polymers
- **Community Investment/Giving**
  - $2.3 million (USD)
  - 7,000 hrs
Layer of Protection Model
What is Process Safety?

Definition – https://www.aiche.org/ccps/about/process-safety-faqs

• "Process Safety is a blend of engineering and management skills focused on preventing catastrophic accidents, particularly explosions, fires, and toxic releases, associated with the use of chemicals and petroleum products." - Center for Chemical Process Safety

• Layers of Protection is a concept that multiple lines of defense combining actions directed by Engineering, Operations, and Maintenance can significantly reduce the likelihood of catastrophic Process Safety incidents from occurring.
Think About a Car

What is Safe?

- You can Engineer a Car to travel “safely” at a speed of 100 km/hr
  - What if you never do any maintenance, is it still safe to drive?
  - What if you travel at a 200 km/hour, is it still safe to drive?

- Engineering, Operations, and Maintenance need to work together to ensure the safe operations of the vehicle
  - The vehicle design, safety systems, the driver interface, driver training, ability to do maintenance, life and reliability of the components…

- Plus you need a Committed Culture
  - Are you committed to driving safely?
Swiss Cheese Model

Preventing Hazards from becoming Losses
http://en.wikipedia.org/wiki/Swiss_cheese_model#

- Process Safety incidents typically involve an initial failure followed by a series of additional failures and/or the discovery of preexisting failures
  
  → 1 in 500 year flood (Initiating Event)
  
  → Built to a 1 in 100 year flood (Design Choice Made)
  
  → Pump failed to start due to fuel issues (Revealed Failure)
    
  → Responded to wrong pump station (Mistake Made)

→ There are Opportunities for Engineering, Operations, and Maintenance to influence this example
La Porte Incident

Chemical Safety Board Investigation

La Porte Incident

- November 15, 2014
- Four DuPont employees were killed
- 24,000 lbs of highly toxic methyl mercaptan released on and off site
- Release occurred inside an enclosed building
- All four employees were inside the building
- Two of the four fatalities occurred during rescue
- DuPont employed 300 personnel at the site
La Porte Incident – the Swiss Cheese Model

Preventing Hazards from becoming Losses

• There were Operations, Maintenance, and Engineering failings in this incident

• Why would multiple groups fail?

→ Culture tends to be the element linking each of these failures
  → The organization likely knew better, but their programs failed
  → There was gap between what they “Asked” for and what they “Accepted”
Layer of Protection Approach

Objective

• Ensure that each inherent Layer of Protection is properly managed
  • What does Engineering need to do?
  • What does Operations need to do?
  • What does Maintenance need to do?

• How do we know each Layer of Protection is healthy?
  • What are the Deliverables?
  • What are the Leading and Lagging Metrics?

• How do we create line-of-sight between individuals and Process Safety?
Layer of Protection Model

“Onion Skin Diagram” – See CCPS “Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis” for more details – model adapted for NOVA Chemicals
Process Chemistry

First Layer

• What is the **Chemistry** that you are trying to control?
  • Chemicals and related reactions bring with them inherent hazards
    • Propane can Explode, Chlorine is Toxic, Nitrogen can Asphyxiate, Triethylaluminium is Pyrophoric…
  • Physical Properties (e.g. temperature) can also create hazards

• This Layer of Protection often focuses on Inherent Safety
  • Can we Minimize, Substitute, or Moderate our chemical processes?
    • Can we substitute for a safer chemical (Bleach for Chlorine)?
    • Can we minimize inventories?
      • The Bhopal tragedy involved the release of an intermediate
    • Lower pressures are typically safer than higher pressures
Runaway: Explosion at T2 Laboratories – CSB Video
http://www.csb.gov/t2-laboratories-inc-reactive-chemical-explosion/

• Exothermic reaction failed to be controlled when the cooling system malfunctioned
• Runaway reaction resulted which gave rise to rapid pressure and temperature increases
• Massive explosion occurred resulting in 4 Fatalities and the destruction of the business
Process Equipment and Design Intent

Second Layer

• How do we Contain the Hazards associated with our Process Chemistries?
  • Our Process Design is the Equipment which contains the Hazards related to our Process Chemistries
  • This Layer of Protection is about containing the Inherent Hazards associated with our facilities
  • The simpler the design the easier it is to maintain and operate

• A key metric for this Layer of Protection is Loss of Primary Containment
  • i.e. are our Hazards Contained within our Processes as intended
Fatal Exposure: Tragedy at DuPont – CSB Video
http://www.csb.gov/dupont-corporation-toxic-chemical-releases/

- Transfer hose ruptured while containing highly toxic Phosgene
- Hose replacement was missed due to errors made in the SAP system
- A Stainless Steel hose was used in place of a preferred Monel hose
- Toxic release occurred resulting in 1 Fatality and 2 employees being exposed
Basic Process Control System

Third Layer

• How do we Manage and Operate our Process Equipment?
  • Our BPCS is the collection of tools and procedures we use to manage our facilities
  • This Layer of Protection is about controlling our chemical properties and the related reactions within our Process Equipment

• This Layer focuses on Operations
  • A key aspect to this Layer of Protection is having high quality operating procedures which are current, easy to follow, and highlight the process hazards which are being managed
Basic Process Control System

Explosion at Formosa Plastics (Illinois) – CSB Video

- Operator opened the wrong valve
  - Believed to be working on a tank in a cleaning cycle but actually opened an operating reactor
- Resulting vinyl chloride release resulted in a fire and an explosion
- 5 Fatalities
- The facility was never re-opened
Critical Alarms and Operator Response

Fourth Layer

- This Layer is about **Regaining Control** of our process if something were to occur
  - How do we know we have a problem occurring?
  - What actions would we take and how quickly?
  - What are we doing to ensure those actions are successful?

- This Layer of Protection focuses on Emergency Operating Procedures
  - A key metric would be the number of deviations from Safe Operating Limits
Critical Alarms and Operator Response

Fire in the Valley – CSB Video

- Safety Interlock Bypassed during start-up
- Critical Alarms were missed and/or not properly responded to
- Massive explosion occurred resulting in 2 Fatalities
Safety Instrumented Systems

Fifth Layer

• This Layer of Protection is about having safety systems in place to Protect our Equipment if we are unable to control our processes
  • Safety Instrumented Systems (SIS) play a key role in ensuring our facilities operate within acceptable levels of risk
  • What are the triggers to activate our SISs and what actions do these systems take?

• The high reliability required of SIS is critical to their success
  • But this can be very challenging to design for (often SIS needs to be independent of other safeguards)
  • Proof testing is critical to ensure desired reliability and functionality
  • False (spurious) trips of SIS can also create significant risks
Safety Instrumented Systems

Deepwater Horizon Blowout Animation – CSB Video
http://www.csb.gov/macondo-blowout-and-explosion/

- 11 Fatalities resulted from an explosion following the blow-out of a well being drilled
- The spill was the largest oil spill in US history
- The blow-out preventer failed to control the event as planned and this failure highlighted the complexity of the blow-out preventer (their SIS) and the difficulties related to designing and testing these systems
Physical Protection Systems

Sixth Layer

- This Layer of Protection is about having the ability to **Manage excess Energy** within our processes

- Pressure Relief Devices are an example of this Layer of Protection
  - In the event of a build-up of excessive energy (typically pressure) how do we vent this energy to a safe location in order to protect our people and facilities
  - Other examples of Physical Protection Systems would be Flame Arrestors, Explosion Relief Systems, Rupture Disks…

- A key metric would be the activation of Process Safety Devices
Physical Protection Systems

Without Safeguards, Pressure Vessels Can Be Deadly – CSB Video
http://www.csb.gov/videos/without-safeguards-pressure-vessels-can-be-deadly/

• Following maintenance a PSV was left blocked in

• A heat exchanger was subsequently over-pressured with Ammonia
  • There was no ability to relieve the built-up pressure

• The Heat Exchanger explosion resulted in 1 Fatality
Post Release Protection Systems

Seventh Layer

• This Layer of Protection is about the steps and processes we have in place and those processes that **Activate and Engage at the time of the event**
  • How do we manage the hazard following loss of containment?
    • Can we limit the material being released through remote emergency valves?
    • How do we put out or prevent a potential fire (without ignition we would never experience a fire)?
  • Where do the released materials go?
  • How are we protecting people (Blast resistant structures)?
  • Buffer zones are also excellent ways to manage potential impacts
• How do we control the event so as to minimize the potential harm?
Blast Wave in Danvers – CSB Video
http://www.csb.gov/videos/blast-wave-in-danvers/

- Community of Danvers, MA was badly damaged following the explosion of accidentally released solvents used in ink manufacturing
- 10 residents injured
- 300 residences and 10 businesses were evacuated
- 77 families displaced while their homes were repaired (25 homes destroyed)
- Buffer zones were not maintained and homes were constructed too close to the facility relative to the potential hazards
Plant Emergency Response

Eight Layer

• This Layer of Protection is about **Safeguarding our People and our Facilities** in the event of an emergency
  • How do we manage a potential event?
    • How do we activate our Emergency Operations Centers?
    • How do we get people to safe locations and keep them safe?

• What steps do we take?
Plant Emergency Response

Chevron Richmond Refinery Fire Animation – CSB Video
http://www.csb.gov/chevron-refinery-fire/

- Emergency Responders investigating a small leak unintentionally causing the leaking pipe to rupture
- The plant was operating during the leak investigation and failed to shutdown while the initial event continued to escalate
- 19 workers exposed to the release, 1 worker trapped in a vehicle during the fire and explosion, and 15,000 members of the public sought medical treatment
Community Emergency Response

Ninth Layer

• This Layer of Protection is about **Safeguarding our Communities and the Environment** in the event of an emergency
  • How do we manage the event?
    • How do we contact others in the event of an emergency?
    • How do we protect the community?

• How do we get help and how do we protect others?
Community Emergency Response

Ninth Layer

- 15 Fatalities and over 160 injuries
- Over 150 buildings damaged or destroyed
- Many of those killed were First Responders
  - First Responders should never have been at risk
Other Groups Also have a Role to Play

Beyond Design, Operations, and Reliability Intent

• Procurement
• Logistics
• Information Technology
• Human Resources
• Health, Safety, and Environment
• Leadership
• …

• An exercise we use is to give leaders sticky notes and have them post where they see themselves playing a role within the matrix formed by the Layer of Protection model and the different life-cycle stages (intent)
CCPS Vision 2020 Model
A Model for Process Safety
https://www.aiche.org/ccps/resources/vision-2020

Industry Tenets

• Committed Culture
• Vibrant Management Systems
• Disciplined Adherence to Standards
• Intentional Competency Development
• Enhanced Application & Sharing of Lessons Learned

Societal Themes

• Enhanced Stakeholder Knowledge
• Responsible Collaboration
• Harmonization of Standards
• Meticulous Verification
Example of a Vibrant Management System

Physical Protection Systems

• As an example Pressure Safety Valves
  • **Design intent**, documentation describing the intended design and related hazard scenario(s)
    • Maintained and controlled documentation
    • Updated through Management of Change process as applicable
    • Reviewed through 5-year Process Hazard and Risk Assessment (PHRA) program
  • **Operations intent**, management and awareness of potential impairments
    • Including risk assessment of impairments and escalation based on times involved
    • Alternate relief strategies, Car Seal programs
  • **Reliability intent**, testing at a frequency and scope to ensure the intended reliability
    • Programs for bringing PSVs in and out of service to allow for testing
    • Documentation of the test results
Example of Disciplined Adherence to Standards

Process Equipment and Design Intent

- Application of internal Loss Prevention and Engineering Standards when designing equipment (often referencing external standards)
  - Application of Facility Change Management Process when making changes
  - Application of Process Safety Life-Cycle Guidelines when assessing risk (design, changes, 5-year PHRA program)
- Operations within Safe Operating Limits while in service (boundaries)
- Application of Risk Based inspection programs during the life of the facility
- Application of Out-of-Service Equipment program when no longer in use
- RAGAGEPs – Recognized and Generally Accepted Good Engineering Practices
Example of Intentional Competency Development

Safety Instrumented Systems

- What does someone need to know to design these systems?
  - What about associated programs like Management of Change?
- What does someone need to know to Operate in partnership with these programs?
  - Again, what about associated programs like Impairment Management?
- What is unique about the testing and maintenance programs for SISs?
  - i.e. what does Assurance and Competency look like for Safety Instrumented Systems?
    - Are SIS being used properly to provide the risk reduction level that is required?
Examples of Lessons Learned

Post Release Protective Systems

• Lots of ways for a PSV to potentially Fail
  • Wrong design (or wrong PSV installed)
  • Found impaired
  • Failed when tested
  • Failed when called upon
  • Worked as per design when called upon (still an incident as earlier layers should have prevented the need for this safeguard to act)

• What can we learn from each individual failure?
• What can we learn from the collection of related failures?
  • How do we institutionalize these learnings once we find them?
The Role of Culture
A Working Definition for Culture

Our Model, and the Importance of Leadership

• What is it that the **Company** is "**Asking**" for?
  • Management Systems and Standards

• What is it that the **Leadership** "**Accepts**"?
  • What actually gets done

• Culture can be defined as the gap between "Ask" and "Accept"
  • The La Porte incident demonstrated several gaps between "Ask" and "Accept"
  • How do you work at closing this gap?
Committed Culture – Core of the Vision 2020 Model

Elements of Culture

• Voice
  • Felt Leadership
  • People Speaking up
  • Open Communication

• Emotion
  • Sense of Vulnerability
  • Pride in our Work
  • Sense of Community

• Discipline
  • Doing things the Right Way
  • Thoughtful Compliance
  • Being Consistent
  • Timely Action
  • Verification
Voice

We need to start a Conversation to ensure we are exchanging information

• Felt Leadership
  • Training for leaders on what to look for and ask for
  • Definition of Culture as the Gap between what programs “Ask” for and what leaders “Accept”

• People Speaking up
  • Safety Interactions (Recognizing good conversations about Process Safety)
  • Safety Moments for meetings (making sure there is Process Safety content available)
  • Encouraging junior people to participate in hazard reviews (new set of eyes)

• Open Communication
  • Fostering the flow of information
  • Sharing of Incidents, Sharing of Metrics
Leadership Field Questions

Process Chemistry

• Questions to Ask
  • What are our Process Hazards?
    • Do we understand the properties associated with each of the chemicals we work with?
    • Are there chemical reactivity concerns?
  • Are there unnecessary Hazards associated with our Process?
  • Can we operate under safer conditions?

“What you don’t have, can’t leak” (Trevor Kletz)
We need to be Predictable

- Doing things the Right Way
  - If the procedure isn’t right, fix the procedure
  - Avoid short-cuts (I use the Jaywalking analogy a lot)
  - Understand why all the steps are done (links back to training)
- Thoughtful Compliance
  - Beyond check the box – thinking vs. doing
- Assurance, Competency, Verification
  - How do we know we have done things right
  - There isn’t a gap between “Ask” and “Accept”
Spot the Hazard

Monthly Promotion Program

• Encourages employees to identify Process Safety Hazards
  • Creates a safe environment to practice identifying concerns
  • Explanations our provided for previous months
• If people can apply this skill in an online setting we would then look for them to apply these skills in the field
  • We get a lot of responses from non-field staff, which is also positive
Emotion

How do we connect with our work

• Sense of Vulnerability
  • Need to know how our work relates to Process Safety
  • Need to recognize that the difference between good luck and good management is difficult to separate

• Pride in our Work
  • Doing the right work with the proper effort
  • Looking to deliver the “Ask”

• Sense of Community
  • This is about our safety, the safety of our coworkers, the safety of our community
  • Everyone needs to be invested in the work
We can’t forget our history

- Program focuses on reinforcing that things have happened in our past and that we need to remain vigilant
  - Documents speak more to the events and less to the very specific learnings from the events (tendency to focus on general learnings)
- Many of our newer staff do not know the history of our organization
  - With retirements, this knowledge is at risk of being lost
Metrics
External Requirements (CIAC/ACC) – Graphic taken from CCPS Publication


Figure 1: Process Safety Metric Pyramid

Process Safety Incident: (Tier 1 PSEs as per API 754) incidents which meet the threshold of severity which should be reported as the industry-wide process safety metric.

Process Safety Event—Tier 2: (Tier 2 PSEs as per API 754) incidents which didn’t meet the definition of PS incident for purposes of the industry PS incident metric. (e.g., Loss of Primary Containment Incidents or fires causing Reportable incidents that restrict work, require medical treatment or were 10% of the TO of a PSI)

Near Miss: Minor LOPCs or System failures which could have led to an incident. (e.g., instrument had failed, pipe wall thickness low)

Unsafe Behaviors or insufficient operating discipline:
measurements to ensure that safety protection layers and operating discipline are being maintained.

CCPS common Lagging indicators,

Described in this document under the "Near Miss" reporting section.

These two types of events should be collected as independent or integrated "Near Miss" company metrics.

Collect for the learning benefit, improve awareness, and enhance PS Culture.

Described in CCPS Leading Metric section.
Lagging Metrics (Tier 3)

Final Measure of Performance

• Part of ever employee’s compensation is our Performance on Process Fires
  
  Hydrocarbons + Ignition => Worst Case Scenario

• We must remove unanticipated Ignition Sources from our process hazard areas
  • Ultimately this is the focus of our Process Fire metric

• We must always maintain Process Containment
  • Ultimately this is the focus of our Loss of Containment - Flammable metric

• If either of these metrics are driven to zero, then the possibility of a catastrophic event also goes to zero
Process Fire Definition

Goes well beyond what most people think of when they think of “Fires”

• For us, a Fire is an event capable of Igniting Hydrocarbon Vapours
  • An unintended oxidation that produces flame, glowing embers, or sparks and/or evidence that this has occurred (i.e. a “Fire”)
  • Pyrophoric materials and/or other reactive chemicals
  • Sparking
  • Electrical Shorting
  • Furnace going Positive

• Industry definitions typically requires Loss of Containment/Involvement of Process Materials for something to be termed a Process Fire
  • We would elevate our classification severity for this aspect within our internal incident program (similarly for injuries or environmental damage)
Use of our Definitions to Drive our Behaviours

• Was the incident in a Process Hazard Area?
  • i.e. could hydrocarbon vapours get to this location?
  • Drive to add Safeguards to limit the extent of Process Hazard Areas (gas detection and shut-off on building air systems, fume hoods in labs, electrical enclosures…)
    • Looking for 2 barriers (normal process containment, plus 1 more)

• Were Process Materials involved?
  • Drive to limit how much material could possibly have been involved (limit inventories for things like lab work, drive to smaller inventories… lower risk)

• Were there damages and/or injuries?
  • Aligns us with CCPS/API reporting requirements
Controlled versus Uncontrolled Process Fires

No Fire is a good thing (but let me explained controlled)

• The Controlled category is to recognize the behaviours we want to see
  • The fire potential was anticipated – i.e. it was known that it could happen
  • This fire potential was documented – i.e. the risk was documented
  • Controls were in place – i.e. a plan was acted on before the fire occurred
  • The fire controls were effective – i.e. the fire was managed
  • There were no damages or injuries – i.e. the event was controlled
• The first things we look at are the permits and procedures when Classifying
  i.e. The people involved thought a fire might occur, documented this potential, put plans in place to manage this risk, these plans proved to be effective, no damage occurred, and no one was hurt
Loss of Containment - Flammable

Keep in it the pipes

- Thresholds align with CCPS and API reporting guidance
  - Corporate targets are based on flammable materials (NFPA 2 or greater) and a release quantity > 10% of the external reporting threshold (i.e. 10% of CCPS/API Tier 2 Value)
    - For a material like Ethane, the reporting threshold is 5 kg (2.5 kg for indoor locations)

- In addition to reporting F-LOC incidents, we also track LOC incidents that fail to meet the F-LOC thresholds as well as Toxic releases (T-LOC)
  - We want to encourage full reporting of all releases no matter how small (i.e. a Culture of Reporting and Learning)
  - We want to implement changes to reduce the number of F-LOC events (i.e. a Culture of Driving Continuous Improvements to prevent reoccurrence)
Critical Alarms and Operator Response

• Design Intent (Leading)
  • 5-year review program on Alarm Objectives, is this Review Program on Schedule?

• Operations Intent (Leading)
  • Number of Standing Alarms, Number of Unauthorized Suppressed Alarms

• Reliability Intent (Leading)
  • Status of testing relative to plan, Testing Results

• Incidents (Lagging)
  • Number of Critical Alarms

• Leading Metrics tend to come from the other groups (Not Process Safety owned)
Conclusions
Conclusions

Vibrant, Disciplined, Intentional, Sharing, Committed

• Need to help people see how their roles influence Process Safety performance
  • Use of a model that allows people to see how their roles plug into safeguarding our facilities
• Develop and establish standards and programs so that people can be successful
  • Need to support this with Training and Assurance systems
• A Committed Culture then becomes the element that drives the overall program
  • Reinforced by concepts related to Voice, Discipline, and Emotion
• Use of Key Metrics to further reinforce the behaviours we are looking for and to monitor progress
Questions, Comments, Suggestions

Thank You

Fred Henselwood
Process Safety Leader
Fred.Henselwood@NOVAChem.com