Overview of the CyberPHA Methodology Including Visualization of the Results Using Bowties

John Cusimano
VP, Industrial Cybersecurity
aeSolutions

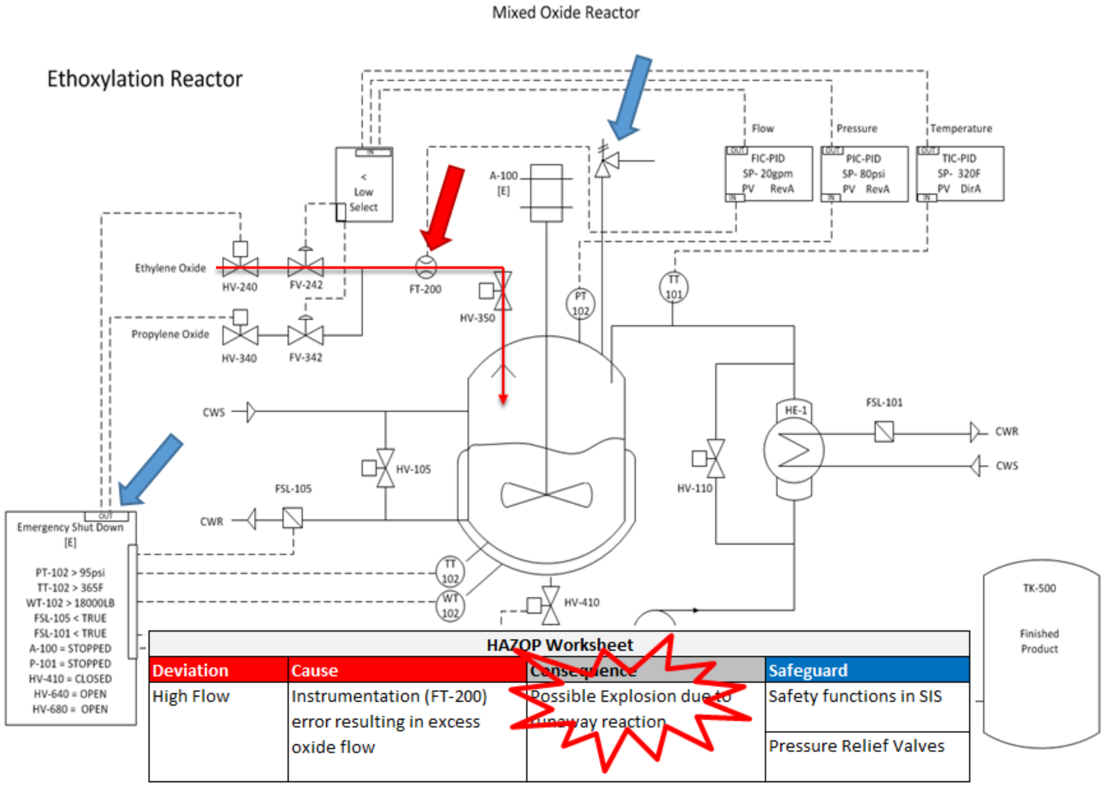
Tim Gale
Senior Industrial Cybersecurity Specialist
aeSolutions

This paper summarizes the CyberPHA security risk assessment methodology, and the use of Bowties to visualize the results.

What is a PHA?

PHA stands for Process Hazard Analysis. It is an organized approach to evaluate hazards associated with industrial processes. Performing such studies is mandated in the US by the process safety management regulation (29 CFR 1910.119). There are many approaches available, such as HAZard and OPerability (HAZOP), Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), What-If, and more.

Figure 1 is an example of a Piping and Instrumentation Diagram (P&ID) of an industrial process, along with a HAZOP worksheet.



HAZOP Worksheet

Deviation	Cause	Consequence	Safeguard
High Flow	Instrumentation (FT-200) error resulting in excess oxide flow	Possible Explosion due to runaway reaction	Safety functions in SIS Pressure Relief Valves

Figure 1: P&ID and HAZOP worksheet

The HAZOP methodology consists of partitioning the process into “nodes” to be evaluated. A diverse team reviews the impact of process conditions (flow, level, temperature, pressure, etc.) by asking deviation questions (too high, too low, zero, reverse, other than, etc.). The group determines and documents what might cause such a scenario, and what its impact might be. In Figure 1, the cause of a high flow deviation is a malfunctioning flow transmitter. The resulting consequence could be a possible explosion. The team then considers safeguards that could prevent or mitigate the event, thus lowering the overall risk. Recommended safeguards in this case include a safety instrumented function, and pressure relief valves.

What is a CyberPHA?

The CyberPHA methodology was developed around 2012. It is a methodology to conduct a security risk assessment for a control or safety system. It is a systematic, consequence-driven approach, very similar to a PHA. A CyberPHA partitions the control system into zones (areas) and conduits (communication paths between them). A diverse team of multiple engineering disciplines (process safety, automation, industrial IT, security, facilitator and scribe) evaluates the threats, vulnerabilities, and consequences of a compromise of the control or safety system. The methodology aligns with standards such as ISA/IEC 62443-3-2, a recently published standard on “Security Risk Assessment for System Design”. It also aligns with ISA technical reports such as ISA TR84.00.09 “Cybersecurity Related to the Functional Safety Lifecycle”.

The methodology leverages established process safety information and techniques. A PHA will identify hazards; a CyberPHA evaluates whether those hazards could be caused by a cyber compromise, and if so, what the consequence would be. It identifies the threats and vulnerabilities that could make each scenario possible. The team identifies these cyber hazards and risks. A key deliverable of the study is a risk ranked mitigation plan. Personnel can then implement countermeasures in the control system as additional layers of protection to lower the risk.

As shown in Figure 1, the PHA looks at the physical process or plant equipment. The CyberPHA, however, looks at the control and/or safety system that might be the cause of a deviation, or might suppress a safeguard. It adds a threat source to the analysis. It considers the vulnerabilities and threats that could be acting on the control system to see if they could lead to those consequences, how that might occur, and most importantly, what countermeasures are in place, and what additional countermeasures should be added to mitigate the risk.

The Five Steps of a CyberPHA

The CyberPHA process includes five basic steps, as shown in Figure 2.

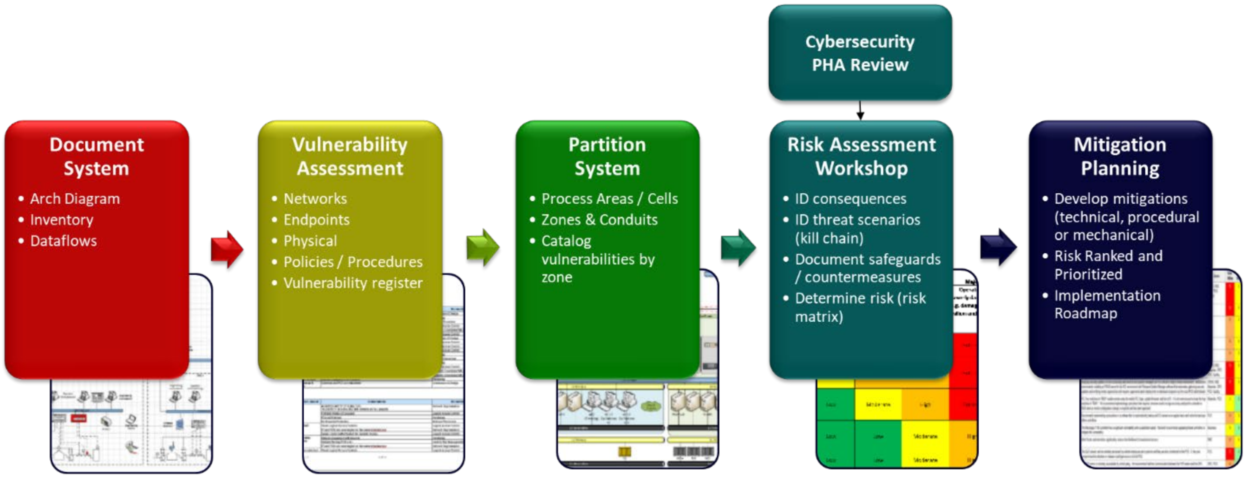
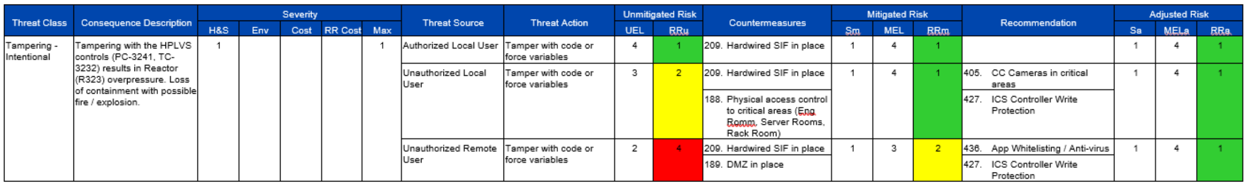


Figure 2: Five steps of a CyberPHA

Like a PHA, there is work that needs to be completed up front. The team needs information about the control system, the networks, servers, etc. The first step is to document the system, typically in a network architecture diagram. This is analogous to the P&IDs used in the PHA. It includes an inventory of the devices on the network and the data flows. The team then evaluates the potential vulnerabilities or weaknesses in the networks, end points, the physical security for the system, policies and procedures. This information is entered into a vulnerability register. The system is then partitioned into process areas, security zones, and conduits. This is analogous to defining nodes in a PHA. The team can then perform a cyber consequence assessment. This consists of a review of the PHA to identify the highest consequence events that could potentially be caused by a cyber compromise. Either the initiating event or safeguard could be cyber vulnerable. Once all the above information is available, a risk assessment workshop may be conducted, similar to a HAZOP. The team proceeds zone by zone, identifies consequences, threat scenarios, safeguards, and ultimately evaluates the risk. This information is then used to create a mitigation plan. All the recommendations are risk ranked, and an implementation roadmap is established.

What do the results of a CyberPHA look like?

Figure 3 shows the results of a CyberPHA. It looks very much like a HAZOP worksheet and is presented in a tabular format. The table contains a large amount of information, including the highest risk scenarios and the means to mitigate the risk. However, the tabular format may be difficult to interpret by those not familiar with CyberPHAs. This is where Bowtie comes in.



Threat Class	Consequence Description	Severity					Threat Source	Threat Action	Unmitigated Risk		Countermeasures	Mitigated Risk			Recommendation	Adjusted Risk		
		H&S	Env	Cost	RR Cost	Max			UEL	RRu		Sm	MEL	RRm		Sa	MELa	RRa
Tampering - Intentional	Tampering with the HPLVS controls (PC-3241, TC-3232) results in Reactor (R323) overpressure. Loss of containment with possible fire / explosion.	1				1	Authorized Local User	Tamper with code or force variables	4	1	209. Hardwired SIF in place	1	4	1		1	4	1
							Unauthorized Local User	Tamper with code or force variables	3	2	209. Hardwired SIF in place 188. Physical access control to critical areas (Eng Romm, Server Rooms, Rack Room)	1	4	1	405. CC Cameras in critical areas 427. ICS Controller Write Protection	1	4	1
							Unauthorized Remote User	Tamper with code or force variables	2	4	209. Hardwired SIF in place 189. DMZ in place	1	3	2	436. App Whitelisting / Anti-virus 427. ICS Controller Write Protection	1	4	1

Figure 3: Sample of a CyberPHA table

What is a Bowtie?

A Bowtie is a graphical way to depict pathways from the cause, the top event, and the consequence. It depicts the different causes and consequences of an event, and the controls that are in place to reduce the risk. Prevention barriers (those intended to prevent an event or lower its probability) are show on the left of the top event. Mitigation barriers (those designed to lessen the consequence, or the severity, of an event that has already happened) are shown on the right of the top event. The diagram resembles a man's bowtie, hence the name.

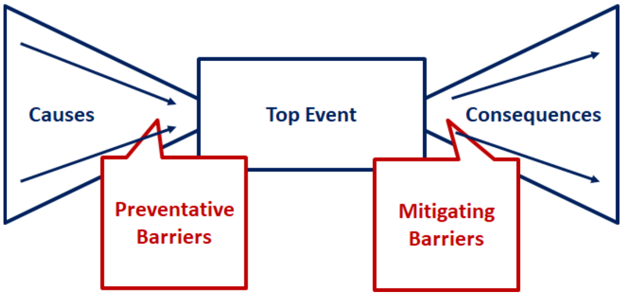


Figure 4: Bowtie basics

Figure 5 is an example of a cybersecurity Bowtie. It shows the various causes, prevention barriers, top events, mitigating barriers, and consequences. The diagram graphically shows the progression of events.

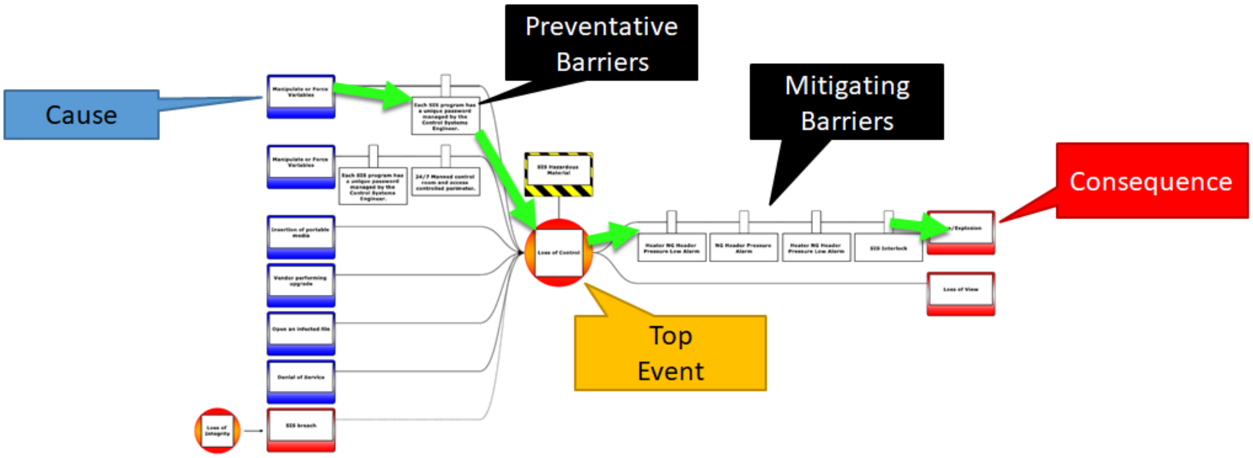
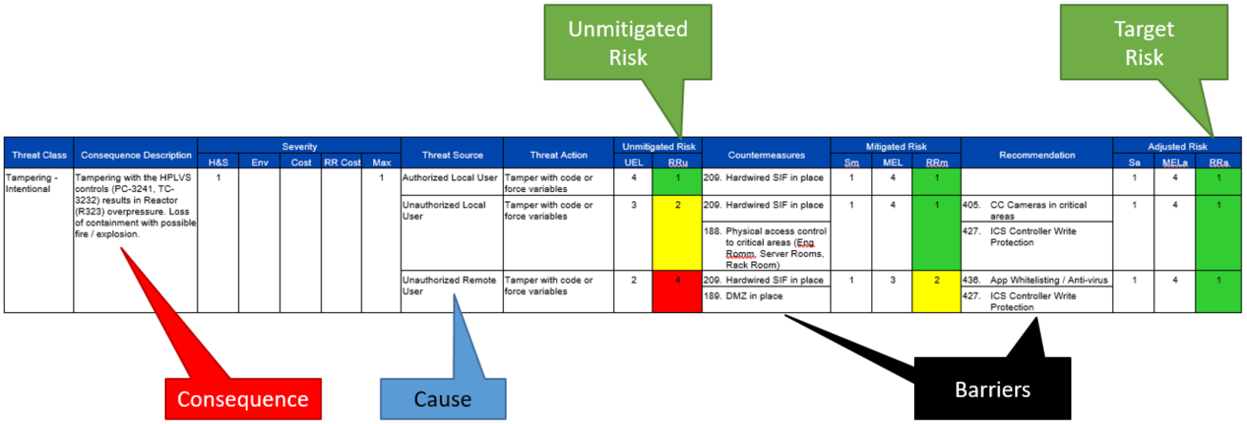

Preventative Barriers
Mitigating Barriers
Cause
Consequence
Top Event
Manipulate or Force Variables
Each SIS program has a unique password managed by the Control Systems Engineer.
Manipulate or Force Variables
Each SIS program has a unique password managed by the Control Systems Engineer.
24/7 Manned control room and access controlled perimeter.
SIS Hazardous Material
Insertion of portable media
Vendor performing upgrade
Open an infected file
Denial of Service
Loss of Integrity
SIS breach
Loss of Control
Heater NG Header Pressure Low Alarm
NG Header Pressure Alarm
Heater NG Header Pressure Low Alarm
SIS Interlock
/Explosion
Loss of View

Figure 5: CyberPHA Bowtie example

PHA/Bowtie comparison

Figure 6 is an example of one PHA result showing consequence, cause, barriers, and risk levels. A full study would include hundreds of rows of such results. Such a massive table can be difficult to interpret without a basic knowledge of how the PHA process works.


Unmitigated Risk
Target Risk
Consequence
Cause
Barriers

Threat Class	Consequence Description	Severity					Threat Source	Threat Action	Unmitigated Risk		Countermeasures	Mitigated Risk			Recommendation	Adjusted Risk		
		H&S	Env	Cost	RR Cost	Max			UEL	RRu		Sm	MEL	RRm		Sa	MELa	RRa
Tampering - Intentional	Tampering with the HPLVS controls (PC-3241, TC-3232) results in Reactor (R323) overpressure. Loss of containment with possible fire / explosion.	1				1	Authorized Local User	Tamper with code or force variables	4	1	209. Hardwired SIF in place	1	4	1		1	4	1
							Unauthorized Local User	Tamper with code or force variables	3	2	209. Hardwired SIF in place 188. Physical access control to critical areas (Eng Romm, Server Rooms, Rack Room)	1	4	1	405. CC Cameras in critical areas 427. ICS Controller Write Protection	1	4	1
							Unauthorized Remote User	Tamper with code or force variables	2	4	209. Hardwired SIF in place 189. DMZ in place	1	3	2	436. App Whitelisting / Anti-virus 427. ICS Controller Write Protection	1	4	1

Figure 6: PHA example

It is possible to take high risk scenarios and show before and after snapshots. Figure 7 shows the unmitigated 'before' risk with no barriers or controls in place. Causes are shown on the left, and consequences on the right. The result in this example is high risk.

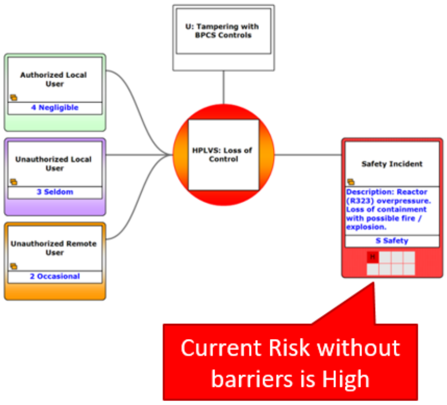

U: Tampering with BPCS Controls
Authorized Local User
4 Negligible
Unauthorized Local User
3 Seldom
Unauthorized Remote User
2 Occasional
HPLVS: Loss of Control
Safety Incident
Description: Reactor (R323) overpressure. Loss of containment with possible fire / explosion.
5 Safety
H
Current Risk without barriers is High

Figure 7: Bowtie example for unmitigated risk

Figure 8 depicts the same scenario, this time showing the existing barriers, and recommended barriers. The result now is lower risk.

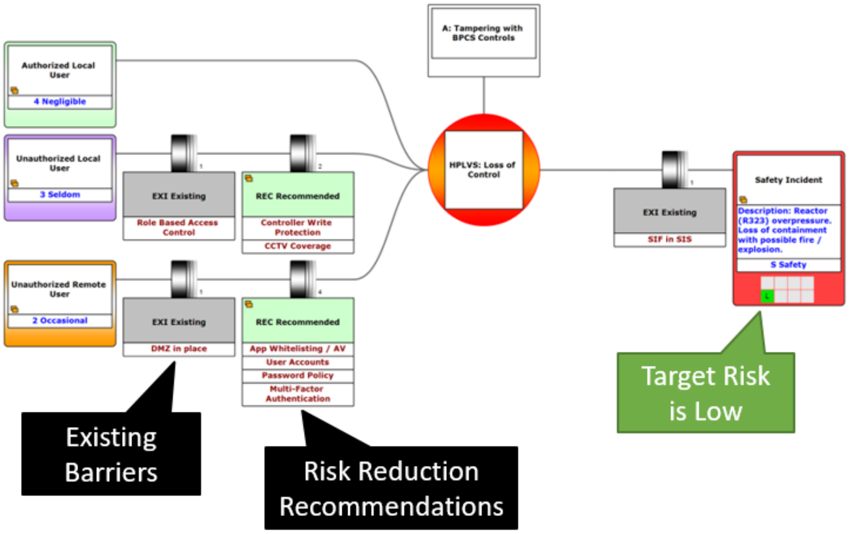


Figure 8: Bowtie example for mitigated risk

Conclusions

Bowtie diagrams provide a more graphical and intuitive representation of complex risk assessments compared to a PHA table. Minimal effort is needed to generate Bowties from existing PHA results, as automated tools are available. Bowties can be used to show the before and after views of a scenario. These graphical diagrams are more easily comprehended by stakeholders and management than mere tables. While it may not be necessary to go through a CyberPHA for less complex facilities, aeSolutions has found that for more complex facilities it is more efficient to do the CyberPHA to record the results, especially if the study is being led live with a team. Bowtie templates can be created for more common scenarios, and libraries can be created to help drive efficiency.