

## CHASE - Visualising cyber security vulnerabilities and risk

Andy Geddes, PX Group, Stockton-on-Tees, UK, and David Hatch, Process Safety Integrity, Derby, UK

This paper presents an approach (CHASE - Cyber Hazard and Security Evaluation) which exploits the collaboration and communication power of bowtie analysis combined with the systematic rigour of HAZOP (or CHAZOP = Computer HAZOP) to efficiently and effectively create Simple and Detailed Risk Assessments associated with the unauthorised operation and/or data manipulations within Industrial Automation Control Systems (IACS).

The technique follows the principles of IEC 62443 (via OG-0086) and the US National Institute of Standards and Technology (NIST) guidance to challenge the IACS zones and conduits (similar to HAZOP nodes and deviations) to identify and evaluate threat events. This enables qualitatively determined appropriate security levels and semi-quantitative prediction of the risks associated with major accidents (COMAH Regulations 2015) and loss of essential services (NIS Regulations 2018).

A graphical format allows the analysis team to more quickly and effectively identify the relationship between physical assets containing hazards, or providing essential services, and the IACS assets that are either critical or related to preventing major accidents or loss of essential services.

Keywords: Bowties, Cyber Security, Essential Services, Functional Safety, Industrial Automation and Control Systems, Major Accidents, Process Hazard Analysis, Process Safety.

### Introduction

Cyber security is wrongly perceived as the responsibility of the IT department in the same way as functional safety is attributed to the Control and Instrumentation engineering discipline. In practice, cyber security is the responsibility of the company Executive Team and covers people, procedures, physical and IT security, asset management and risk assessment. The threats and consequences associated with cyber security are very broad.

While there is growing concern about cyber attacks, attackers, and the general vulnerabilities of Industrial Automation Control Systems (IACS), proper consideration of the damage and destruction that can result from a breach is not always practical. Conventional analysis techniques do not support the breadth, depth and lateral thinking required to identify WHO can get in, WHERE, WHEN, and HOW they can get in and also WHAT damage they can do once they are in.

The NIS Regulations 2018 (NIS) and COMAH Regulations 2015 (COMAH) set out broad goals for the management of cyber risk resulting in the Loss of Essential Services (LSE) or release of Major Accident (MA) hazards. The National Centre for Cyber Security (NCSC) has published a sector agnostic Cyber Assessment Framework (CAF). This is not intended to assess compliance with the regulations, but to help users and regulators assess the state of cyber security. The Health and Safety Executive (HSE) acts as the Competent Authority for both NIS and COMAH, at least in the oil and gas sector, and has issued Operational Guidance (OG-0086) which they use to judge compliance with the regulations.

OG-0086 defines the basic level of compliance, and requires a Cyber Security Management System which includes risk assessment to ensure that security threats are understood and addressed. It recognises that detailed analysis is required to determine the specific potential major accident consequence of each threat and its likelihood. It also stresses that threats, and vulnerabilities to threats, change over time and that previous history does not give an indication of future likelihood.

BS EN/IEC 61511-1 Edition 2 (61511) is recognised as established good practice for functional safety in the process sector. It requires that security vulnerabilities of a Safety Instrumented System (SIS) are identified. This must assess identified threats, potential consequences, and any requirements for additional risk reduction. It also requires identification of dangerous combinations of output states of the SIS which must be avoided. Such combinations may be initiated by a cyber attack.

OG-0086 references IEC 62443-2-1 which requires both a Simple Risk Assessment to identify the most critical scenarios and a Detailed Risk Assessment to challenge the physical and functional assets to ensure that they are adequately protected. It states that assessments may be recorded in a conventional simple tabular form which is more expedient but does not offer the holistic and hierarchical oversight to move between Simple and Detailed Risk Assessments. However OG-0086 also supports the use of bowtie diagrams. This paper proposes a new use of the bowtie technique to visualise hazard scenarios in a way that facilitates Simple and Detailed Risk Assessments which follow industry good practice but in a more efficient and effective way than conventional tabular or worksheet formats.

### Cyber security and process safety

Cybersecurity is the prevention of illegal or unwanted penetration, intentional or accidental interference with normal operations, or inappropriate access to or manipulation of information. In most cases a cyber threat to an IACS has the potential to result in a process consequence. Cyber security is therefore part of process safety.

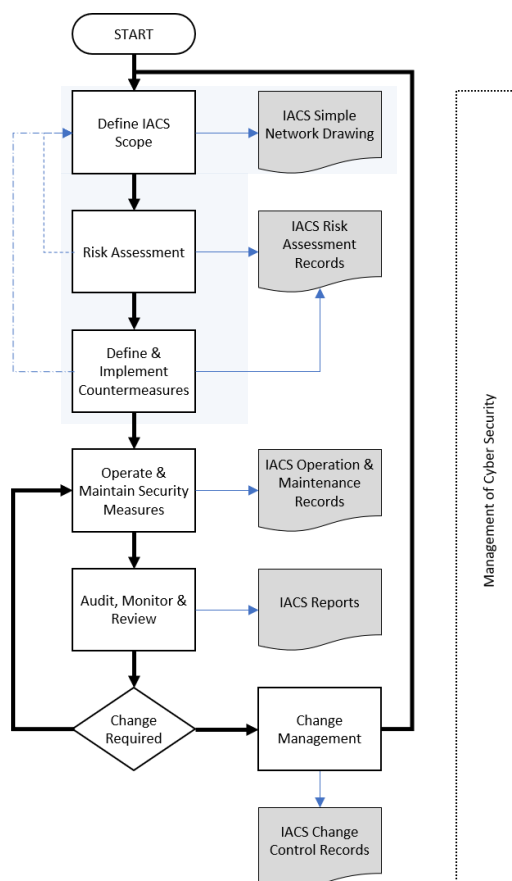
This paper presents a technique which is founded on the principles and good practice documented in HSE, NCSC, IEC and NIST publications. It recognises that as threats develop, techniques must adapt to keep pace and is therefore intended to be a modular and scalable approach which is adaptable to different scenarios.

## Scope

Cyber security (like functional safety) is a continuous process that operates within a lifecycle of analysis, implementation and operation, and which is supported by appropriate maintenance and robust management systems. The following highlighted OG-0086 lifecycle phases are the focus and scope of this paper:

- definition of IACS scope
- risk assessment
- definition and implementation of countermeasures

This is shown in **Figure 1** below, which gives an overview of the whole lifecycle in OG-0086:



**Figure 1: IACS lifecycle (OG-0086)**

### CHASE Step 1: Identifying the process zones and consequences

OG-0086 emphasises that “in order to defend a system, it is first important to know what is to be defended”. An IACS requires direct protection to avoid or reduce the indirect impact of attack on physical assets such as major unit operations or equipment. IACS consist of both physical (hardware) and logical (software) assets that may be vulnerable to attack, and good practice requires a simple network diagram to represent the key components within the IACS scope.

To illustrate the principles of asset visualisation, we shall use extracts from the Investigation into the Buncefield Fire and Explosion. Note that this source is only intended to explain the methodology and does not bear any resemblance to the actual or historical design or operation of the facility – this is a familiar case study which offers a simple process that is readily understood.

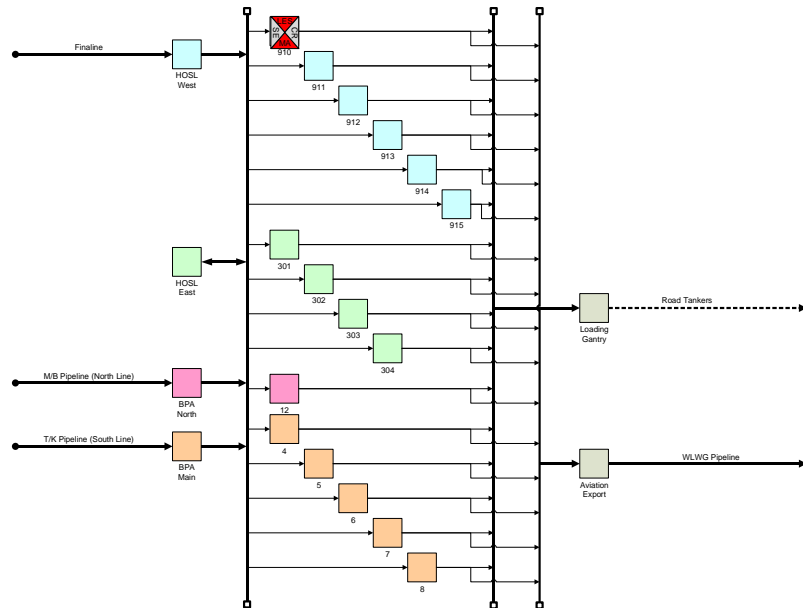
The Buncefield site was split into several process zones as shown below in **Figure 2**:



**Figure 2: Buncefield Site (Investigation Report)**

Using the numbering for the major tanks, a topological representation is constructed that condenses the process into a simple block diagram. The colours align with the sub-site colours from the map in **Figure 2** above and denote process zones.

Once the physical assets (or tanks) have been laid out they can be associated with MA and LES. However, owner/operators of Non-COMAH/NIS sites may want to consider consequences with the potential for significant harm to people,(safety) and the environment (SE), and commercial and reputational harm (CR).



**Figure 3: Buncefield Asset block diagram**

Legend used:

SE (permanent harm to People or Environment)		LES (Loss of Essential Service)	
MA (MAH/MATTE)		CR (Commercial & Reputational)	

Existing HAZOP information can be used to justify assessment of consequence. This simple block diagram will help with future decisions about how the IACS network should be segmented, particularly when designing new or replacement IACS assets.

**CHASE Step 2: Identifying IACS zones, types, inherited consequences and importance**

The breakdown of the IACS into *zones* (connected by *conduits*) is an important task that all standards and guidance require. It is comparable to the sub-division of a process or plant into nodes for HAZOP studies. In practice this is determined by historical IACS design decisions. For new IACS systems, this will require several iterations to achieve the optimum design.

Conventional diagrams such as **Figure 4** are complex and congested. Therefore, a simplified, but more information rich, network diagram is proposed, see **Figure 5**.

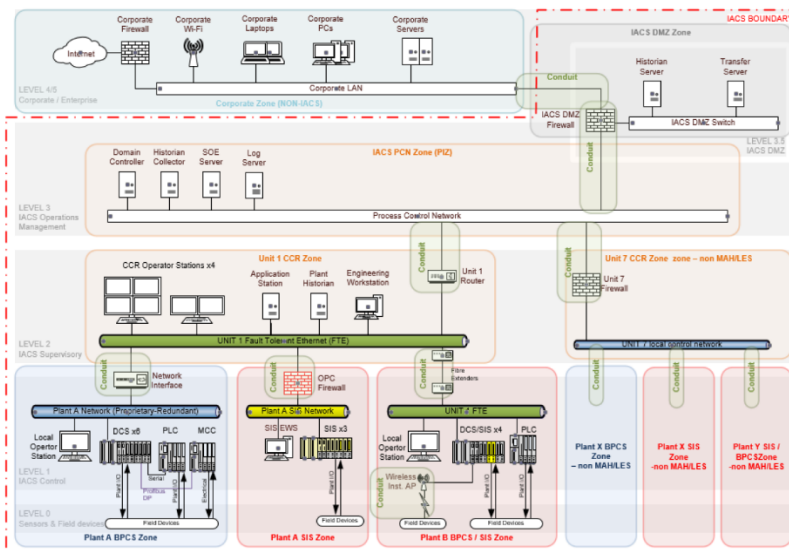


Figure 4: Typical IACS representation (OG-0086 Figure 3.3)

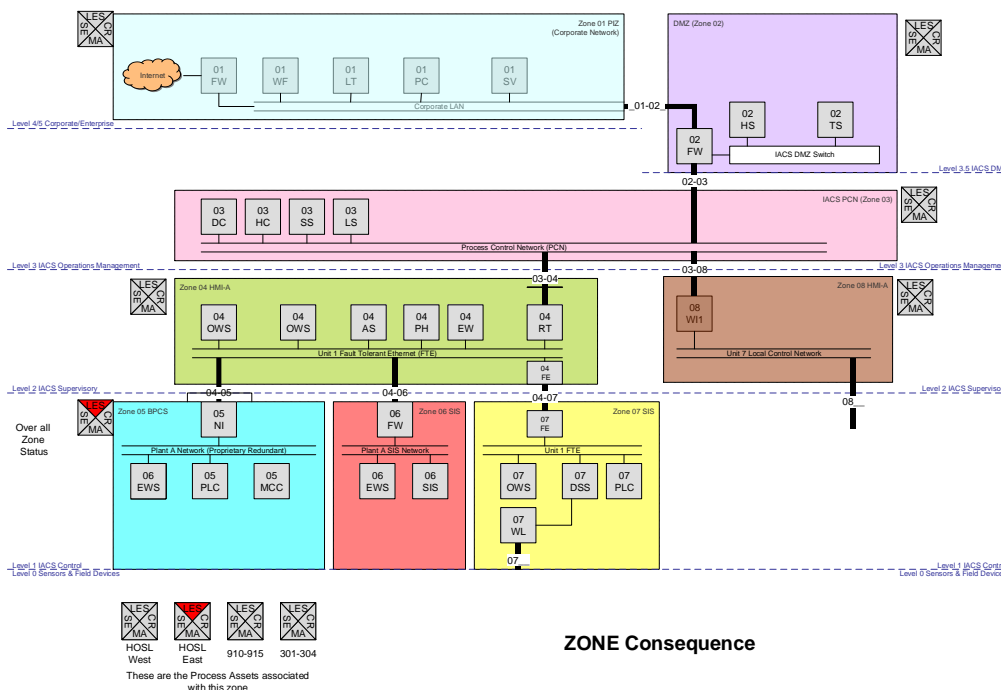


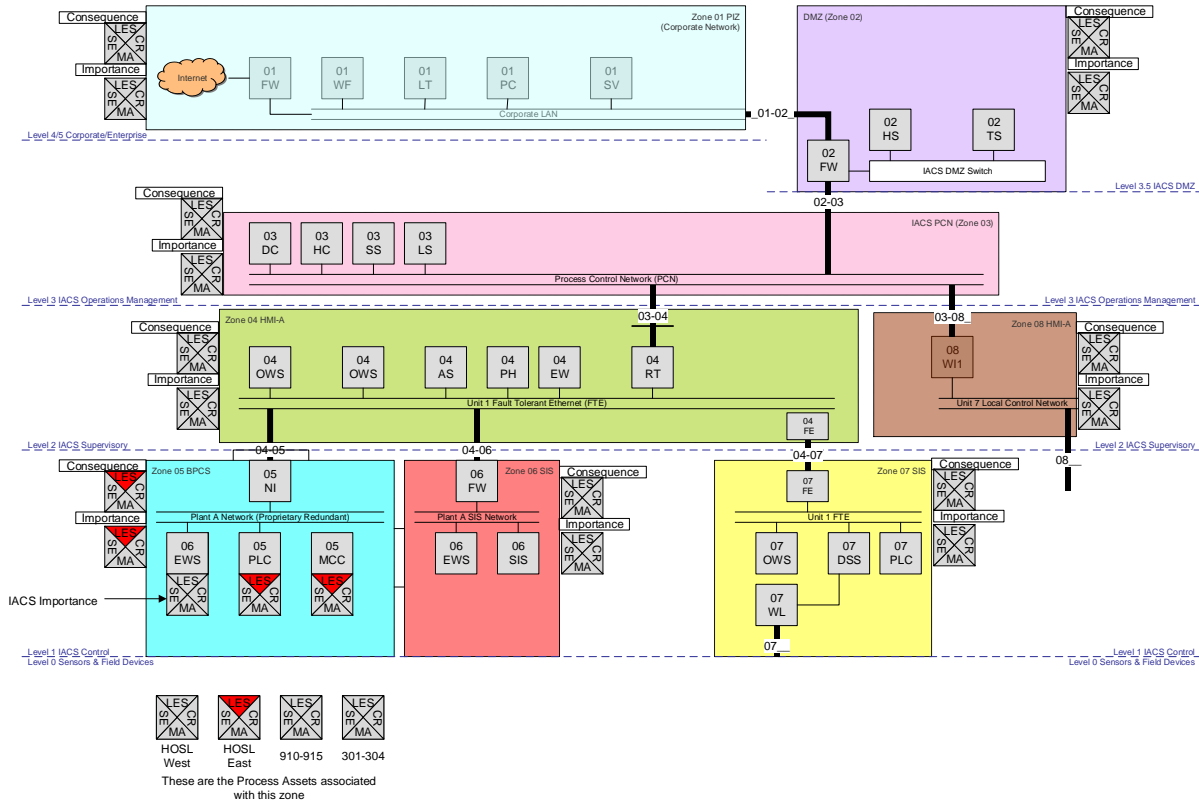
Figure 5: Simplified IACS network combined process consequences and IACS zones

The sequential numbering (01, 02, 03...) refers to the IACS zone and the 2-letter abbreviations represent the IACS asset types (FW - Firewall, WF - Wi-Fi, etc.). The conduits between zones are uniquely numbered (e.g. 02-03 is the conduit between zones 02 and 03). The zones are colour coded to clearly identify the IACS zone boundary. The IACS zones may or may not

correspond to process zones depending on the original design decisions. At this stage the type of IACS zone is identified: BPCS, SIS, etc. The IACS zone also inherits the worst consequence from all the associated Process zones.

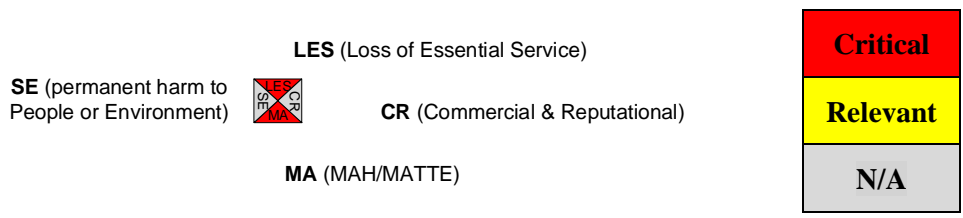
**CHASE Step 3: Simple Risk Assessment**

Conventional risk assessments consider both the severity of the consequences and the likelihood or frequency that those consequences will occur. OG-0086 and other standards and guidance recognise that it is extremely difficult to predict with any certainty the likelihood of an attack.



**Figure 6: IACS Zone Importance, and Consequence**

OG-0086 guidance distinguishes between relevant and critical IACS zones. Relevant zones contain IACS assets that indirectly perform functions supporting the process zones for which relevant consequences have been defined. Critical zones contain IACS assets which directly perform functions supporting the process zones for which relevant consequences have been defined.



**Figure 7: IACS Asset Importance**

IACS zones which are critical or relevant to MA and LES can be identified. This is a key point as assessing every IACS zone and asset on a site for every consequence would be an onerous task with diminishing benefits. However it may be beneficial to include other undesired consequences such as non-COMAH SE or CR.

The risk is then ranked based on zone, consequence and importance. The greatest risk is associated with IACS zones which have critical IACS assets and high consequence.

Risk ranking the IACS zones may require some iteration, particularly if the zone sub-division is not deemed to be appropriate.

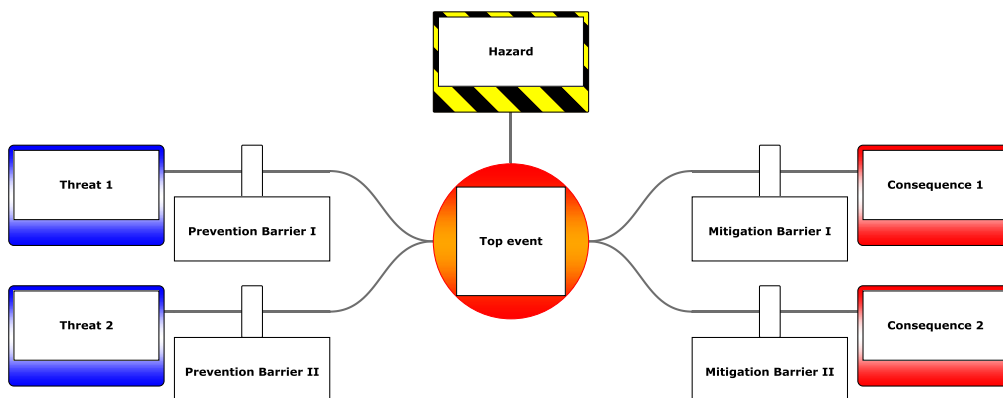
A more appropriate approach (not detailed in this paper) would be to align with the concept of Security Levels (SL) which are ranked 1 (lowest) to 4 (highest) which are similar to but very distinct from the Safety Integrity Levels (SIL) of Functional Safety. It is recognised that any approach needs to be properly calibrated to match the corporate risk tolerability criteria.

**CHASE Step 4: Defining countermeasures**

On conclusion of the assessment phase, the lifecycle progresses to defining and implementing countermeasure. OG-0086 provides an interpretation of the basic level of countermeasures which should be deployed to address anticipated threat types. Not every countermeasure is appropriate to every threat type and it is acknowledged that threats are difficult to predict and describe and therefore a generic approach is required.

Each threat type has one or more appropriate countermeasures intended to protect against or detect cyber security attacks and the relationship between the threats and the countermeasures is visualised in a bowtie diagram.

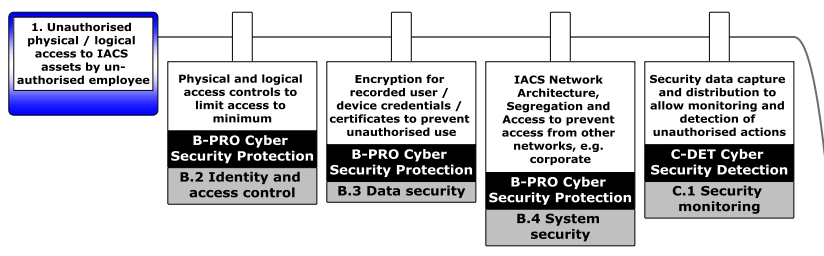
The basic elements of bowties are summarised in **Figure 8 below:**



**Figure 8: Basic bowtie**

The principles of bowties are explained in the Center for Chemical Process Safety (CCPS) and the Energy Institute (EI) “Bow Ties in Risk Management: A Concept Book for Process Safety”.

The threats are adversarial attacks (although accidental, structural and environmental causes may still exist) and the barriers are the IACS countermeasures. A bowtie model of the scenarios using the 11 generic threats from OG-0086 can be built. For example, generic threat 1 and the generic countermeasures from Appendix 5 of OG-0086 results in **Figure 9 below:**



**Figure 9: OG-0086 Table 5.1 bowtie detail**

This graphical representation is then used as a visual check list to determine which countermeasures (barriers) are present and how well they are implemented, and where countermeasures need to be added or strengthened to achieve the minimum expected protection.

Based on current levels of engagement between the HSE and duty holders, achieving this level of verification is the first step in demonstrating that cyber security risks are sufficiently well understood and that basic countermeasures are implemented and managed.

**CHASE Step 5: Detailed risk assessment**

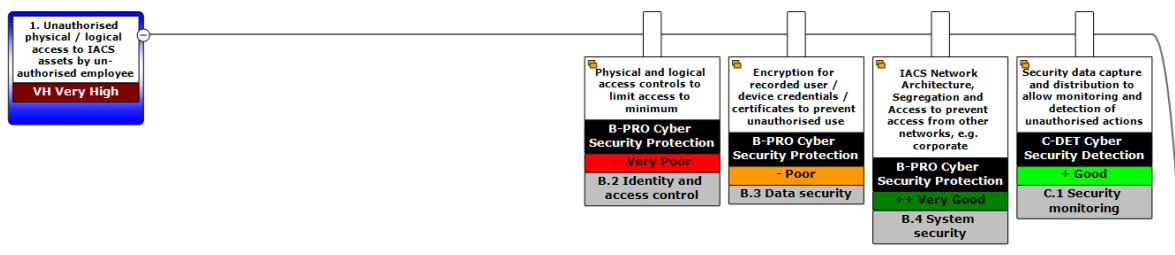
As the levels of cyber security awareness grow, it is to be expected that more detailed analysis will be required (and expected) in order to progress from generic assessment by type to consideration of specific threats, hazards and countermeasures.

The bowtie model provides a framework for the addition of more detail as the analysis progresses. Better intelligence and wider experience will provide increasing levels of confidence on likely adversaries and their potential and propensity to attack.

Using the zone and conduit model, potential breaches can be visualised in a bowtie and the associated threats (including non-adversarial threats) can be qualified according to their anticipated likelihood which are balanced by countermeasures (or bowtie barriers). The risk of an individual zone being breached (with the subsequent potential for harm to or caused by physical assets) may be determined by the following factors:

- the number of threats and their likelihood
- the number of barriers and their effectiveness
- the number of consequences and their severity

An example of a quantified threat line in a bowtie diagram is shown in **Figure 10** below:



**Figure 10: Qualified risk assessment extract**

The NIST Special Publication 800-30 “Guide for Conducting Risk Assessments” offers a method for qualifying risk based on the characteristics of the attacker (capability and intent) and the target (relevance and attractiveness) and the potential level of impact that may result from an attack. It also offers a method for qualifying non-adversarial risks. Quantitative evaluation of risk is theoretically possible but is not representative because attack frequencies are difficult to predict.

The impact on the physical assets should either already exist in a Process Hazard Analysis (PHA or HAZOP) or in bowtie format. If the bowtie already exists, then the diagram is simply modified to introduce a threat which is the loss of IACS (or relevant IACS component) integrity (i.e. a cyber attack). If the safety analysis for the asset is not in bowtie format, then it is created from scratch or transcribed from the PHA as follows:

HAZOP	Bowtie
Causes	Threats
Consequences	Consequences
Safeguards associated with the Cause	Prevention Barriers
Safeguards associated with the Consequence	Mitigation Barriers

At a high level, the physical asset bowtie can be condensed into an overview which considers the five barrier types described within the CCPS/EI Bowtie Concept Book as shown below in **Figure 11**:

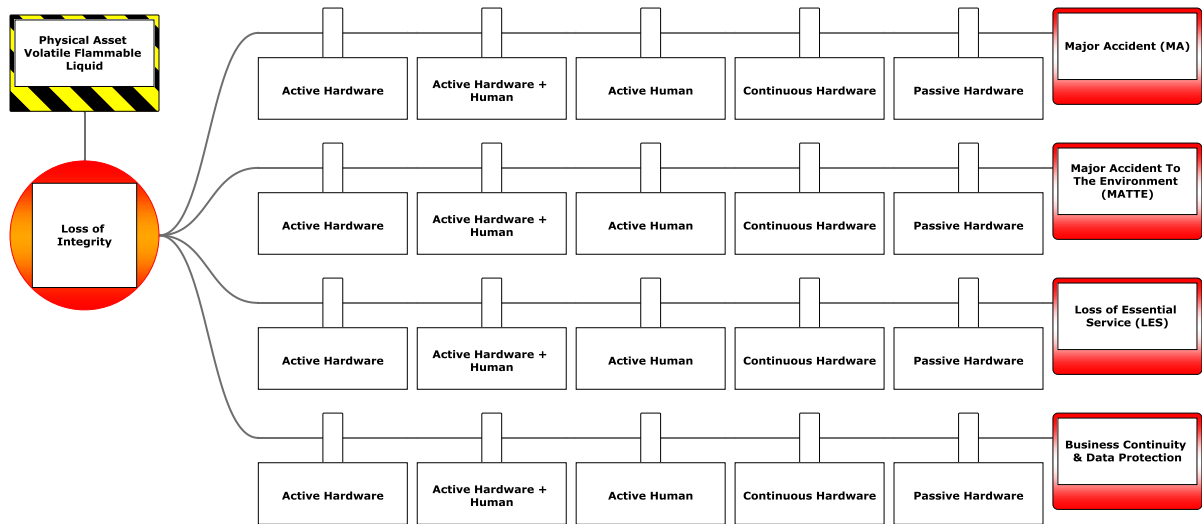


Figure 11: Physical asset overview bowtie

The following barriers types are considered:

- Active Hardware (e.g. BPCS, SIF, Relief devices etc)
- Active Hardware and Human (e.g. alarms)
- Active Human (e.g. competence and vigilance)
- Continuous Hardware (e.g. ventilation)
- Passive Hardware (e.g. bunds etc)

The IACS bowtie (with the CAF barriers on the threat or prevention side) can then be connected to the physical asset bowtie (with the CCPS/EI barriers on the consequence or mitigation side) as shown below in Figure 12:

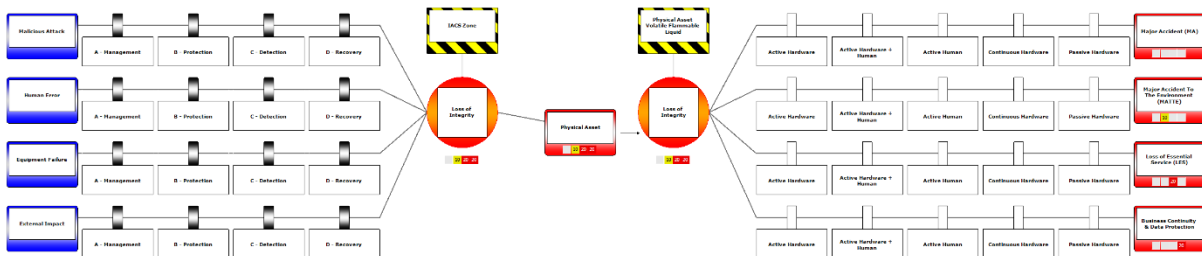


Figure 12: Connected IACS and physical asset bowties

This provides end-to-end visibility of the potential path from adversarial attack or non-adversarial compromise that could lead to loss of service or containment on the plant and indicates the barriers (or types of barriers) that prevent or slow that escalation. It is these barriers that require further scrutiny to determine their presence (do they exist?) and performance (do they have the necessary capability and reliability to meet the risk target?).

Breaking down complex logical and physical systems into sub-systems represented by interconnected diagrams provides a more manageable approach and a more understandable presentation.

Returning to the Buncefield example, a diagram of all threat types considered for an individual zone e.g. Zone 5 (Plant A BPCS) would look like Figure 13:



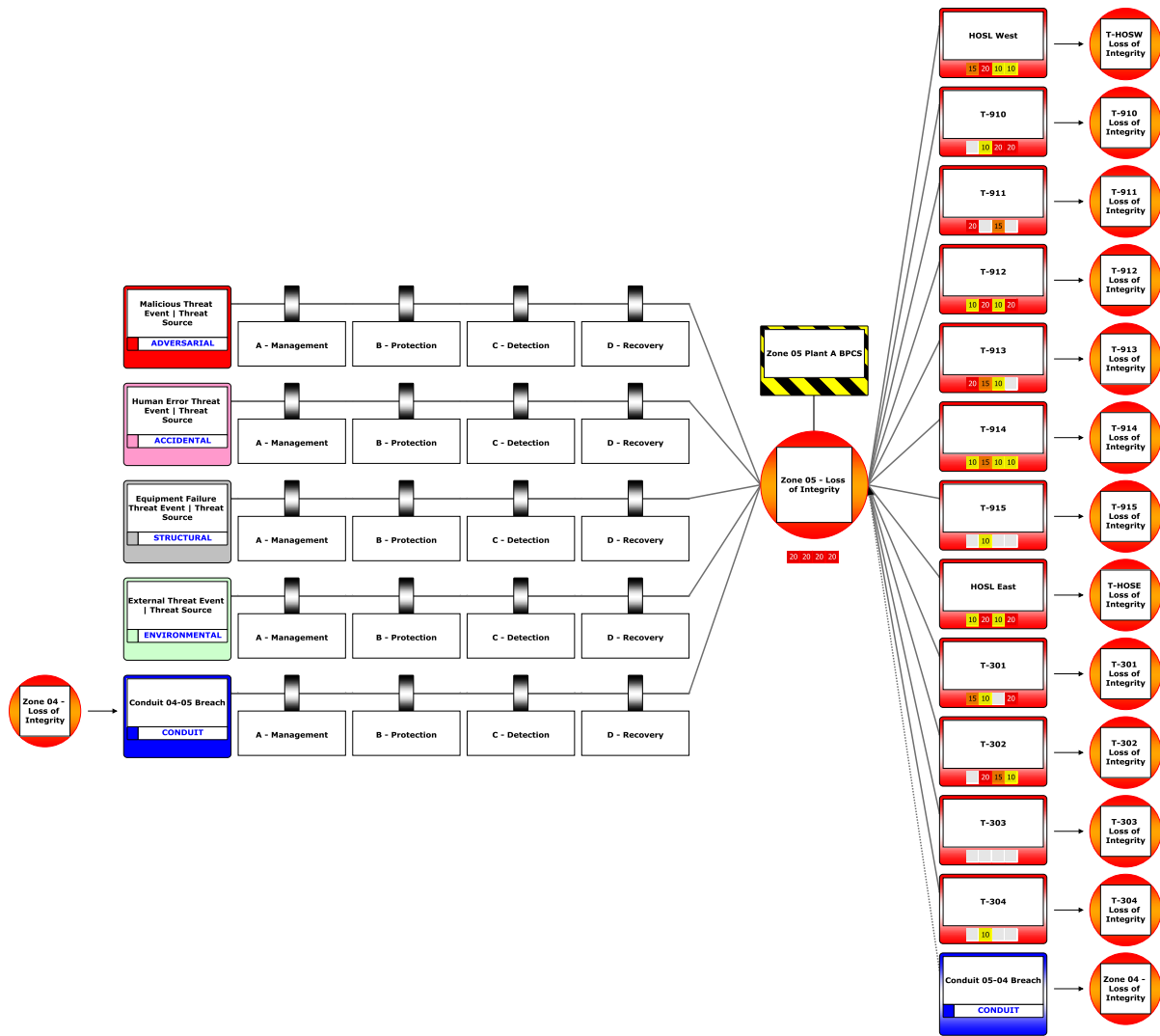


Figure 13: Developed IACS zone bowtie

This shows the internal or direct threats within the zone and the connected or indirect threat from other zones (via conduits e.g. from Zone 4). It also shows the consequences resulting from a zone breach or compromise on subordinate assets (tanks) and connected zones (again via conduits e.g. to Zone 4).

One of the connected assets e.g. Tank 912 would look like Figure 14 below:

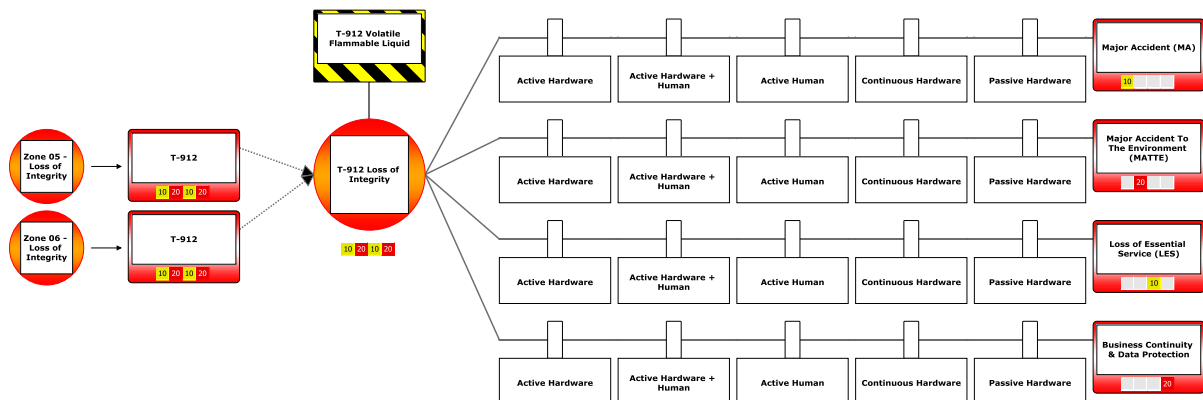


Figure 14: Developed physical asset bowtie

Here, Tank 912 is potentially vulnerable to cyber attack (or non-adversarial compromise) via either Zone 5 or Zone 6 because it is both controlled by the Plant A BPCS and protected by the Plant A SIS respectively.

The scale and complexity of the relationships between the IACS zones and the physical assets can (like the IACS network diagram or the Buncefield tank topology) be summarised in a simple but effective relationship model as shown in **Figure 15** below. This highlights that unauthorised entry into or within a single zone can result in unrestricted access across the IACS and its subordinate assets:



**Figure 15: Bowtie relationship model**

Although this representation shows the potential paths between IACS zones and physical assets, impact on the process does not necessarily have to occur via the inputs and outputs (I/O) which interface with the plant instruments and equipment. It is possible that, for example, denial of service, deletion or manipulation of critical data can occur within rather than at the interfaces of the IACS. Note that the representation above assumes that conduits are bi-directional as the worst case.

**CHASE =Hazardous Scenario Evaluation**

The management of functional safety has become increasingly (but not completely) mature in the process industries and recognised good practice is documented in the BS EN 61511 series of standards. Within these standards, clause 8.2.4 of 61511 part 1 requires a security risk assessment which the previous sections of this paper aim to address. Part 1 includes a specific section on Safety Requirement Specifications (SRS) and the SIS. Safety requirements are listed in clause 10.3.2 which includes requirements to identify and take account of common cause failures.

Developing the bowtie model into specific hazard scenarios e.g. tank overflow as shown below in **Figure 16** and assigning IACS zones or assets to threats and/or barriers can be used to expose the impact of common cause failures as well as the vulnerabilities to IACS attack or compromise.

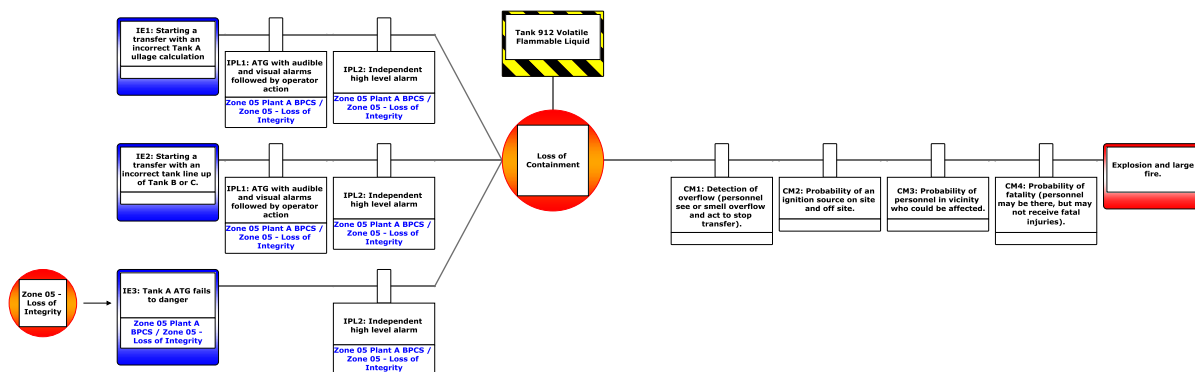


Figure 16: Hazardous Scenario Evaluation

In this example a breach of IACS Zone 5 could create a threat which could result in the top event (Loss of Containment) and if several threats leading to the top event also are vulnerable to the same zone then there is potential for coincidental initiating events. Similarly, if the prevention barriers are all within the control or protection of the same IACS zone (Zone 5 in this example) then loss of integrity of that zone could defeat or degrade some or all the barriers that prevent the top event and so expose the physical asset to potential danger due to common cause failure.

**Conclusion**

Cyber security is a cause of unease for the process industry due to the potential to lose or give away control of critical assets or infrastructure. The Health and Safety Executive in its role as regulator naturally wishes to focus on Major Accidents and the government wishes to focus on Loss of Essential Services. However the moral obligations and financial expectations of companies require consideration of the impact of a compromised (whether adversarial or not) Industrial Automation and Control Systems (IACS) on the environment, business operations and reputation.

The starting point for any risk assessment is to define what needs to be protected (both physical and logical assets) and thereafter to assess where an attack may occur and evaluate the potential consequences. This can be more effectively conducted by using a topological rather than literal representation of assets and IACS zones with their inter-connecting conduits.

An examination of who may attack and how likely any particular attack could be based on the effectiveness of the measures to manage, protect, detect and recover using the recognised good practice of the CAF. Using a bowtie representation of these cyber countermeasures or barriers enables gaps (or indeed duplication) to be identified.

Visualisation of MA and LES scenarios provides a common understanding to assist with decision making and resource deployment as the duty holder is better informed of the criticality of the barriers that need to be implemented and sustained. It allows individual or common vulnerabilities to be exposed and addressed by targeted design and maintenance. It enhances management of change because the context of barriers within the overall protection portfolio is more apparent.

The methods proposed in this paper can be considered equivalent to the early stages of the IChemE series of Hazard Studies which range from 1 to 6 in their conventional format. This equivalence is summarised in **Figure 17** below:

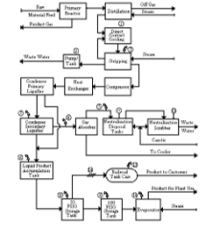
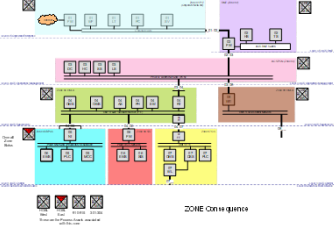
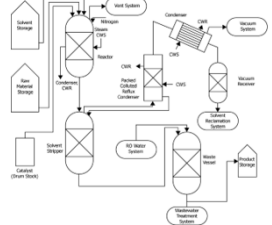
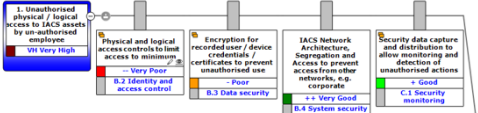
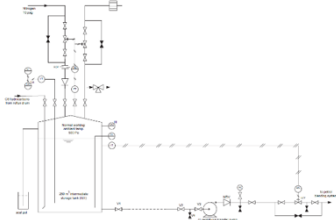
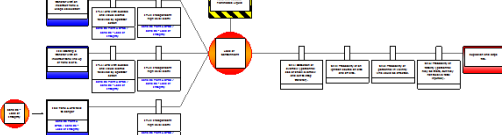
Hazard Studies (IChemE)	Cyber Security (CHASE™)
<p><b>Hazard Study 1</b></p> <p>Concept Block Diagram</p> 	<p><b>High Level Risk</b></p> <p>OG-0086 App 4</p> 
<p><b>Hazard Study 2</b></p> <p>HAZID Process Flow Diagram</p> 	<p><b>Detailed Risk Assessment</b></p> <p>OG-0086 App 5 &amp; NIST &amp; CAF</p> 
<p><b>Hazard Study 3</b></p> <p>HAZOP P&amp;ID</p> 	<p><b>Hazardous Scenario Evaluation</b></p> <p>CCPS/EI</p> 

Figure 17: Comparison between Hazard Studies and Cyber Security studies

Increasing scrutiny is applied as the design or installation becomes progressively more detailed.

**Benefits**

Established bowties can be enhanced by connecting cyber security threats to provide a more holistic view of the potential dangers to assets.

Bowtie visualisation of barrier-based risk management makes the physical and logical risks more understandable so that assessments can be carried out more efficiently and effectively and the outcomes and any remedial measures can be better appreciated and supported by all stakeholders – not just IT or process safety specialists.

**References**

Center for Chemical Process Safety, *Bow ties in risk management. A Concept book for process safety.* (Hoboken, NJ.: Wiley, 2018).

*Control of Major Accident Hazard Regulations 2015.* (COMAH) Statutory Instruments 2015 No. 483. [\[legislation.gov.uk/ukxi/2015/483/contents/made\]](http://legislation.gov.uk/ukxi/2015/483/contents/made)

Crawley, F. and Tyler, B., *HAZOP: Guide to Best Practice.* (Amsterdam: Elsevier, 2015). 3rd edition.

*Functional Safety. Safety instrumented systems for the process industry sector.* BS EN 61511, Parts 1 to 3, 2nd edition, 2017.

Health and Safety Executive, *Cyber Security for Industrial Automation and Control Systems (IACS).* 2nd edition. [\[www.hse.gov.uk/foi/internalops/og/og-0086.pdf\]](http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf)

*Industrial Communication Networks - Network and system security. Parts 1 to 4,* IEC 62443 2009-18.

*Network and Information Systems Regulations 2018.* (NIS) Statutory Instruments 2018 No.506. [\[www.legislation.gov.uk/ukxi/2018/506/made\]](http://www.legislation.gov.uk/ukxi/2018/506/made)