A Barrier Focused Approach

HOW TO GET STARTED WITH PROCESS SAFETY VOLUME 2

EDITION: #1

Release Date: June 2016 **Revised:** January 2016

SETTING THE STANDARD IN OIL AND GAS SAFETY

ENERGY SAFETY CANADA

About Energy Safety Canada

Energy Safety Canada is the oil and gas industry's advocate and leading resource for the continuous improvement of safety performance. Our mission is to help companies achieve their safety goals by providing practices, assessment, training, support, metrics and communication.

AVAILABILITY

This document as well as future revisions and additions, is available from:

Energy Safety Canada
150 - 2 Smed Lane SE, Calgary, Alberta T2C 4T5

Phone: 403 516 8000
Toll Free: 1 800 667 5557
Fax: 403 516 8166
EnergySafetyCanada.com

ACKNOWLEDGEMENT

Energy Safety Canada gratefully acknowledges the many individuals who volunteered their time and effort to complete this document.

DISCLAIMER

This document is intended to be flexible in application and provide guidance to users rather than act as a prescriptive solution. Recognizing that one solution is not appropriate for all users and situations, it presents generally accepted guidelines that apply to industry situations, as well as recommended practices that may suit a company's particular needs. While we believe that the information contained herein is reliable under the conditions and subject to the limitations set out, Energy Safety Canada does not guarantee its accuracy. The use of this document or any information contained will be at the user's sole risk, regardless of any fault or negligence of Energy Safety Canada and the participating industry associations.

Preface

PURPOSE

The purpose of the How to Get Started with Process Safety library of documents is to provide practical steps for companies in the oil and gas industry managing process safety risks (as “process safety” risks). While managing risks that are process safety risks is not new to the industry, for some companies managing these risks under the banner of process safety is new. This library is designed to help companies rapidly understand what is meant by process safety and assist them in identifying their most significant process safety risk as well as their existing management components and operational practices that fall under process safety management.

This volume, A Barrier Focused Approach, provides a step-by-step guide for a company interested in managing its most significant process safety risks or major accident hazards. It provides practical advice on how to identify these hazards and their controls and then enhance awareness, accountability and active monitoring of these critical controls.

HOW TO USE THIS GUIDELINE

The intended audience for some elements of this document is senior management or senior operational managers who carry risk management responsibilities. This would also include, but not be limited to, those specifically assigned senior roles in either process safety or, more likely, assigned health, safety, and environmental (HSE) roles. It should also be of interest to anyone assigned the task of developing and/or implementing process safety for an organization in the oil and gas industry.

The actual step-by-step guidance on developing a critical control management program within a company would be of prime value to anyone assigned a key role in the development and implementation of this type of program.

LIMITATIONS

This document does not represent an industry standard on process safety. Process safety as a discipline and process safety management practices are established in a number of well-known standards. This document and the How to Get Started library are limiting themselves to offering advice on the practical demands of process safety implementation.

Table of Contents

Introduction

There is no one right way to get started on a journey to process safety maturity. Every company must decide what strategy will be most effective for them when it comes to improving their process safety management.

The Benefits

The barrier focused approach that is outlined in this document has the potential to deliver the following benefits:

- It leverages existing, in house knowledge and experience.
- It is readily scaled – the effort required usually scales with the size of company and complexity of the operation(s).
- It goes directly to identifying and controlling the most significant hazards or risks – rather than starting with supporting elements.
- It enables effective communication of an operation's risks and controls for all involved from senior management on through front-line workers.
- It enables effective communication between companies working together on an operation or worksite. Where contracting and operating companies share safety systems, it allows both parties to speak a common language on process safety.
- It creates appropriate levels of accountability for process safety from the front line on through to senior management.
- It provides a practical platform to measure success in process safety management (before a major incident occurs).

The barrier focused approach draws on standard process safety concepts. If a company selects this approach, it should integrate with an existing, developing, or yet-to-be developed "process safety management system".

This approach has been adopted by the International Council on Mining and Metals (Health and Safety Critical Control Management: Good Practice Guide) and variations of this approach already exist within upstream oil and gas companies.

Who Can Benefit?

Any company engaged in hazardous operations may benefit from a barrier focused approach. The prime audience in mind here are companies with the following characteristics:

- Have ***experienced technical personnel*** with a deep understanding of their operations and their inherent risks
- Have an ***existing operating history*** with lessons learned along the way
- Have existing expertise in the industry standard controls for the operations they conduct
- Have ***existing management system(s)*** (e.g., QA/QC, HSE, "Operational Excellence", etc.) that are already functional and capable of being applied and referenced with respect to barriers/controls
- Have not been directly engaged in a traditional process hazard assessment (PHA) exercise (e.g., HAZOP, FMEA, FTA, ETA, LOPA, etc.)

Companies that have a longer history with traditional process safety elements and PHAs may still wish to consider the benefits of the barrier focused approach outlined here. For these companies, the qualitative approach of identifying top events and barriers (especially with a bowtie diagram) may well be familiar as a final step in a more detailed quantitative risk assessment process. These companies may still wish to consider the value of the simplified critical control documentation, accountability, and monitoring suggested in the following pages for their most important controls.

2.0 The Swiss Cheese Model

The barrier focused approach is based on an established theory of accident causation popularly known as the "Swiss Cheese Model" (and attributed to James Reason).

Major process safety incidents are nearly always the result of failures in multiple barriers – the lines of defense that exist to ensure hazardous energy and material are not released. All barriers have inherent weaknesses. If all barriers fail simultaneously, a disaster results. To see this in more concrete terms using a well-known process safety disaster, see Appendix 1 which offers BP's own "Swiss Cheese" diagram of the Macondo accident.

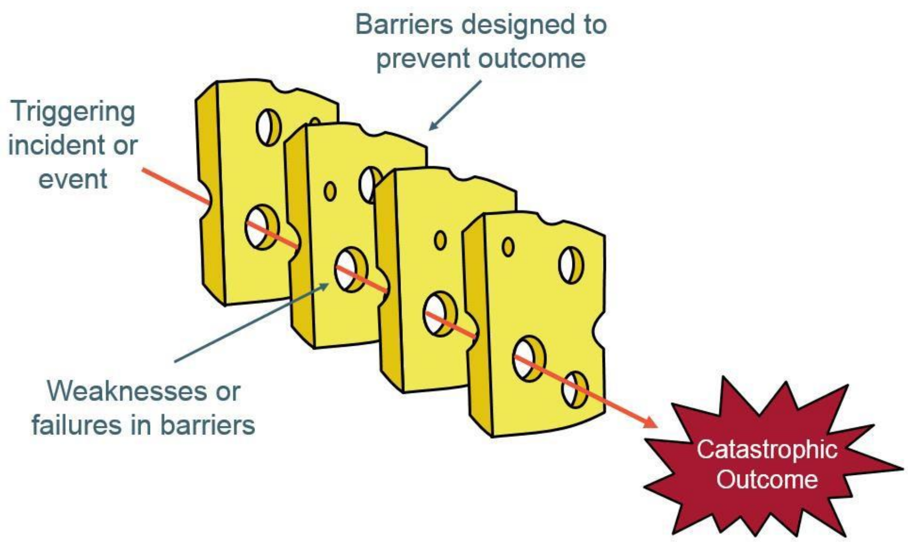


Figure 1: The Swiss Cheese Model

The barrier focused approach outlined in these pages puts the focus squarely on the barriers (the "cheese slices") and seeks to prevent major process safety incidents by:

- Clearly identifying the required barriers
- Effective implementation of the barriers
- Active measuring and monitoring the success of the barriers

Essentially this is reverse engineering the "Swiss Cheese accident" to prevent the major incident from ever occurring.

"Barriers" = "Controls"

In the remaining explanation, the term "control" will be used for "barrier". This better aligns with existing safety and risk language that speaks of "hazard controls" or "risk controls". In some contexts, barrier language might be more appropriate. In others, control language will resonate. For our purposes, they mean the same thing – the systems, people, or equipment counted on during a hazardous operation prevent an unwanted incident.

3.0 Preparation

Adequate preparation is key to getting the most out of implementing the barrier focused (or critical control) approach.

Some Questions to Ask (and Answer) at this Stage

Before making a final decision on pursuing this barrier focused approach, consider the following questions:

- What is the intended scope?
- For example, is this a pilot project on a single type of operation or project? Or are you systematically tackling all facets of your operations with major incident / process safety risks? Your top three (four, five, etc.) major incident risks?
- What are the objectives or specific deliverables?
- Are there existing projects at a corporate, business unit, project, or site level that will complement or serve as a hindrance?
- Who will be critical to the success of this undertaking?
- What business unit, existing departments or functional units need to be included for this to really work? (closely related to previous question but not always identical)

Perhaps the most critical—

- Do you have sufficient senior management support for this to be successfully implemented and sustained?

Additional Questions to Answer (at least Provisionally) in your Plan

Anyone setting out to facilitate implementation of this barrier focused approach should also have answers (or a plan to arrive at provisional answers) for the following questions. These may well be adjusted as a result of the process itself.

- How will you determine your major hazards or incident risks?
- What method will you use to identify the possible threats, consequences, and controls for the major hazards?
- Who is best suited to provide and validate these?
- What will be your criteria for a critical control?
- What do you want captured in your critical control documentation?
- What are the essentials of your verification process?
- Who needs to validate the control documentation?
- How will accountabilities be assigned?
- How will accountabilities and responsibilities for elements of critical controls be communicated?
- In what context(s) will critical control performance be assessed and addressed to drive continuous improvement?

Who to Include?

As a general rule, hazard management only succeeds if you involve both decision making and affected personnel in the process of hazard identification, assessment and control. In the barrier focused approach outlined here, participants need to be familiar with known major hazards, critical controls, and the essential elements of those controls. As such you should include a sampling of the following in your working group(s):

- Engineering support personnel
- Project/program managers
- Line managers/superintendents
- Experienced front-line supervisors
- Experienced front-line workers
- Less experienced supervisors and workers (fresh eyes and perspective)

Remember, a key premise here is that both the major hazards or risks and the critical controls are known to experienced personnel. The process will only work if these individuals are central to the process. Their knowledge and buy in is essential.

4.0 Identify the Major Hazards/High Consequence Events

The first step is to identify the major hazards or potential high consequence events that will be subject to this process.

For complex facilities and operations, these typically emerge as part of an extended, technical process hazard assessment process.

However, for many operations in the oil and gas industry, there are only a small, well known set of possibilities that apply to a particular type of operation. The history of major incidents suggests that when things go catastrophically wrong, experienced and knowledgeable personnel were typically aware that the incident was possible. For experienced manager and supervisors, these are the potential catastrophic outcomes that “keep them up at night”. To maximize the value of this approach, you want to capture the events with the most serious consequences.

If you involve the right mix of operational expertise (see “Preparation”), any one of the following (or combination of the following) approaches may be used to create a list of major hazards or high consequence events as your starting point.

The assembled participants brainstorm suggestions or have a facilitated group discussion followed by consensus-based decision making (especially in less complex, more straightforward operations)

- The assembled participants brainstorm suggestions but ultimately work with a metric that determines what counts as a “major hazard” (e.g., serious injury, fatality, x fatalities, x volume spill, x level of cost, etc.)
- A formalized risk assessment process using established, relatively technical process hazard assessment (PHA) methodologies is carried out. This process then produces a list of residual risks that demand further attention based on the potential for a high consequence outcome.

Appendix 2 offers a list of examples of major hazards or high consequence events by operation type in the oil and gas industry. These are ***suggestive*** to get your process started and ***not exhaustive***.

Challenging and Overcoming “That Could Never Happen”

One of the challenges in this exercise is arriving at the (usually) low probability, high consequence events that should be addressed. There are two challenges in this identification exercise:

- Dismissing a possible major incident risk too quickly because “that could never happen”.
- Chasing incredibly remote major incident risks and wasting valuable resources that could be applied to more pressing and plausible risks.

So, for example, if a company involved in fracture stimulation operations were to spend time concerned about helicopters or planes crashing on their pumping operations—that would likely be a waste of time and resources. Especially if that time could be spent on a more plausible (albeit low probability) event such as the potential of high-pressure fracture fluid migrating to an adjacent well with destructive consequences.

In a session where major hazards or possible high consequence events are identified, it is important that the facilitator challenges group members that dismiss suggestions (their own or someone else’s) on the basis that the event “could never happen.”

Probing why it could never happen is essential. If the answer is based on the containment of control equipment or worker procedures or competency, the answer is it could happen (even if these workers have never personally experienced it). Process safety events are stories of equipment, people, and processes that should have prevented the incident but did not for one reason or another. On the other hand, if the suggestion comes from a poor understanding of the materials or processed involved and this is validated, it may not be worth considering.

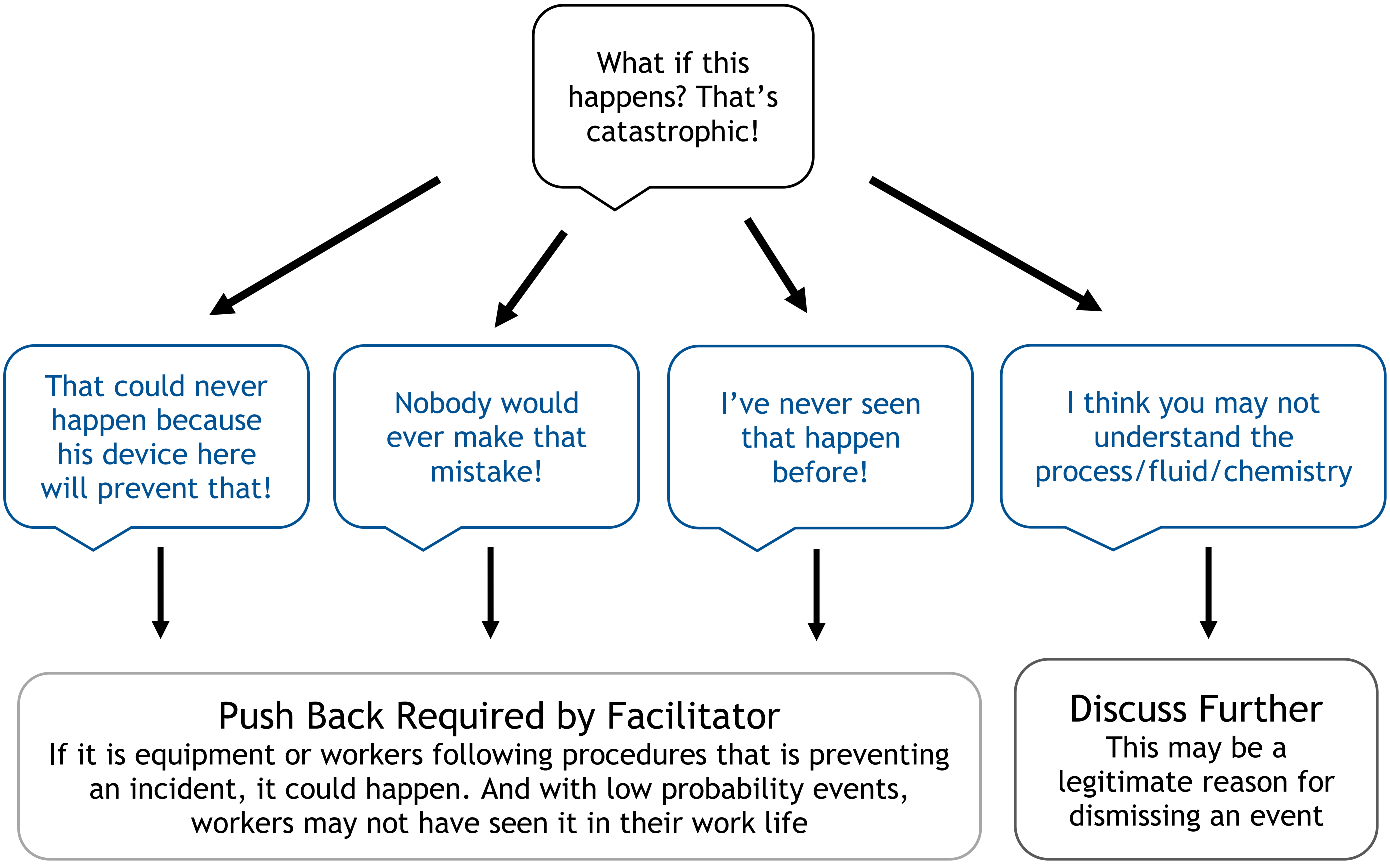


Figure 2: Facilitating identification or major hazards

5.0 Identify Controls

Once the major hazards or top high consequence event or events have been identified, the next step is to identify the controls that can prevent and mitigate these events. These will typically be existing controls although in some cases additional controls will be brought forward for consideration. To fully address and assess controls, there needs to be a shared understanding of the threats that might trigger the top identified event(s) and the possible consequences that will flow from that event.

One effective way to capture these visually is with a bowtie diagram. A bowtie:

- Provides an easy-to-understand visual layout – all threats and consequences and the controls for a given major hazard or top event can be seen at a glance
- Sort controls into preventive and mitigating barriers (an important distinction that is sometimes missed)
- Creates clarity when discussing the adequacy of controls
- Serves as a communication tool when creating awareness or training personnel on controls

A step-by-step guide to facilitating and developing bowtie diagrams for the purposes of identifying controls is provided in Appendix 3, 4 and 5.

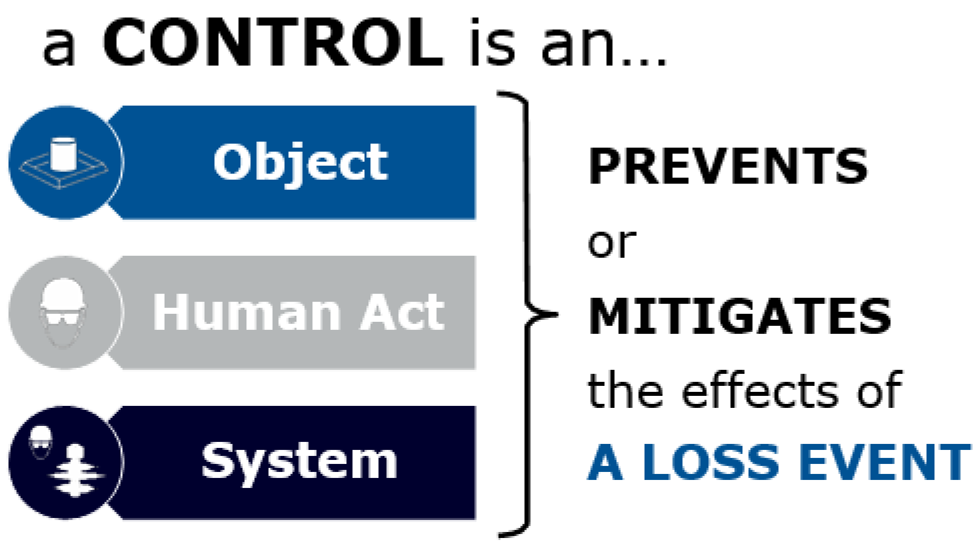


Figure 3: Defining a control

What Counts as a "Control"?

All companies have a variety of existing strategies to prevent major incidents of the sort identified as "top events". A company that meets regulatory requirements, follows industry standard practices, and has undergone some form of risk or hazard assessment process will have controls in place for these events.

For the purposes of this barrier focused approach, a “control” is:

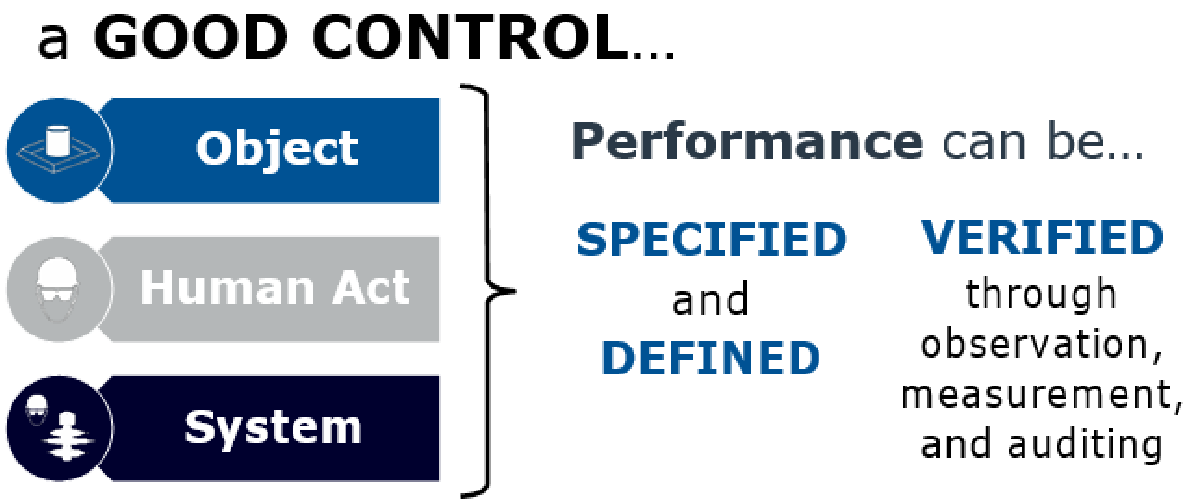
- An object (i.e., engineered device), human act, or system (combination of human act and object) that prevents or mitigates the effect of a loss event.

It is important in this approach to distinguish between elements that support controls and the controls themselves. So, for instance, if a control is that a worker must recognize an alarm and turn off a piece of equipment, then training, supervision or a procedure document may provide vital support to that human act or system. But these are not the control itself in the strictest sense. A management plan may identify hazards and controls, but in itself does not serve as a control. A program to stop and do a risk assessment is good practice and may lead to better application of required controls, but it is not a control itself. These control “supports” will be captured—but in a later step.

Evaluating Controls

With the barrier focused approach outlined here, a “good control” will have the following characteristics:

- Its performance can be specified and defined



- Its performance can be verified through observation, measurement, and auditing

Figure 4: Defining a good control

Once controls are identified, some form of assessment of the overall control strategy is in order. At this point, the following types of questions should be raised and answered (at least provisionally):

- Are the controls identified appropriate and relevant for each initiating threat?
- Are the controls sufficient?

One way to “weigh” controls (instead of simply counting them) is to sort them out based on the hierarchy of controls (see Appendix 7). Engineering controls (which is where “objects” fit) are typically more reliable than controls that fit the “human act” or “system” type controls. The latter usually depend on a worker following procedures, training, and/or competency and ability to recognize the situation for what it is. This introduces a human factor that makes them less reliable.

If a bowtie is used to illustrate controls, colour coding controls may provide an at-a-glance visual to distinguish between stronger and weaker controls.

6.0 Identify the Critical Controls

In this step, all the controls are evaluated or tested to determine if they merit extra attention as “critical controls”.

In general terms, ***a control that is crucial to preventing or mitigating a high consequence event is critical***.

Companies will need to decide their criteria designating a control as critical, but the following tests should be considered (at minimum):

- If the control was missing or failed, does the risk of an event and/or its consequences go up immediately (even with other controls in place)?
- Is the control effective for multiple threats or does it mitigate multiple consequences?
- Is this the only control for a particular threat or consequence?
- Is there any history of this control failing and this leading to a near miss or actual significant loss, either within the company or within the industry?

A “yes” to any of these would suggest the control is critical.

Given the extra attention, effort, and resources that will be assigned to critical controls, ***being selective at this point is essential***. Bear in mind the following:

- Managing the critical controls is about preventing high consequence events (and especially those with low probability/frequency) – this is not about preventing all incidents.
- Controls that fall outside of the “critical” category will not disappear.

Remember, the list of “critical controls” is subject to change in the future as:

- The program cycles through a continuous improvement loop
- Control strategies change in response to incidents or technology changes
- The program becomes more efficient.

The key—start with a manageable list to maximize early success.

7.0 Document the Essentials for Critical Controls

Having identified critical controls, the next stage is to summarize key essentials for each critical control. Within formal process safety management systems, these will sometimes be referred to as "performance standards" (and completed with varying degrees of detail and complexity).

Documentation for each critical control should ideally include the elements outlined in the table below. Where possible, use the same personnel as were involved in the identification of controls (i.e., bowtie building exercise) to create or validate these documents. Creating a first draft of these documents immediately following or as part of a bowtie building exercise with those most familiar with the control strategy helps prevent confusion or misinterpretation of controls at a later date. The key to these documents being effective is to:

- Keep the language as simple, clear and free of technical jargon as possible.
- Fit the essential information on a given critical control on a single page (whenever possible).
- Test the documents with non-specialists. Can they make sense of them?

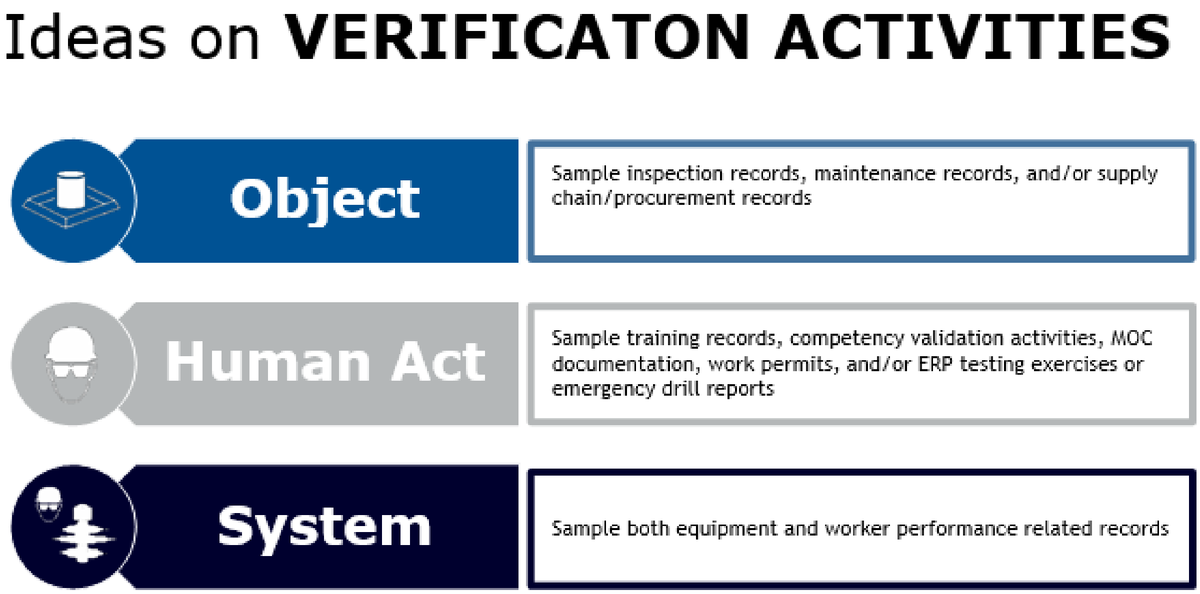
Appendix 6 provides an example of simplified critical control documentation based on the table below.

ELEMENT	QUESTION(S) TO ASK / ANSWER
Objective(s)	In the simplest terms, what exactly is the control expected to do in order to prevent or mitigate an event?
Performance Requirements	In slightly more technical terms, what must the control do in order to meet the stated objective?
Supporting Activities / Dependencies	Are their systems or processes within the company that support or ensure the control delivers on its objective? (e.g., work procedures, training, inspection, maintenance, reporting, etc.)
Verification Activities	What needs to be sampled and reviewed to establish the control is or can meet its performance requirements? How often?
Triggers for Investigation / Shut Down	In terms of the verification activities – what thresholds would trigger either a further investigation into the critical control or operational shutdown?
Accountabilities	(See next section)

Verification Activities

This element is critical to maximizing the value of a barrier focused approach. It requires careful consideration.

Ideally, the verification activities should be based on the existing support activities for a critical control's performance. Building on existing support activities may reveal not just the state of the control's performance, but the health of the support activities themselves. The graphic below provides some starter suggestions for the type of verification activities applicable to each type of control.



8.0 Assign Accountability for Critical Controls

General Accountability

Successful, long term management of major hazards and their corresponding controls requires every level of the workforce or operation to fulfil their role in the process.

LEVEL	OVERALL RULE IN MANAGING OR MONITORING CRITICAL CONTROLS
Senior Managers	• Ensure line managers have systems for checking critical controls • Carry out spot checks for themselves • Provide "felt leadership"
Line Managers	• Ask supervisors how they know front line workers are implementing critical controls • Carry out spot checks themselves • Provide leadership
Front Line Supervisors	• Talk to front line workers under their supervision and ask specific questions about critical controls and their roles with those controls • Ensure task related to critical controls or support of critical controls are a top priority in managing work and workload • Perform regular checks on critical control equipment and active workers to observe implementation firsthand
Front Line Workers	• Implement the critical controls • Participate in cross-checks to ensure critical controls are implemented and are/will be engaged when required

Specific Accountabilities

At this point in the process, there should be documentation that captures the following:

- Major hazard(s) / high consequence event(s)
- Critical controls and their function for these events
- Supporting activities / dependencies for these controls
- Verification activities

Specific accountabilities for each of these items may be captured in the preceding step— especially in those organizations where existing job descriptions naturally align with particular roles in implementing and monitoring critical controls. However, in other organizations this will be new and requires additional deliberation and buy-in from all affected stakeholders.

To effectively monitor controls over time, ownership (by title and, if possible, by name) needs to be assigned to elements captured within the critical control documentation. At minimum consider an owner for:

- Each major hazard / high consequence event
- Each critical control
- Each verification activity (or group of activities)

This ownership structure for high consequence events, their critical controls, and control verification has the best chance of success if it is:

- Documented in a simple, straightforward manner with expectations on activities and decision-making clearly laid out
- Specifically captured in the job descriptions of the assigned owners
- Integrated into performance evaluations

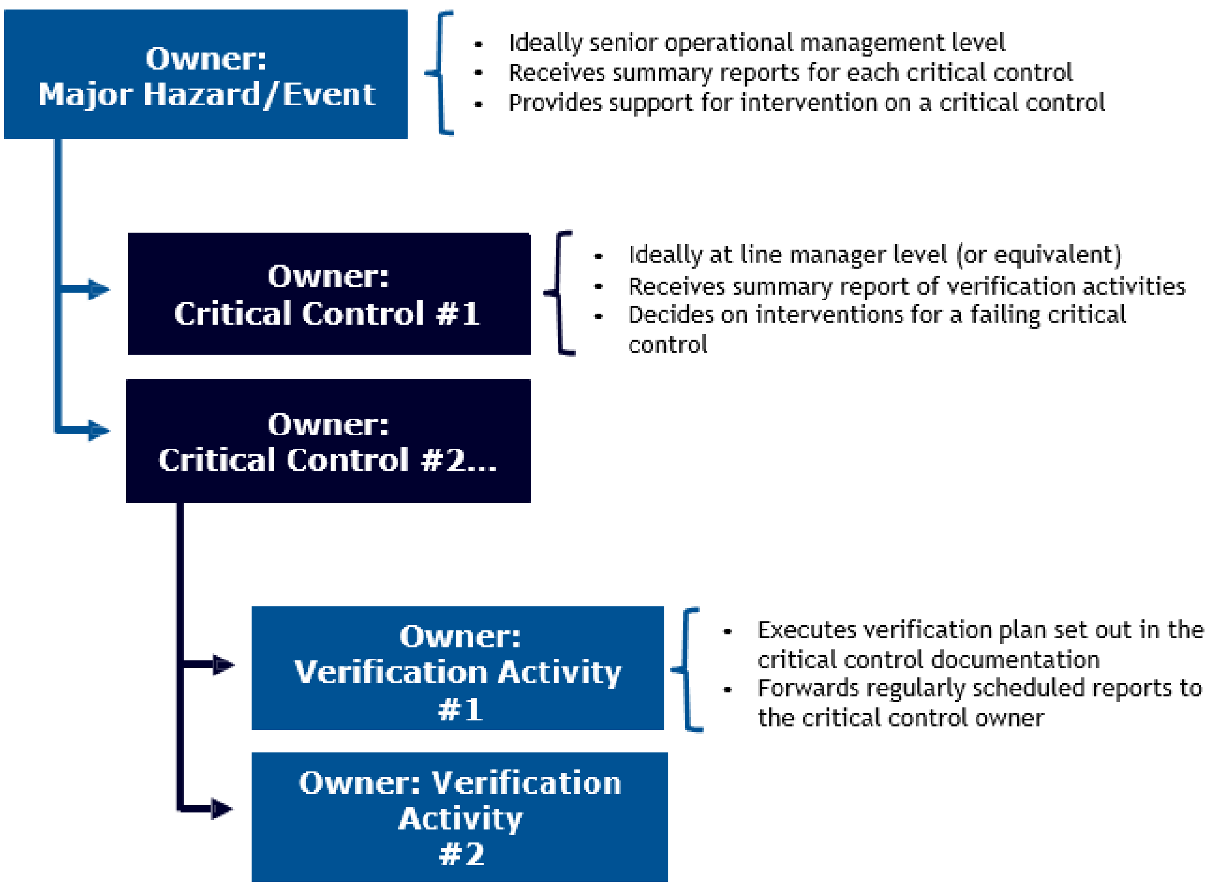


Figure 5: Assigning accountability

9.0 Implement and Monitor the Critical Controls

The process of reviewing high consequence events and their controls will, in some cases, lead to a realization that a company needs to:

- Simplify existing controls and/or their supporting systems
- Enhance existing controls and/or their supporting systems
- Implementing new controls and support systems
- Adjust critical controls and how they are managed for site specific or project specific reasons

Basic principles of project management apply to these efforts. These efforts require:

- A project owner with sufficient seniority to ensure completion in a timely fashion
- A clear project scope with defined deliverables
- Milestones with dates and a final deadline for implementation
- Sufficient engagement and communication with stakeholders (including front line supervisors and workers whenever possible) and especially those with extensive operational experience

Communication Efforts

In the process outlined, the emphasis in each step is on keeping the documentation as clear, straightforward, jargon-free, and as simple as possible. This pays off in the implementation and monitoring phase. A readable and user-friendly document may be repurposed in communication and training efforts that raise awareness of major hazards and their corresponding critical controls.

- Bowties
  - Provide an overview of controls and the path from threat to consequence.
  - Can be used with a variety of audiences including front line workers to better understand the "why" of critical controls and reinforce required procedures and behaviours.
- Critical Control Documentation
  - Provides an overview of the specifics of critical controls.
  - Allows anyone assigned a specific role in the critical control document or support systems to see how their task fits a larger goal and why it is important.
- Accountability Documentation
  - Provides an overview of specific responsibilities with respect to critical control monitoring.
  - Allows anyone assigned a specific role in critical control monitoring to see what is expected of them at a glance and how their role relates to others in the monitoring process.

Document Control

Document control is also critical. Whenever critical controls have been adjusted to meet site specific, project specific or unique operational circumstances, it is key to capture these changes in the related documents (e.g., bowties, critical control documentation / performance standards, accountabilities, etc.) and circulate these with all relevant stakeholders.

Monitoring Efforts

Simple, readable documents also help demystify the monitoring efforts for everyone involved.

The verification plan and accountability structures created earlier in the process now need to be executed.

Monitoring can also be worked into other existing management activities:

- Senior management visits
  - Critical control documents provide a way to enhance senior management worksite visits as operational and/or safety personnel can rapidly brief senior management on the types of questions to ask and things to look for in their worksite visit. This adds considerable value to senior management visits for all parties involved, putting emphasis on “critical safety issues” often bypassed in these visits (which otherwise tend to be heavy on personal safety).
- Incident reporting
  - Incident reporting and investigation systems may become more effective with assigned owners for major hazards and critical controls. Near misses or failures related to either of these now have an established owner that carries responsibilities to ensure an adequate investigation and apply lessons learned.

    Note that this presumes that incident investigation methods will identify and highlight failures in critical controls. An organization should ensure their incident reporting and investigation methodology is applicable to critical controls—and ideally prompts the investigator to consider critical controls.
- Reporting on safety for senior executives
  - Injury-based rates have been the staple of many company’s “safety metrics” for reporting purposes. Verification and other monitoring activities related to critical controls allow for organizations to measure performance that is far more indicative of risk exposure to high consequence events.

For further information on developing process safety metrics, begin by consulting an industry standard such as:

- Process safety – recommended practice on key performance indicators, OGP Report No. 456 (November 2011)

10.0 Respond to Inadequate Performance

If critical controls are systematically identified and monitored, inadequate performance should now be identified through:

- Reports from verification activities that highlight performance that is below the established threshold.
- Incident reports (both near misses and events) and investigations that identify critical controls not performing as required or show critical control were (or may have been) inadequate.

Either of these should trigger a further investigation into the performance of a given critical control. Assigned owners for major hazards and the critical control in question should provide leadership and accountability to ensure these are thorough.

A Two-Tier Investigation

Failures need to be analysed on two levels.

First, the critical control failure itself needs to be probed, using questions like:

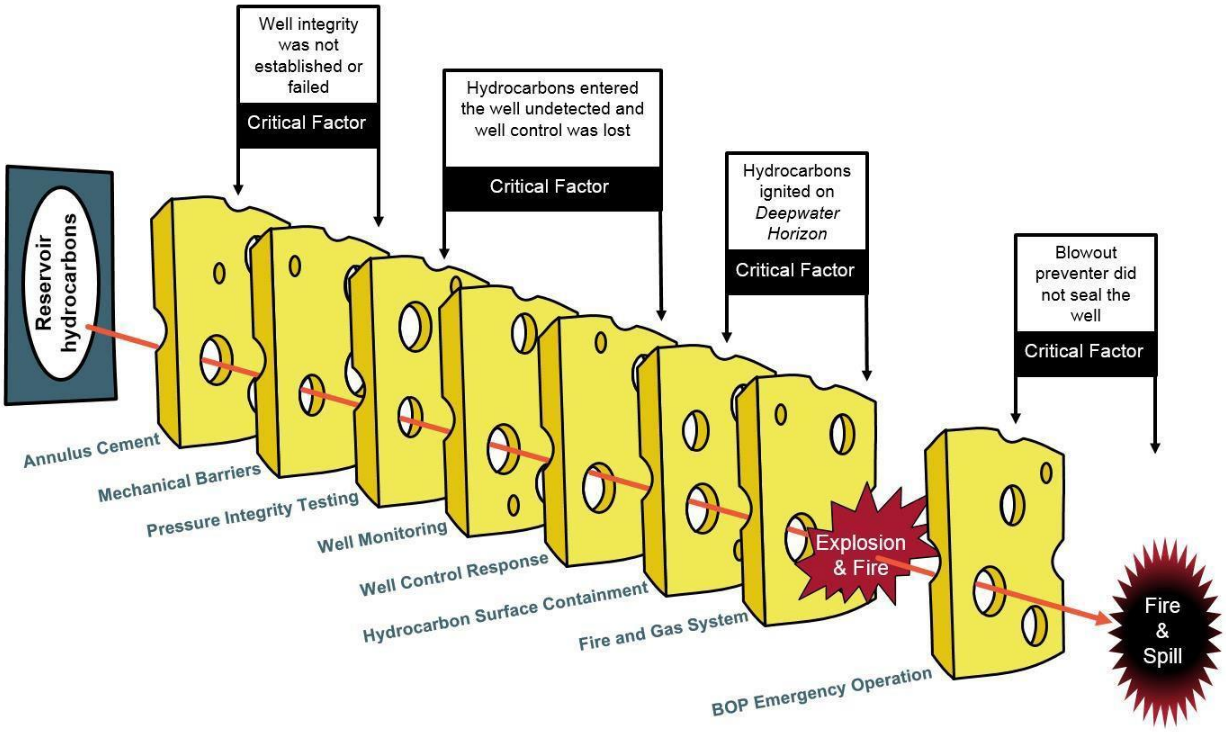
- How precisely did the critical control fail or perform below standard?
- What were the immediate and root causes for this performance failure?

Based on the answers here, a second level of questions needs to be asked to probe the overall control strategy and effectiveness of the existing control strategy, documentation, implementation, and monitoring. For example:

- Was the critical control (even if functioning correctly) sufficient for the event that transpired or nearly transpired?
- Does the incident suggest a critical control needs to be redesigned or an additional critical control added?
- Does the list of potential threats or consequences need to be redrafted in light of the event or learnings from the event?
- Was the description of the critical control and its expected performance sufficient in light of the event?
- Did/do major hazard and critical control owners understand the required function and operation of the critical controls under their responsibility?
- Are different owners required and/or is additional training required for owners?
- Are there failures in support systems that need to be addressed?
- Are the existing verification activities sufficient to detect potential control failure or do they need to be adjusted and/or changed outright?

The investigation should provide concrete recommendations arising from any failure.

Appendix 1: The BP Swiss Cheese Model of the Macondo Incident*



*adapted from Andrew Hopkins, Disastrous Decision: The Human and Organizational Causes of the Gulf of Mexico Blowout (Sydney: CCH Australia, 2012), 7.

Figure 6: The BP Swiss Cheese Model for the Macondo Blowout

Appendix 2: Examples of Major Hazards/High Consequence Events

EXAMPLES OF MAJOR HAZARDS / HIGH CONSEQUENCE EVENTS IN OIL AND GAS OPERATIONS (*FOR ILLUSTRATION PURPOSES ONLY*)	
Drilling	• Loss of well control • Derrick collapse • Ignition of hydrocarbon based drilling fluid
Completions	• Loss of containment of production fluids • Loss of containment / ignition of flammable completion fluids • Introduction of oxygen into closed systems
Oilfield Trucking	• Loss of containment / ignition during loading and unloading flammable or toxic fluids (e.g., H_2S) • Loss of containment / ignition during transport
Storage	• Loss of containment of stored flammable or toxic fluids • Introduction of oxygen into closed systems • Potential fire, explosion, or toxic exposure during maintenance or other operations with “empty” storage tanks
Pipeline	• Loss of containment of gas or liquids in the pipe
Production Facilities	• Loss of containment of gas or liquids, especially gas in enclosed spaces ○ Various PSEs such as flange leaks, vessel ruptures, valve failures, PSV release, etc., could be captured either as major hazards and treated as such or captured as threats initiating a greater high consequence event (based on the overall control strategy)

Appendix 3: A Step-by-Step Guide to Facilitating a Bowtie Building Session

A Bowtie at its Most Basic

A bowtie is a simple diagram used to capture and illustrate threats, controls, and consequences of a major accident or loss event. At its most basic, it has the structure you see below.

There can be multiple threats and typically multiple preventive controls between an initiating threat and the loss event and multiple mitigative controls between a loss event and a given consequence.

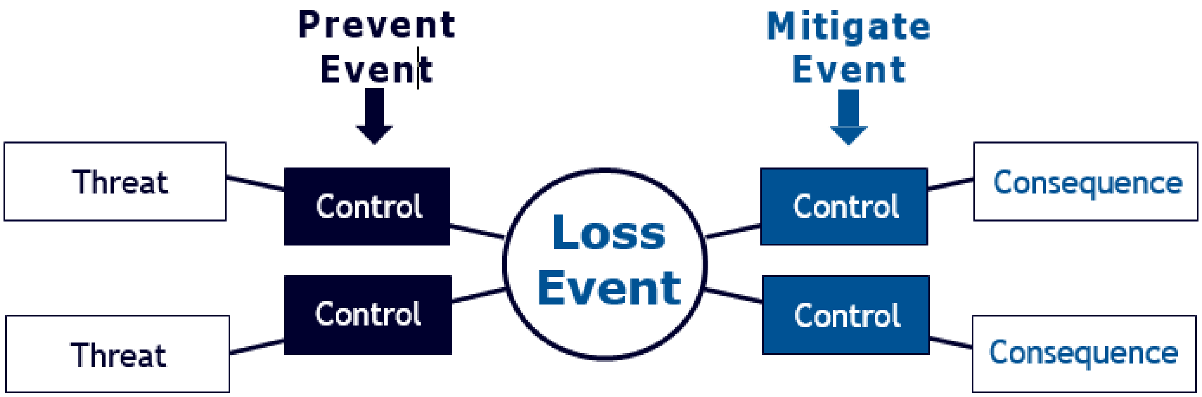


Figure 7: The Basic Bowtie

Teaching the Basics Quickly

If a group of operational experts and personnel working with bow tie illustrations for the first time, one quick technique to teach the basic concept is to have participants build a bow tie for a vehicle accident. A pencil and paper (or whiteboard) are all that is needed. Ensuring a basic understanding of the two sides of the bowtie and controls is key at this stage. Precise "rules" that have been generated for more technical bowtie development can be put aside here to keep things simple and moving.

Have participants start with the loss event in the middle and threats and consequence on left and right. Individuals and groups will vary in what they put down.

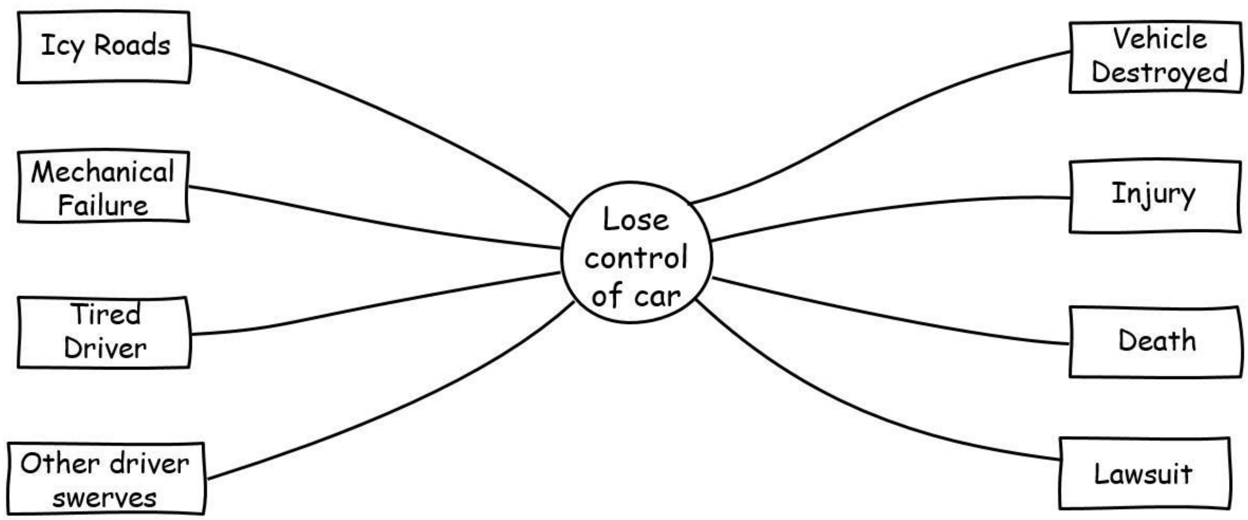


Figure 8: Learning the Bowtie Basics, Part 1

The next step is to add the controls that will prevent or mitigate this event. Expect even more variety here.

Ensuring the basic concept is clear is more important here than applying best practice in bowtie building. This example (based on actual workshop outcomes) is typical in “breaking the rules” at various points (see further Appendix 5: Some Advanced Tips for Bowtie Development).

What matters is at this point participants have sufficient knowledge to begin developing bowties for the top events / major accident hazards.

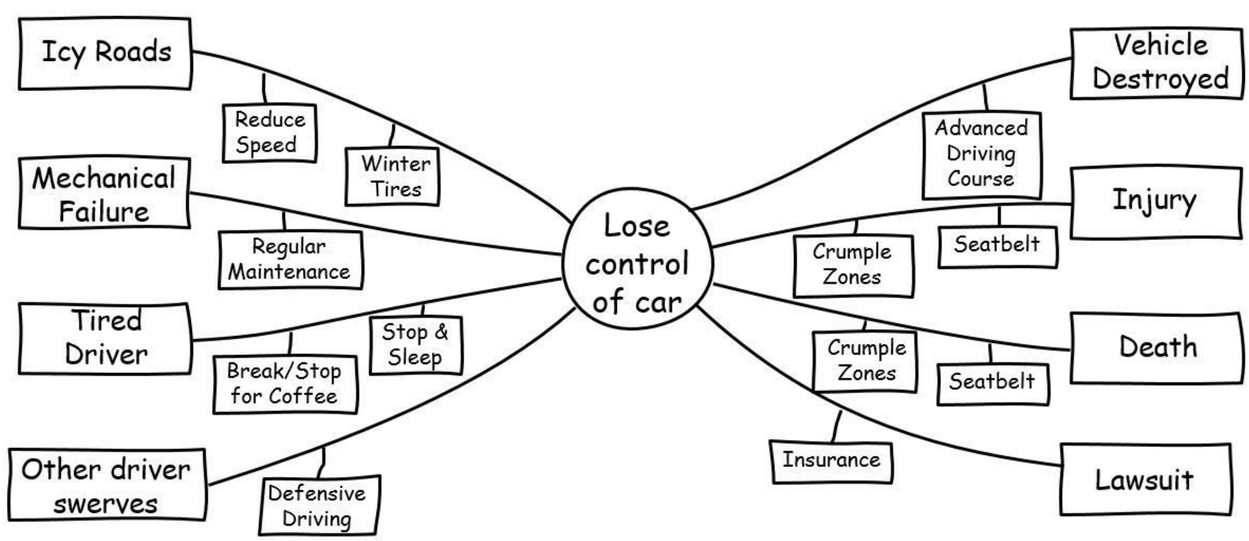


Figure 9: Learning the Bowtie Basics, Part 2

Build a Bowtie for a Major Hazard / High Consequence Event

Once the bowtie concept is understood, facilitators can move immediately to developing bowties for major hazard event. Typically, bowties start with a decision on the top event, then listing threats, consequences, and finally controls. In reality, the process is more iterative and there needs to be some flexibility in the course of building a bowtie with a group of subject matter experts.

Consider your initial bowtie development a brainstorming session. You can refine and adjust the controls or other elements of the bowtie after you have captured your initial ideas. Appendix 6 offers examples of multiple iterations of bowties built in industry workshops.

These four elements are consistent and common to all bowties. Depending on the approach or software support chosen, another three elements may also appear in a bowtie diagram. See Appendix 4 for an additional visual guide for elements such as “hazard”, “escalation factor”, and “escalation factor control”. Facilitators and ultimately organizations will need to make a judgment call on the addition value these provide versus the complexity they introduce.

Online Video Resource

There are also excellent online resources offering an overview and tips for creating effective bowtie diagrams. Here is one from BakerHughes, a company that has applied this method to their upstream operations.

- BowTie Risk Assessment Method (Baker Hughes)

Tips for Identifying Top Events

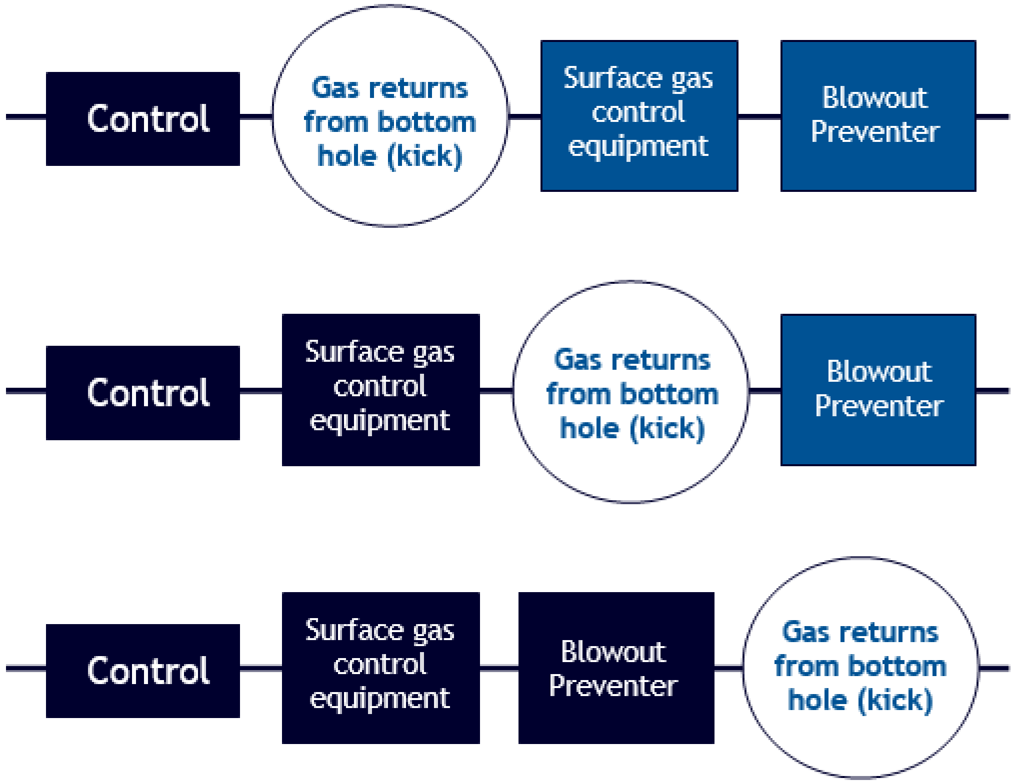
Once major hazards or high consequence events have been identified, distilling what is the “top event” in the bowtie analysis needs to happen. Sometimes these will be expressed in terms that work as your middle “top event”, but often they are expressed as “serious consequences”. For instance, burning down or blowing up a facility may be a possible high consequence event. But the “top event” in the bowtie would likely revolve around an uncontrolled release of hydrocarbons.

The rule of thumb for what goes in the centre of the bowtie is that it should:

- Address the “major hazards” or “high consequence events” that are of greatest outstanding concern to the company or operational group
- Have multiple initiating threats
- Have multiple consequences (i.e., it must be the event before major damage has occurred and while there is still a possibility for recovery or mitigation)

Some experimenting may need to happen, and you may need to shift your “top event” to the left or right in the overall accident chain.

For example, suppose a company involved in a drilling operation is addressing loss of well control while drilling. Is the top event loss of sufficient bottom hole pressure, gas returns at the surface, or uncontrolled gas returns and release at the surface? Notice this decision will then affect whether the gas separator and other gas control equipment at surface or the blowout preventer (which shuts in the well at surface) or are on the left (as preventive controls) or the right (as mitigative controls). While strong opinions may exist one way or the other, in terms of the approach outlined here, there is no absolute right or wrong answer. Be willing to adjust as you go if the bowtie becomes complex or unworkable.



Tips for Identifying Threats

To maximize success with the bowtie, threats should describe specific events that:

- Can lead to the top event independently (if intervening controls fail)
- Are plausible
- Are not simply a failed control

Distinguishing triggering threats from control failure is very important as the end goal here is to focus on critical controls. Revisit any threat statement that is simply a failed control and look for a preceding initiating threat. This allows the control to appear on the bowtie as a control—and likely a critical control.

Tips for Identifying Consequences

When crafting the bowtie, consequences listed should describe specific events that:

- Can lead directly from the top event (if intervening controls fail)
- Are expressed in operational terms that are easily understood

It is useful to keep the bowtie as simple as possible. If there are multiple consequences that all have identical controls, consolidate them on a single line in subsequent drafts.

Tips for Identifying Controls

Controls are objects (typically engineered devices), human acts, or systems (a combination of human act and object) that prevent or mitigate the effects of the top event.

- Controls need to clearly prevent escalation to the top event or mitigate a particular consequence.

Controls should be stated in a way that it is clear how that control is preventing the top event or mitigating a particular consequence. So, for example, a “training program” or “management system” will not prevent or mitigate anything. A worker who knows precisely what to do in a given situation and does it—that “human act” is the control. A training program that attempts to ensure a worker knows what to do will be captured in documentation related to that control. And this training may be included in monitoring strategy for this control. But it is useful to distinguish the two at this stage.

A key here is that listing every possible control (major or minor) may lead to a bowtie so complex that it loses its value. Bowties are most helpful when they can show at a glance the major direct controls that prevent particular initiating threats from escalating into catastrophes.

- Controls should be sequential and independent whenever possible.

Ideally, controls should be independent— and if “counting controls” is adopted by a company, this becomes critically important. For example, if a two-barrier policy is mandated, they must be two truly independent barriers. However, for the purposes of trying to capture critical controls, being overly strict may be self-defeating. To cite an example from the Civil Aviation Authority guidance, fire detection and firefighting may be put on a bowtie as two separate controls even though fire detection is not actually a control without a firefighting response and firefighting can only begin after fire detection. However, if each has its own issues and potential weaknesses that need to be addressed, treating them as independent for the sake of simplicity in managing critical controls may be more valuable than adherence to a particular bowtie methodology.

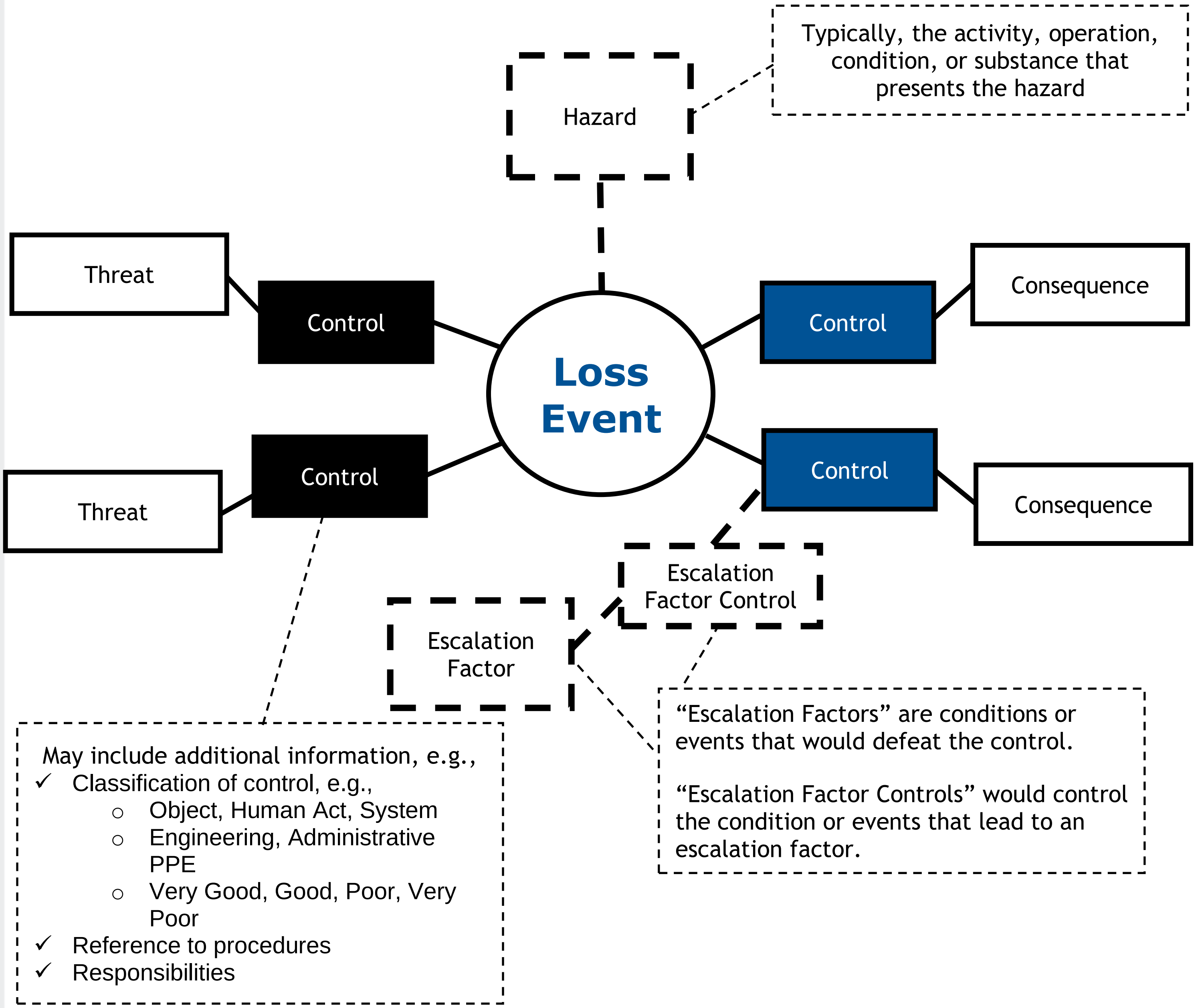
Ideally, controls should also be sequenced if they are applied in that fashion (e.g., if control x doesn’t work, control y is engaged). This isn’t always possible as some are simultaneous or in some circumstances only one of a number of possible controls may be engaged. At this stage capturing the necessary controls is more important than making the bowtie illustration more complex. Like any tool, it has its limitations.

Appendix 4: Additional Bowtie Elements

It is relatively common to find bowties that include three elements in addition to the four common elements of loss event, threat, consequences, and controls. Commercial software products in particular will frequently offer some of the options illustrated here.

For a quick overview on these additional elements, see:

- Bowtie Risk Assessment Method (Baker Hughes)



Appendix 5: Some Advanced Tips for Bowtie Development

When facilitating a bowtie building session, capturing the necessary information without fussing over absolute proper bowtie building technique is essential. However, if bowties are used on an ongoing basis as communication or reference tools, the following tips may be applied when moving from rough drafts to final products.

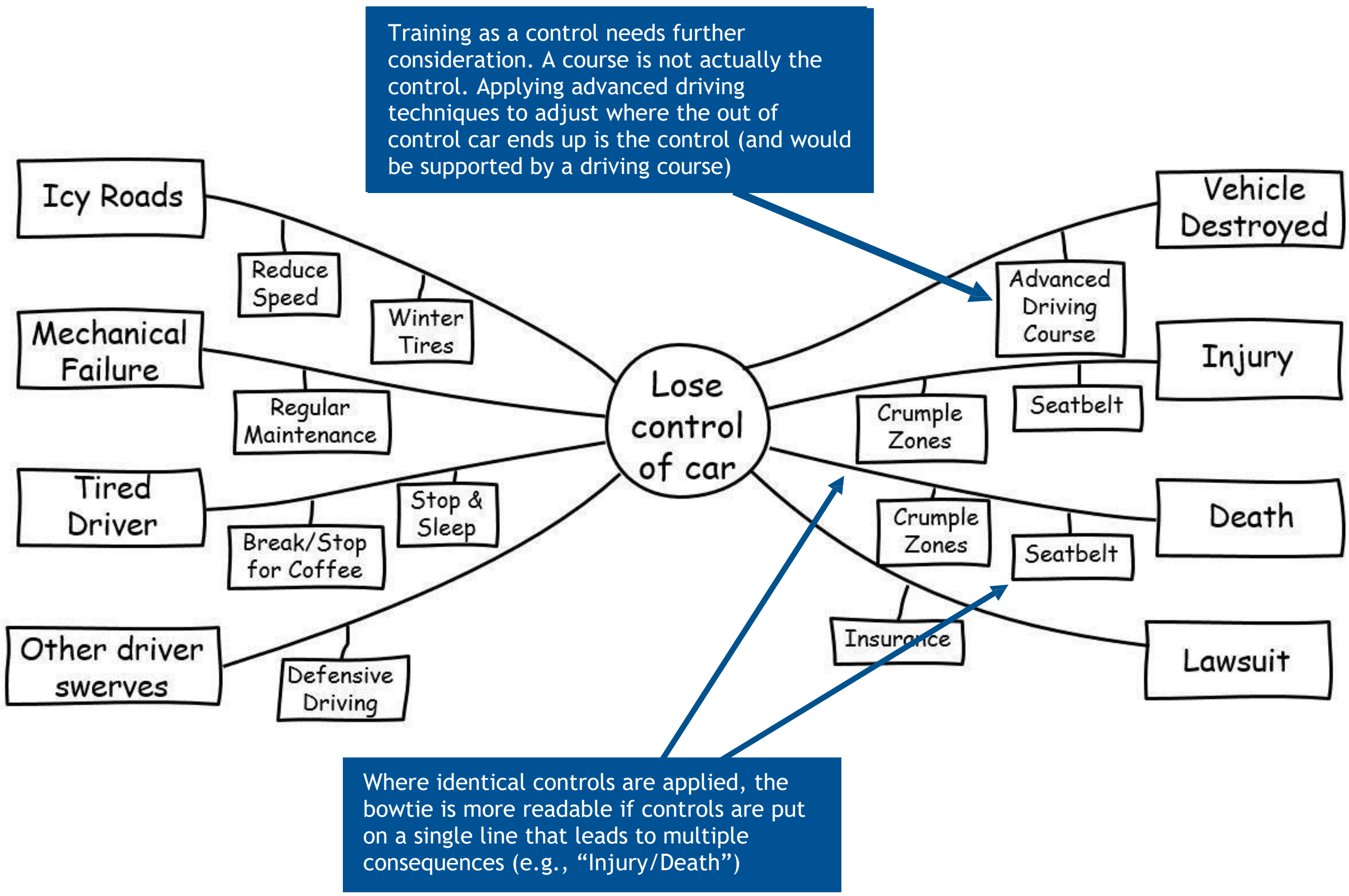


Figure 12: Advanced tips for bowtie development

Appendix 6: Sample Bowties from Industry Workshops

In the following pages, various iterations of bowties from actual bowtie building workshops are provided by way of illustration.

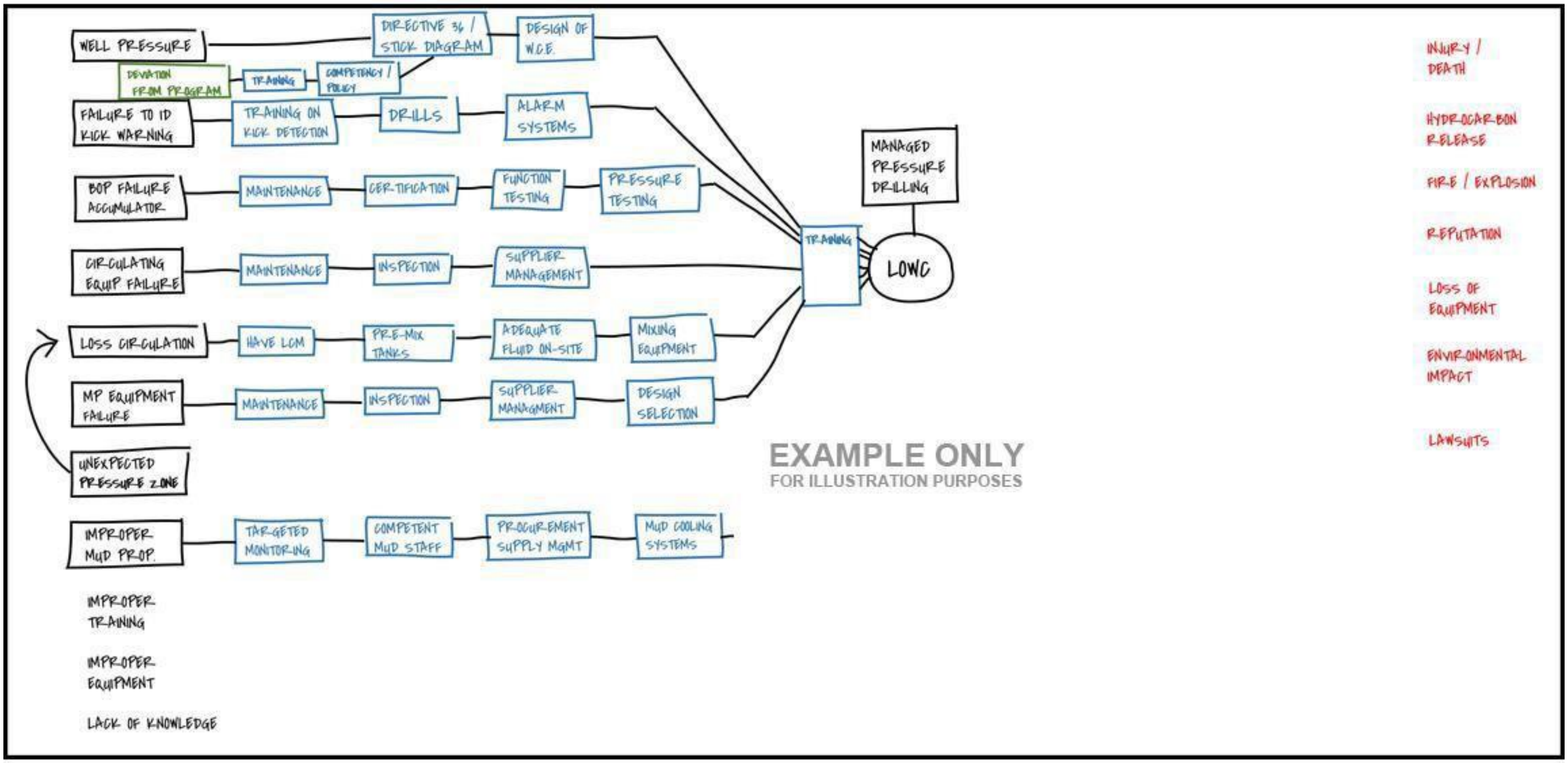
Please note these are for illustration purposes only and are not intended to be applied as is to actual industry operations.

Tablet size versions (17x22 inch) of this appendix are available online.

Middle of First Round of Bowtie Building for "Loss of Well Control" for Managed Pressure Drilling

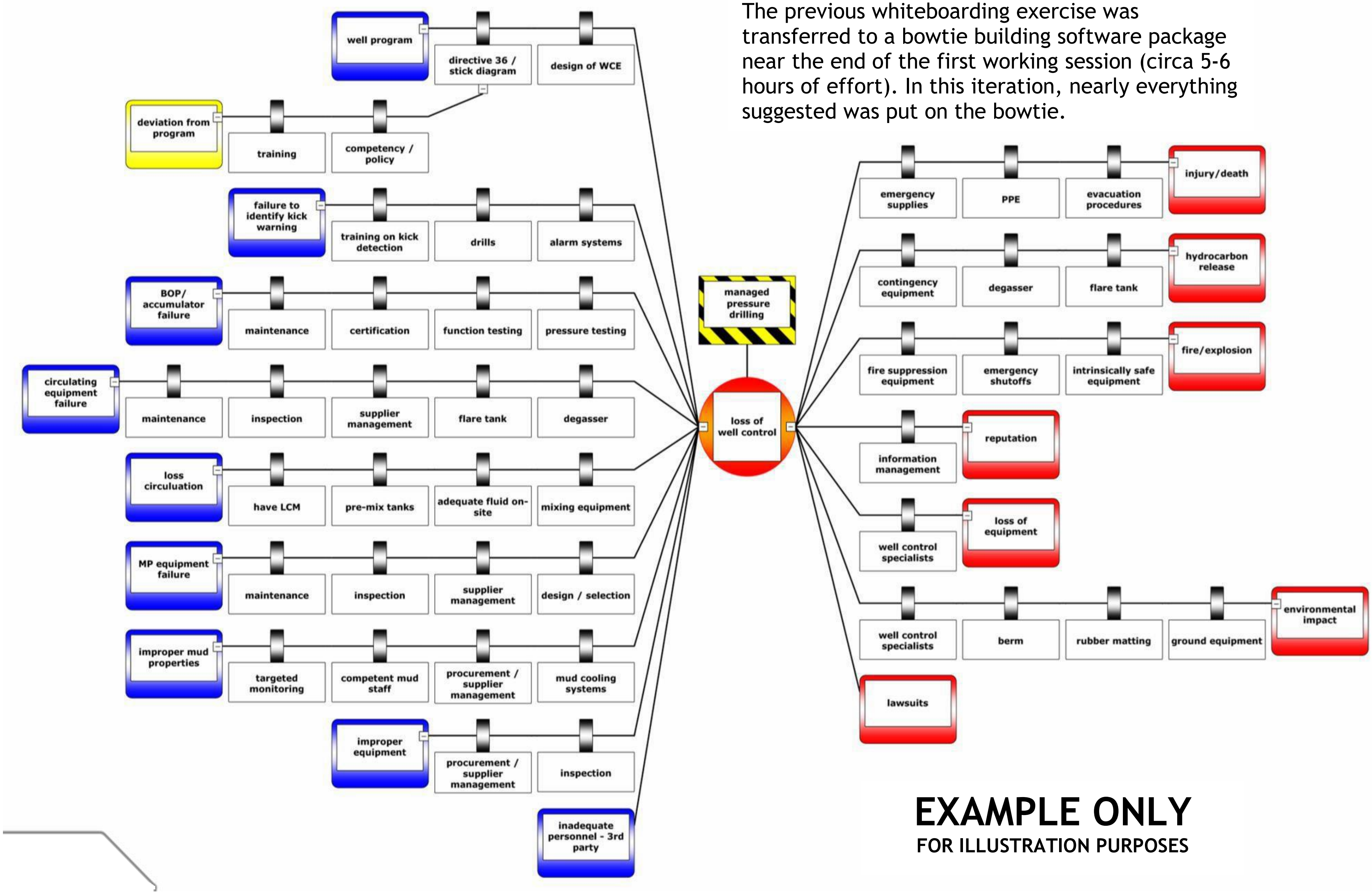
This represents the mid-point in a working session that brought together experienced drilling personnel to work out a sample bowtie for the first time.

After explaining the basics of a bowtie illustration, the groups selected a potentially hazardous operation, an appropriate top event, possible threats (in black on left), consequences (in red on right), and are now adding preventive controls (in blue). The goal in this exercise was to capture as much as possible from the operational personnel. Once the main elements are captured, fine tuning such as putting controls in an appropriate sequence, consolidating threats, or improving terminology can take place.

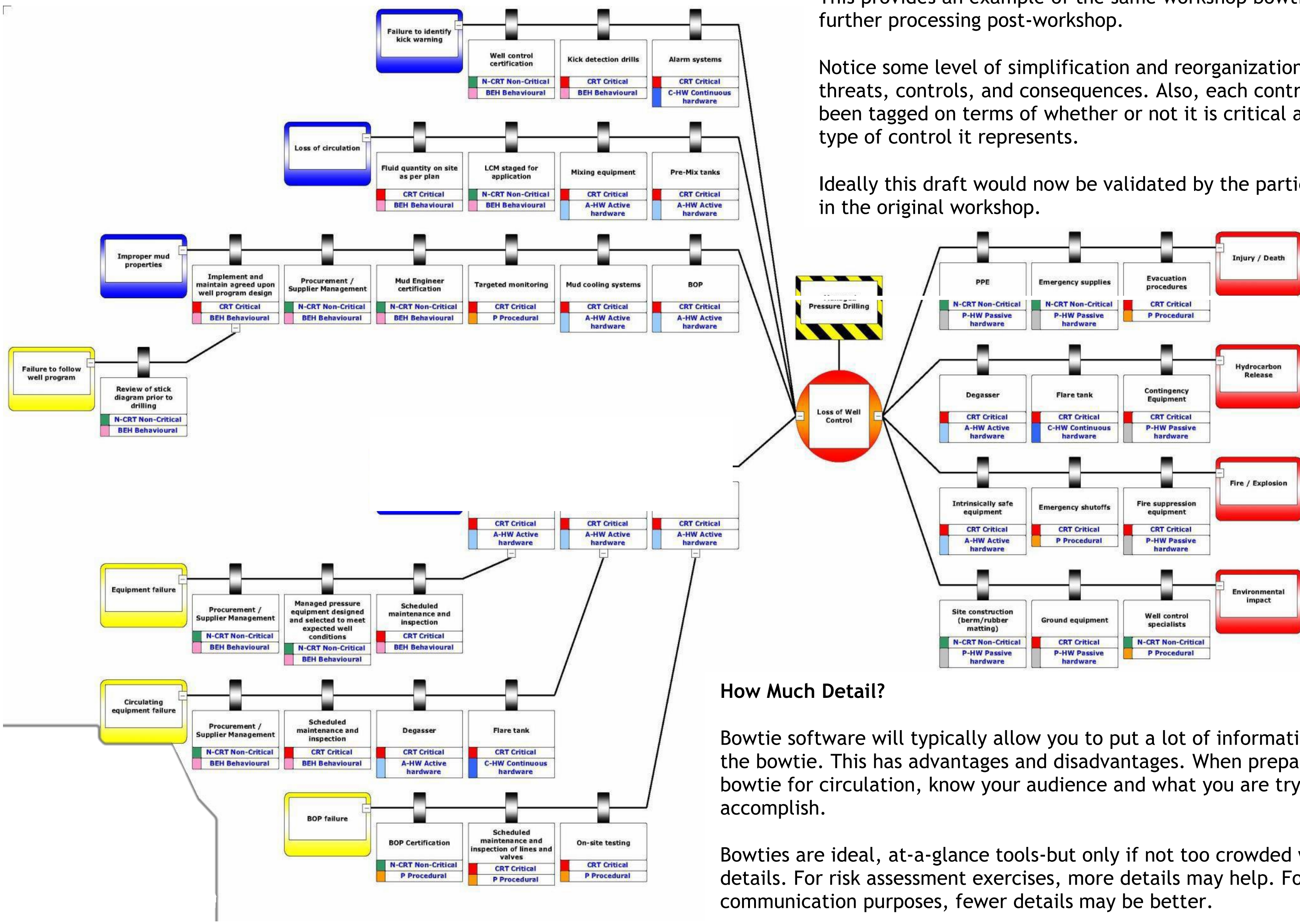


First Draft (end of first working session)

The previous whiteboarding exercise was transferred to a bowtie building software package near the end of the first working session (circa 5-6 hours of effort). In this iteration, nearly everything suggested was put on the bowtie.



EXAMPLE ONLY
FOR ILLUSTRATION PURPOSES



Second Draft

This provides an example of the same workshop bowtie after further processing post-workshop.

Notice some level of simplification and reorganization of threats, controls, and consequences. Also, each control has been tagged on terms of whether or not it is critical and the type of control it represents.

Ideally this draft would now be validated by the participants in the original workshop.

How Much Detail?

Bowtie software will typically allow you to put a lot of information onto the bowtie. This has advantages and disadvantages. When preparing a bowtie for circulation, know your audience and what you are trying to accomplish.

Bowties are ideal, at-a-glance tools-but only if not too crowded with details. For risk assessment exercises, more details may help. For communication purposes, fewer details may be better.

Appendix 7: Template and Sample of Simplified Critical Control Documentation

Simplified Critical Control Documentation Template

The following template has been adapted from the ICMM Health and Safety Critical Control Management Good Practice Guide (2015). Ideally, all essential elements should be captured on a single page and in as non-technical or specialist language as possible. If used as a communication document in hard copy, consider including a case study related to the hazard and critical control on the back for discussion purposes. Note that the number of performance requirements will vary based on the complexity of the control.

<table>
<tr><td colspan="2">**Major Hazard:**</td><td>**Owner:**</td></tr>
<tr><td colspan="2">**Critical Control Name:**</td><td>**Owner:**</td></tr>
<tr><td colspan="3">**Critical Control Objective:**</td></tr>
<tr><td>**Performance Requirements**</td><td>**Supporting Activities / Dependencies**</td><td>**Verification Activities**</td></tr>
<tr><td></td><td></td><td>**Owner:**</td></tr>
<tr><td></td><td></td><td>**Owner:**</td></tr>
<tr><td></td><td></td><td>**Owner:**</td></tr>
<tr><td colspan="3">**Triggers for Investigation / Shut down:**</td></tr>
</table>

Sample of Critical Control Documentation

<table>
<tr><td colspan="2">Major Hazard: Loss of containment when hydrocarbons and H2S enter the wellbore during tripping out of hole</td><td>Owner: Drilling Manager, Operations (Drilling company)</td></tr>
<tr><td colspan="2">Critical Control Name: Blow Out Preventer (BOP)</td><td>Owner: Regional Drilling Manager, Operations (Drilling company)</td></tr>
<tr><td colspan="3">Critical Control Objective: Shut in and containment of hydrocarbons within 50 meters of well (out of atmosphere)</td></tr>
<tr><th>Performance Requirements</th><th>Supporting Activities/Dependencies</th><th>Verification Activities</th></tr>
<tr><td>Certification is current (yes/no)</td><td>Certification every 3 years (as per AER Directive 36: shop servicing and testing)</td><td>Automatic advance warning and notification of expiry dates in asset management system
Owner: Maintenance Manager, Operations (Drilling company)

Twice a year audit of expiry dates and recertifications in asset management system

Owner: Regional Manager, Operational Excellence (Drilling company)</td></tr>
<tr><td>Holds pressure to a specified regulated pressure documented in tower sheet (Yes/No)</td><td>Documented pressure test prior to drilling out casing and time interval determined testing</td><td>Confirmation of BOP tickets: Rig Manager-Second Line BOP Drillers-First Line BOP tickets

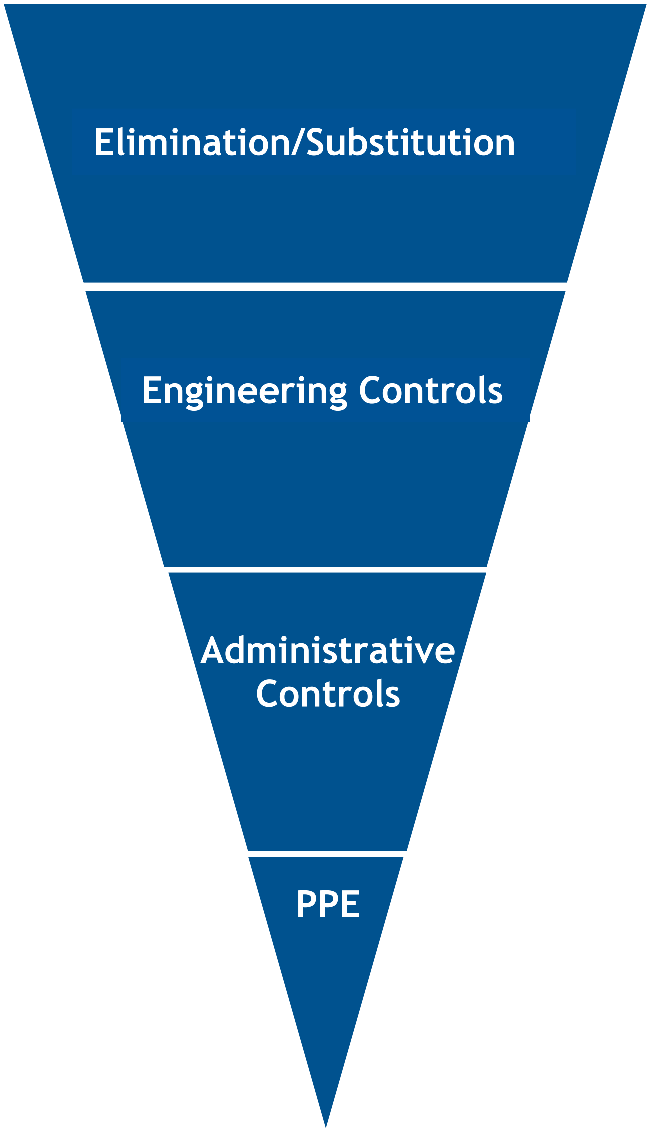
Pressure test documentation in tower reviewed during drilling supervisor field visit (minimum once every 3 months)
Owner: Rig Manager (Operator) and Drilling Supervisor (Drilling Company)</td></tr>
<tr><td>Drilling crew fully competent in BOP shut in</td><td>Weekly BOP Drill conducted and documented by Driller in tower sheet

Identified deficiencies corrected within reasonable time frame</td><td>BOP drills and corrective action log documentation reviewed during drilling supervisor field visit (minimum once every 3 months)
Owner: Drilling Supervisor (Drilling Company)</td></tr>
<tr><td colspan="3">Triggers for Investigation/Shut down:
Any loss of control resulting in a loss of containment of hydrocarbons above or downhole
Any more than 1 failure in BOP certification, 2 missed pressure tests, or missed drills</td></tr>
</table>

Appendix 8: The Hierarchy of Controls Applied to Fire and Explosion Hazards

The following diagram was designed to illustrate control priorities when managing fire and explosion hazards in upstream oil and gas operations. The hierarchy of controls is one way to “weigh”, rather than “count” controls. The most effective and reliable controls are at the top, with generally decreasing reliability and effectiveness as one descends down the hierarchy of controls.

Standard Hierarchy of Controls



Fire and Explosion Control Priorities (with e.g.'s)

- Design for minimum risk through "inherently safer" concept
  - Eliminate flammable fluids
  - Substitute for higher flash point
  - Increase distance
  - Reduce corrosion rates through improved metal section

- Incorporate safety devices or protective safety design features
  - Relief valves, automated emergency isolation valves, or automated depressurization / deinventory devices
  - Active / passive fire protection
  - Meeting electrical classification requirements
  - Backflow prevention systems and blowout preventers
  - Flare and disposal systems

- Automated warning devices / signals (requiring manual intervention in response)
- Administrative controls & procedures
  - Standard operating procedures
  - Emergency operating procedures
  - Startup / shut down procedures
  - Access controls

- Personal Protective Equipment
  - Fire resistant coveralls / clothing / undergarments
  - Safety glasses
  - SCBA or respirator for egress

Appendix 9: Advanced Process Hazard Assessment (PHA) Methodologies

The following provide a brief introduction to the range of process hazard assessment (PHA) methodologies typically practiced in contexts where process safety is a longstanding practice (e.g., chemical manufacturing, refining, etc.).

What-If Analysis and Checklists

A What-If analysis is a simple qualitative hazard identification method which can be used in the early stages of a project, or for non-complex processes. The attraction of a What-If is the intuitive ease of the method (it is inherently understood by almost all). However, the drawback of this method is that it can fail to capture cause-consequence pairs since its success is very much a function of the knowledge of the resources used to develop the What-If method. The What-If method can be supplemented by a series of Checklists which point out common equipment failure mechanisms, but the study may still be deficient if the individual does not have adequate experience with these methods.

A Checklist is a very simple risk review method, but its drawback lies in its simplicity. Checklists by themselves can limit the thought processes of the review team, and so the use of a Checklist prior to a What-If review is not recommended. Similarly, a checklist by itself can narrow the focus and attention of the review team to the content of the checklist and reduce their ability to validate the local environment and risk conditions. Hence, performing Checklist reviews in isolation of other techniques is not recommended.

Hazard and Operability Study (HAZOPS)

This hazard identification and assessment method is used to identify the consequences of deviating from the defined operating parameters of the process under study. It uses guidewords to determine the effect of deviations from the parameters at a theoretical point in the process referred as a node. The node is chosen to be representative of a section of the process which operates at the same conditions. The technique can be time consuming and requires the input of key personnel, knowledgeable of the design intention of the process, as well as the current operation of the process.

Failure Mode and Effect Analysis (FMEA)

This method focuses on analysing equipment performance by evaluating how equipment could fail and the consequences. This hazard assessment identifies the failure modes of equipment components and the effect of the failure mode on the critical function of the equipment. The failure mechanism is assigned severity, frequency or probability, and criticality scores to determine a rank ordering of failure mechanisms for the components, which is then used to assign a priority for design improvement. This method is a semi quantitative method. The technique can be time consuming and requires the input of key personnel, knowledgeable of the design intention of the components, as well as the current operation of the equipment. Although the concept of components and equipment can be extended to larger scale chemical processes, the technique is often most useful when examining the failure mechanisms of individual machines. The FMEA approach has a well- deserved reputation for efficiently analysing the hazards associated with electronic and computer systems or systems which primarily have binary states, whereas the HAZOP Study approach may not work as well for these types of systems.

Layer of Protection Analysis (LOPA)

This method is a semi quantitative tool for analysing and assessing risk. In LOPA, the individual protection layers proposed or provided for a hazard scenario are analysed for their effectiveness. The analysis typically considers single cause-consequence pairings. The combined effects of the protection layers are then compared against risk tolerance criteria. The method is often used to facilitate communication (e.g. SIS, SIF, SIL, IPL) between the hazard and risk analysis community and the process control community and is often used in support of calculations required by IEC 61508, IEC 61511, and ISA84. The method is not as robust as a Fault Tree analysis since the logic typically concentrates on simultaneous conditions and circumstances. As such, the Boolean logic underlying the analysis is typically only considering "AND" functionality, as compared to Fault Tree analyses which consider both "ANDs" and "ORs".

Event Tree Analysis (ETA)

This analysis is typically used to document the development of a specific event (from its initiation to its various consequences). The method is a quantitative risk assessment and is similar to a fault tree analysis except in its approach to the flow of information. In an event tree, the information flows from the initiating event to the final outcomes (for example explosion, pool fire, jet fire, flash fire, toxic release). It models the order in which the elements fail. Additionally, an event tree may not include common cause failure which is included in fault tree analyses. The method is an example of inductive reasoning.

Fault Tree Analysis (FTA)

This analysis method is typically used to document the development of a specific event from its final outcome back to its various causes. The method is a quantitative risk assessment and is similar to an Event Tree analysis, except in its approach to the flow of information. In a Fault Tree, the information flows from the final outcome event to the initial causes. Each branch of the tree uses Boolean logic diagrams to develop all possible prerequisites for a specific condition to occur, until all initiating conditions are identified. As such, this method is an example of deductive reasoning.

The method will take into account the frequency distributions of each element of the tree, as well as any common cause failure probabilities. A Fault Tree will calculate the frequency of the final outcome by Boolean logic. It will also allow the analysis of the system to evaluate the shortest path from initiating events to final outcome. The technique can be very time consuming and requires the input of key personnel knowledgeable in the specific technique, the design intention of the process, the failure modes, and the current operation of the process.

Guidance regarding the technique can be found in many monographs and training sessions, including:

Quantitative Risk Analysis (QRA)

This method is a fully quantitative method which determines the frequency, likelihood, and consequences of hazardous events. In this technique, a team will examine a process and develop a list of all hazardous events which have the potential to exist in that process. These hazardous events are examined to determine all the means with which they can be caused. The probability of various outcomes is then developed. Estimating the frequencies and consequences of rare accidents is a synthesis process that provides a basis for understanding risk. Using this synthesis process, you can develop risk estimates for hypothetical accidents based upon your experience with the individual basic events that combine to cause the accident. (Basic events typically include process component failures, human errors, and changes in the process environment, and more information is usually known about these basic events than is known about accidents.) System logic models are used to couple the basic events together, thus defining the ways the accident can occur. Typically, the results of these analyses are summarized in F-N curves, and aggregate fatality estimates, although different criteria can be considered.

Bowtie Diagrams

In and of themselves, Bowtie Diagrams are not typically used in quantitative process hazard analysis. Rather, they can be used to capture and communicate the findings of any of the methods listed above or a structured, qualitative hazard evaluation where processes are well understood. They are frequently used in European safety case studies when quantification is not possible or desirable. Bowtie Diagrams are simple summaries that can help illustrate the multiple threats that contribute to a single hazardous scenario, the preventative controls used to stop the event from being realized, and the corrective or mitigative controls, that can then be used to reduce the impact of the hazardous event on a number of risk receptors. The diagrams are useful in their simplicity and clarity. However, they can become difficult when they are used as the basis for a probability calculation, or if they are used to show the effect of multiple initiating threats on multiple hazardous scenarios. It combines two methodologies presented in earlier sections, Fault Tree Analysis and Event Tree Analysis, and uses the format of an incident investigation and root cause analysis technique known as Causal Factors Charting. The Bow Tie analysis offers a cost- effective approach for a screening hazard evaluation of processes that are well understood. This approach is a qualitative hazard evaluation technique ideally suited for the initial analysis of an existing process, or application during the middle stages of a process design.

Aligning PHA methodology and Types of Operations / Processes

Different PHA methodologies will offer strengths and weaknesses depending on the nature of the operation or type of process under review. For example, some methods such as What- If/Checklist Analysis, HAZOP Studies, Event Tree Analysis and Human Reliability Analysis are better able to analyse batch processes than others (e.g. Fault Tree Analysis, FMEA, Cause- Consequence Analysis). These latter methods cannot easily deal with the need to evaluate the time-dependent nature of batch operations.

In the following table, PHA techniques are matched with corresponding objectives. These judgments are intended for preliminary use only and is not exhaustive in terms of assessment methodologies.

OBJECTIVE	FORMAL ASSESSMENT	FIELD LEVEL ASSESSMENTS
Summary information uses	• Bow Tie Diagrams • Event Tree Analysis	• Bow Tie Diagrams • Event Tree Analysis
Technology design and selection issues	• What If/Checklists • HAZOP • FMEA • Event Tree • Analysis • Quantitative Risk Analyses • Fault Tree Analysis	• Bow Tie Diagrams • What If/Checklists • Job/Task Safety Analyses

Day-to-day tasks	• What If/Checklists • Critical Operating Procedure Reviews • Event Tree Analysis	• What If/Checklists • Job/Task Safety Analyses
Special tasks	• What If/Checklists • HAZOP • FMEA • Event Tree Analysis	• What If/Checklists • Job/Task Safety Analyses
Management of Change Issues	• What If/Checklists • HAZOP • FMEA • Event Tree Analysis • Quantitative Risk Analyses • Fault Tree Analysis	• What If/Checklists • Job/Task Safety Analyses
Investigations	• Root Cause Analysis • Event Tree Analysis • Fault Tree Analysis	

For further study,

- *Guideline for Hazard Evaluation Procedures*, 3rd edition, Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers (AIChE), New York, NY 2008, ISBN 978-0-471-97518-2
- *Evaluating Process Safety in the Chemical Industry – a User's Guide to Quantitative Risk Analysis,* Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers, (AIChE), New York, NY 2000, ISBN 0-8169-0746-3
- *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd edition, Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers, (AIChE), New York, NY 2000, ISBN 978-0-8169-0720-5
- *Guidelines for Developing Quantitative Safety Risk Criteria*, Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers, (AIChE), New York, NY, 2009, ISBN 978-0-470-26140-8
- Smith, David J., *Reliability, Maintainability and Risk* - Practical Methods for Engineers, 7th edition, Elsevier, Burlington MA, 2005, ISBN 978-0-7506-6694-7
- *Layer of Protection Analysis - Simplified Process Risk Assessment,* Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers, (AIChE), New York, NY, 2001, ISBN 0-8169-0811-7
- *Guidelines for Safe and Reliable Instrumented Protective Systems*, Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers, (AIChE), New York, NY, 2007, ISBN 978-0-471-97940-1

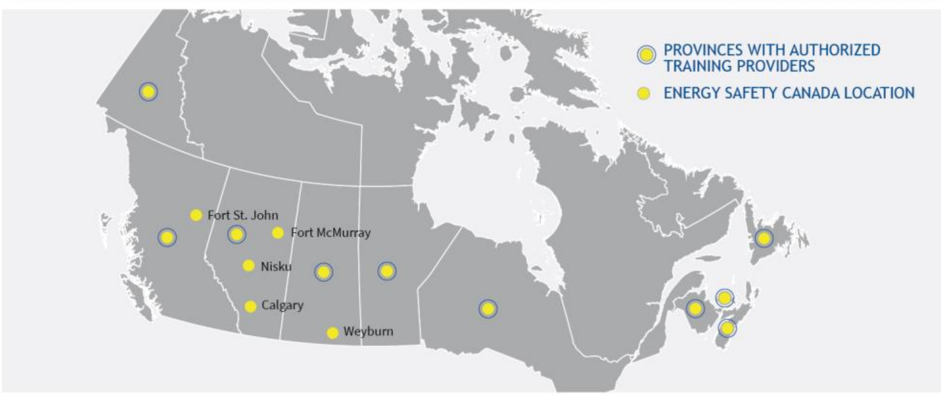
- *Guidelines for Enabling Conditions and Conditional Modifiers in Layer of Protection Analysis,* Center Chemical Process Safety (CCPS), American Institute of Chemical Engineers, (AIChE), New York, NY, 2014, ISBN 978-1-118-77793-0
- *Guidelines for Risk Based Process Safety*, Center for Chemical Process Safety (CCPS), American Institute of Chemical Engineers, (AIChE), New York, NY, 2007 ISBN 978-0-470-16569-0
- Tweeddale, Mark, *Managing Risk and Reliability in Process Plants*, Elsevier Science (USA), Burlington MA, 06/2003, ISBN 0-7506-7734-1

SAFETY DOESN'T CLOCK IN AND IT DOESN'T PUNCH OUT. IT'S 24/7.

ENERGY SAFETY SERVICES:

- Virtual training
- Safety services
- Company consultations
- Data reports
- Certificate of Recognition

LOCATED WHERE YOU ARE:



Phone:	Email:	Web:
1 800 667 5557	Safety@EnergySafetyCanada.com	EnergySafetyCanada.com