Bowtie method and Industrial Internet of Things

Glenn Moffett
gmoffett@our.ecu.edu.au

Abstract

This paper uses the bowtie method as a visual aid for the security risk assessment and treatment of components in the Industrial Internet of Things (IIoT). Threat modeling and related controls are used to identify threats as input to bowtie creation. Bowtie features are applied using identified and related threats to IIoT devices to create bowtie examples. Multiple bowties are associated to identify the path a cybercriminal could exploit. Based on the use and review of the bowtie method there are benefits to using bowties as a visual risk management tool, however definition, scope, management and integration are considerations for expanded use and shared understanding. Further research areas for the use of bowties in cybersecurity are identified.

Keywords
Industrial Internet of Things, IIoT, Bowtie method, Bow tie, Risk assessment, Risk treatment, Threat modeling, Security, Cybersecurity

Note
Thank you to CGERISK for providing a free trial version of the BowTieXP software for use with this paper.

INTRODUCTION

Industrial Internet of Things (IIoT) in general is not a new or novel concept to industrial businesses that include energy, mining and manufacturing (Thiagarajan, 2016). Sensors, actuators, machine to machine communication, data collection, analysis and visualization have comprised Industrial Control Systems (ICS) for decades. Aspects that are new – or newer – include additional mobile device types, improved analytics and the ability to install components that communicate directly with services off premise – i.e.: cloud – or bypass traditional data paths. These services include data storage, data sharing, analytics and visualization. Business requirements are driving the adoption of new IIoT technologies that improve efficiency, reduce downtime and aid in energy management programs. Additionally, these solutions can be implemented for a fraction of the cost of traditional ICS systems and have the potential to provide competitive advantage (de Ruijter & Guldenmund, 2016).

With these new features comes responsibility and the introduction of additional risk. A 2014 report indicates that 37% of energy companies in the USA were compromised (Pagliery, 2014). While it is unlikely that all of these were related to IIoT there are examples where control systems connected to the internet have been compromised (Glenn, Sterbentz, & Wright, 2016). Reviewing data from that year using a quantitative risk calculation indicates a 90% confidence level of an energy company being successfully attacked between 36% and 44%.

The security practitioner has several tools at their disposal to manage cybersecurity risk. This paper will use the bowtie method to visualize aspects of the risk assessment and treatment process for IIoT scenarios. Firstly, the IIoT system to be modelled will be identified. Then a risk identification approach is applied to identify a subset of risks using threat modeling. Next, bowties and related features are applied to selected IIoT scenarios. Bowties are reviewed based on the efficacy to support the analysis and treatment risk management functions. The bowtie method is a valuable tool to visualise and support the identification, analysis, evaluation and treatment of risks. The bowtie does not replace these risk steps, instead enhancing and enabling communication and discussion on the complex topic of security risk. Bowties used with governance and appropriate context have the potential to improve an organizations security posture.

INDUSTRIAL INTERNET OF THINGS (IIOT)

An IIoT solution can comprise several components, interactions and objectives. Industrial use cases may have different security objectives compared to a traditional IT environment. The CIA triad of confidentiality, integrity and availability can be upended in an industrial setting whereby integrity and availability can be more important than confidentiality (Plósz et al., 2014). For example, it can be more important for a Control System Engineer to have access to the data, than for it to be protected. From a systems theory approach the components of an IIoT system can include hardware, sensors, actuators, software, data and information, connectivity, people, processes and the environment (Thiagarajan, 2016).

Connectivity enables interactions between components introducing additional risks. Types of data flows are shown in Figure 1 highlighting the component and type of data as identified by the Industrial Internet Consortium. Management flows enable updating of software and device configuration. The information domain is the flow of data and information that provides visibility to the industrial process monitored by sensors. Control flows initiated by the application enable actuators, SCADA, DCS systems to receive configuration changes for visualization purposes or to modify process operations.

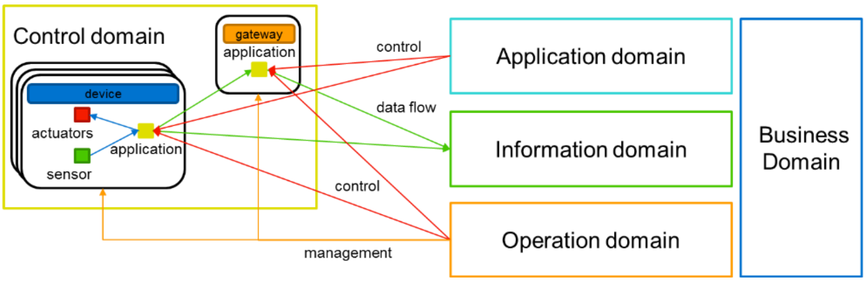


Figure 1 - Functional domains, flows to/from control domain based on Industrial Internet Reference Architecture. (Industrial Internet Consortium, 2017).

For the purposes of this paper the following scenario is used to research stolen credentials, unauthorized access and compromised data flow events as bowties:

> IIoT device connected to industrial equipment (for example mobile compressor) to provide telemetry for a service provider to monitor and manage asset(s).

BOWTIE OVERVIEW

The bowtie method traditionally has been used in the process of risk management to aid in the assessment and treatment process. Possibly the first reference to bowties is from a Queensland Australia university course in 1979. Shell in the early nineties integrated the method so that, “fit for purpose risk controls were consistently in place” (Lewis & Smith, 2010) across the global organization. While the initial focus was in Oil and Gas for safety, the methodology is applicable to and is being used in other industries and domains including cyber security ("The History of the Bowtie," n.d.).

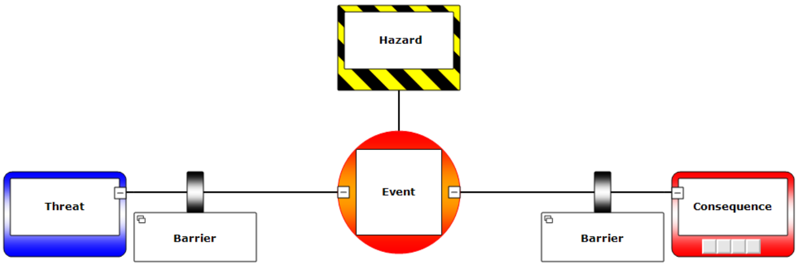


Figure 2 - Bowtie template format

The objective of the bowtie method is to manage hazards. Each hazard can have one or more events and these two items – a hazard event pair – make up the centre of the bowtie (Figure 2). One or more threats and consequences are then listed on the left and right respectively. Between threats and the event, and consequences and the event are one or more barriers. The bowtie method is not unique in the management of safety hazards. Two other methods, fault tree and event tree analysis methods are loosely represented by the left and right side of the bowtie respectively. These tree methods along with cause consequence diagrams and barrier thinking predate bowties (de Ruijter & Guldenmund, 2016). Each of the bowtie components are described in Table 1.

Bowtie Concept	Description	Example
Hazard	Danger aspect	IIoT Device
(Top) Event	Lose control over the hazard that could cause harm	Unauthorized access
Threats	What could cause the event	Default credentials
Consequences	What could occur due to the event	Malware installed
Barrier	What could stop or prevent an event	Prevent a threat: Change default credentials
	What could recover or mitigate an event	Recover from a consequence: Restore software image
Escalation Factors	What could reduce or eliminate the effectiveness of a barrier	Failure to change credentials
Recovery Barriers	What could prevent the escalation factor	Generate unique credentials during installation

Table 1 - Bowtie concepts

To utilize the bowtie method hazard and event pairs need to be identified. Hazards relate to the components of the system being assessed, including for example, an IIoT device. Examples of devices include a gateway that connects to a number of devices or a device that incorporates or is connected to sensors and/or actuators. Events are a loss of control of the hazard that cause an interruption or negative consequence for the organization (Lewis & Hurst, 2005). For example, if an IIoT device – the hazard – collecting emissions data is unable to collect that data – an event – due to a denial of service attack – the threat – the organization may incur financial penalties – the consequence. Events relating to a hazard can be identified using several methods with the objective to identify relevant events based on the defined system. One method to identify events is threat modeling.

THREAT MODELING TO BOWTIE

Threat modeling used as part of a security development lifecycle is one method for risk identification of software threats. Microsoft Thread Modeling software can visually represent software objects, interactions, boundaries and provide a report and threat list. The list of potential threats are associated with a software component and categorised using the STRIDE model (Table 2). The threat, software component and categorization can be mapped to bowtie threats, hazards and threat properties respectively.

Using a combination of an IIoT system and scenario described earlier an exercise was undertaken to create a threat model that resulted in 195 identified threats (Figure 3). The threat model is not intended to be exhaustive, providing instead a representation of threats and consequently has not fully assessed or peer reviewed. The resultant threat list was then copied to Microsoft Excel and modified prior to importing into the BowTieXP application scrap book. Threats from the scrap book could then be dragged onto hazard diagrams to build out a bowtie. Context information was also imported so that each threat included a description and threat type (STRIDE category). BowTieXP was used to create bowties from the threat list and other identified threats for use in this paper.

Category	Description	Example
Spoofing	Masquerade as trusted resource	Rogue access point Compromised device
Denial of Service	Impact availability and/or performance	Data collection from sensor to cloud is interrupted
Repudiation	Deny performing an action	Rogue device writes to data store

Information disclosure	Unauthorized access to data	Data store with incorrect authentication
Tampering	Unauthorized modification of data	Configuration changes
Escalation of privileges	Obtain administrative control a system(s)	Web server vulnerability enables privilege access

Table 2 – STRIDE threat categories and examples for IIoT scenarios (Scandariato, Wuyts, & Joosen, 2015).

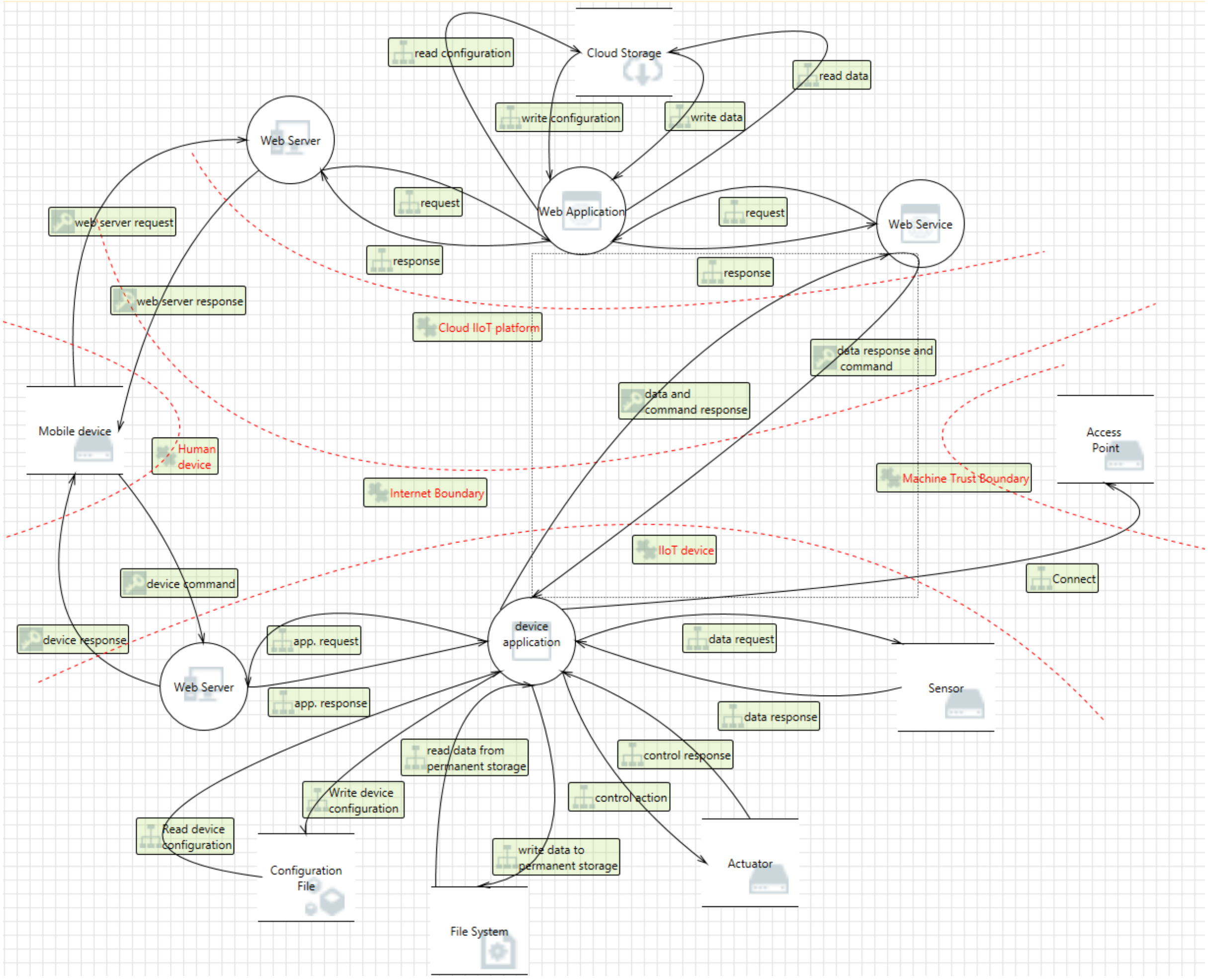


Figure 3 – Exploratory threat model for components of an IIoT solution (195 threats identified)

An approach was required to select a subset of threats to model as bowties for this paper. With the previously identified requirement of integrity and availability identified from the CIA model, two areas of focus were identified, the IIoT device and the IIoT application. The application scenario being suitable to bowtie based on the software threat model. The next step involved defining sample hazard event pairs to start the bowtie creation process (Table 3) prior to gaining an understanding of the bowtie features.

Hazard	**Top Event**	**Description**
IIoT device	Un-authorized access	High level generic security event
IIoT device	Stolen credentials	Specific event
IIoT device	Data flow is compromised	Sensor data is tampered with
Network	Compromised	High level generic security event
Web Server	Compromised	High level generic security event

Application	Compromised	High level generic security event
Sensor	Interfere with data collection	Tamper with sensor
Actuator	Send unauthorized commands	Control actuator

Table 3 - Bowtie hazard/event pair examples

BOWTIE FEATURES

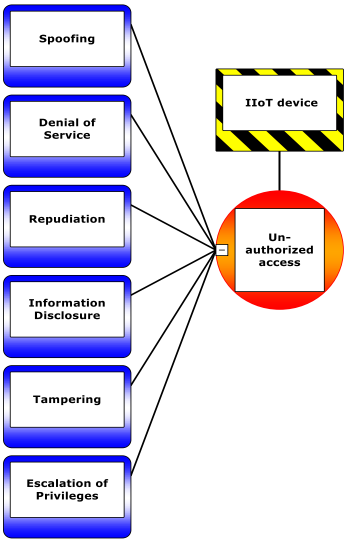


Figure 4 - Threat modeling categories mapped to a bowtie

One possible approach to visualize threat models as a bowtie is by threat categories (Figure 4), however this will complicate the risk process. For example, one type of spoofing is the illegal use of credentials. There are different approaches to preventing illegal credential use depending on the nature of the threat. If the use of default credentials is the threat, then a threat control is to change the default credentials. Confidentiality of data flow between an IIoT device and authenticating client is another control that is relevant to stop a Man In the Middle (MITM) threat that could allow the reuse of identified credentials. Use of threat categories in this way (Figure 4) conflates different individual threats complicating risk analysis and risk treatment. The policy of requiring default credentials to be changed is potentially a lower effort than requiring confidentiality between devices. The security practitioner may have to decide which threat to treat based on the cost and benefit. If both of these controls are grouped under the one threat of spoofing, this does not enable the practitioner to make an informed choice. The alternative approach shown in Figure 5 lists each threat individually with control barriers identified for each threat. Barriers are explored in the next section.

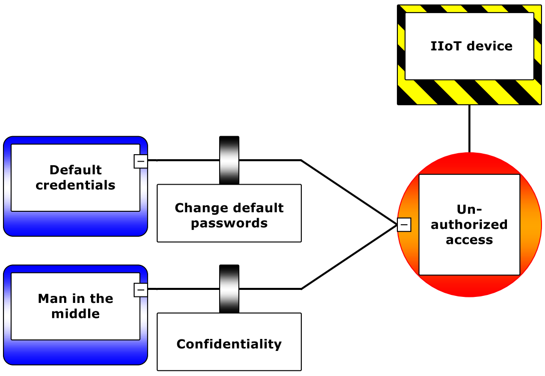


Figure 5 - Individual threat mapped to an event

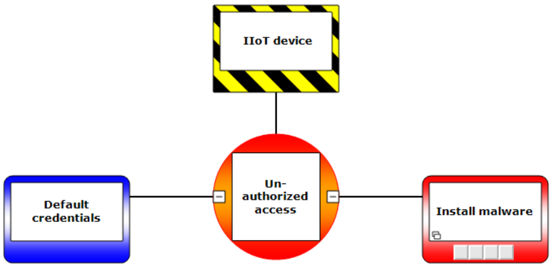


Figure 6 - Bowtie example

The bowtie in Figure 6 visually describes the spoofing event *unauthorized access* identified as part of the threat modeling exercise. The bowtie can be described as the unauthorized access – the event – to an IIoT device – the hazard – which could be exploited by the use of default credentials – the threat – and consequently enable the installation of malware – the consequence.

Barriers

The next step in the development of the bowtie is to identify barriers that control and prevent or mitigate and recover from an event (CGERisk, 2015; de Ruijter & Guldenmund, 2016). A barrier is consistent with a control in risk management terminology that aims to modify the risk (ISO/IEC, 2011). While the term barrier may be associated with blocking, no barrier is necessarily perfect and consequently each barrier should be considered as part of the overall path from threat to consequence. Multiple barriers may be appropriate or required. Barriers can be identified from sources including best practices, threat modeling, subject matter experts and applying standard cybersecurity controls (NIST, 2003; "Top 5 CIS Controls," n.d.). Centre for Internet Security (CIS) control number three refers to secure configuration of which changing default account details is one control to harden the system. Change account details is a barrier to prevent a threat actor accessing the device using the default credentials. Should a threat actor be able to use default credentials, then a mitigation strategy would be to detect malicious activity on the device and act as per policy either through a technical or process action to recover the system. The two barriers are displayed in Figure 7.

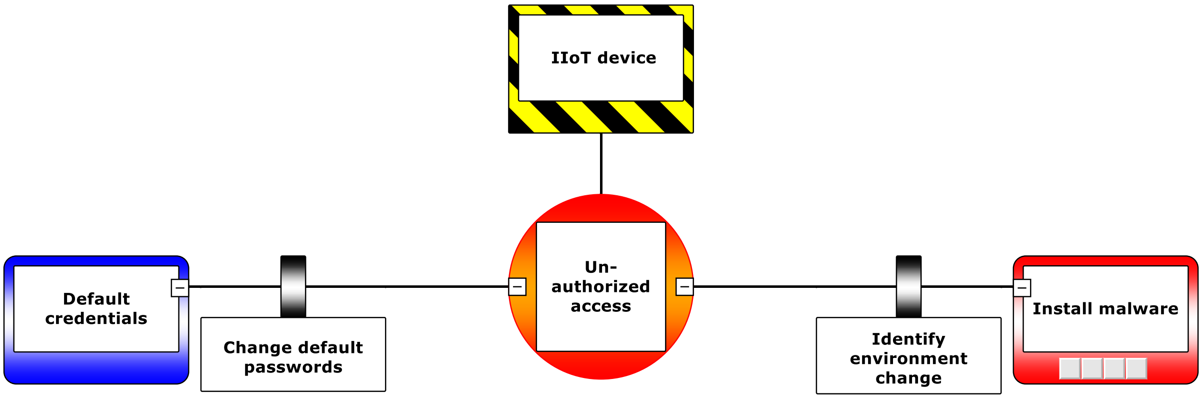


Figure 7 - Bowtie with example barriers

Multiplicities are to be expected for threats, barriers and consequences for a given event. The bowtie method allows for the visualization of these multiplicities to enable the security practitioner to represent these threats and consequences, along with barriers. Figure 8 incorporates additional threats and related barriers. Similarly, consequences and barriers are shown in Figure 9. This visual representation allows the viewer to identify common barriers and the level of protection or recovery that is possible. A challenge could be to represent an event with a high number of threats, consequences and barriers. In this instance a more granular or focused bowtie event could be mapped.

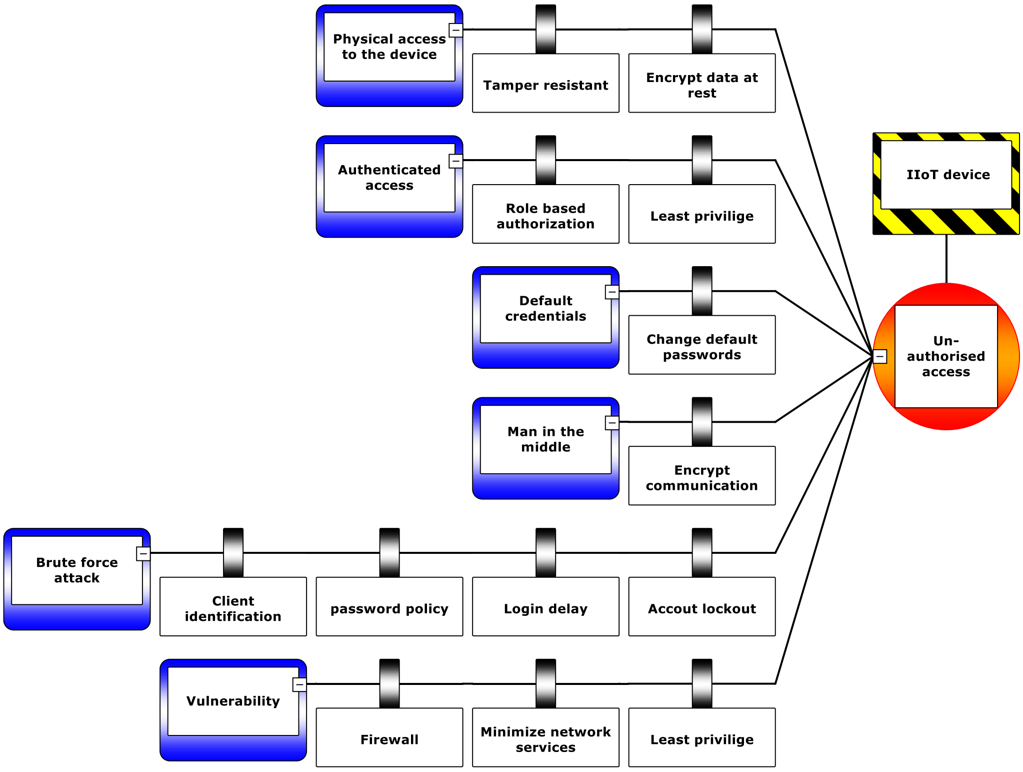


Figure 8 - Threats along with control and preventative barriers for unauthorised access to an IIoT device

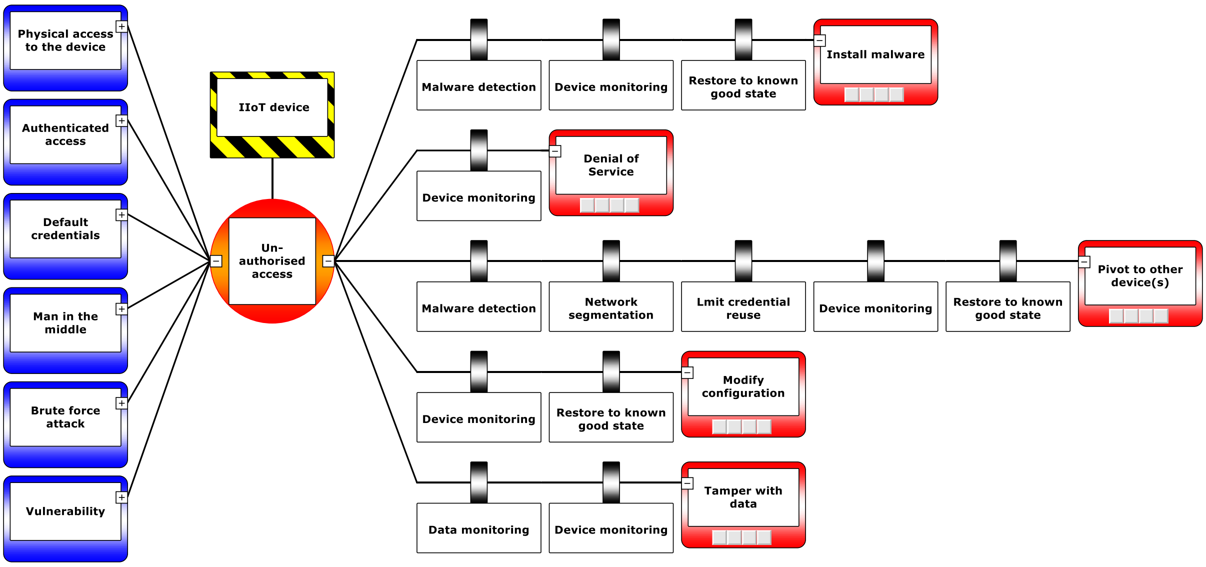


Figure 9 - Mitigation and recovery barriers for consequences due to unauthorised access to an IIoT device

Escalation factor

In addition to the base bowtie defined already, there are several other features to describe the risk environment. Firstly there is the notion of an Escalation Factor which can compromise or reduce the ability of a barrier. Figure 10 incorporates the *Policy not implemented* escalation factor with a prevention barrier. This addresses the scenario where a risk prevention activity – *Change default passwords* – could fail.

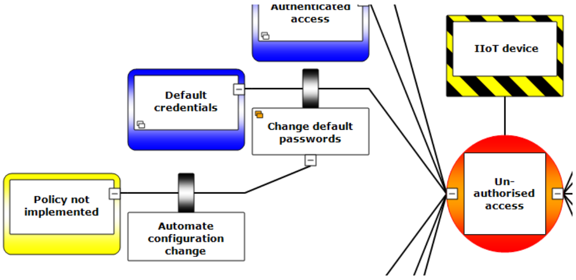


Figure 10 - Escalation factor example

Barrier category

Bowties can support additional annotation to assist in the identification, analysis and treatment of risk. While there can be several barriers for a given threat or consequence, the efficacy of the barrier can impact risk assessment and treatment. Barriers can serve different functions providing additional granularity (**Error! Reference source not found.**) and reduce uncertainty. Defining the category for a barrier may require subject matter expertise, consequently there is a trade-off as to whether the definition of categories is worth the level of effort. One of the benefits of categorized barriers is in the risk treatment process, where with multiple barrier options, their efficacy can be compared. Barrier categories are identified by colour in Figure 11.

BARRIER CATEGORY	DESCRIPTION
ELIMINATE OR CONTROL	Stop the threat
PREVENT	Prevent the event
MITIGATE	Minimize the impact of the consequence
RECOVER	Restore to known good state

Table 4 - Barrier categories

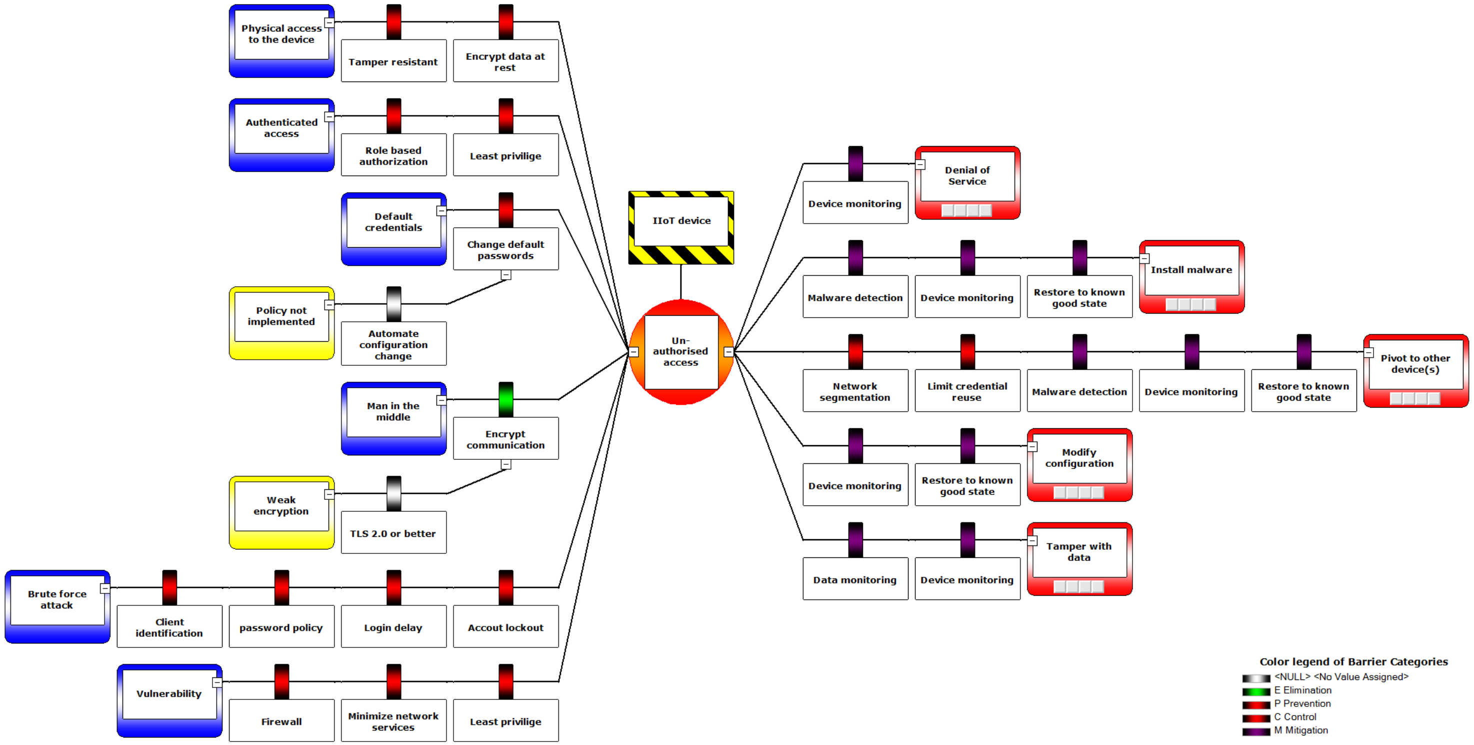
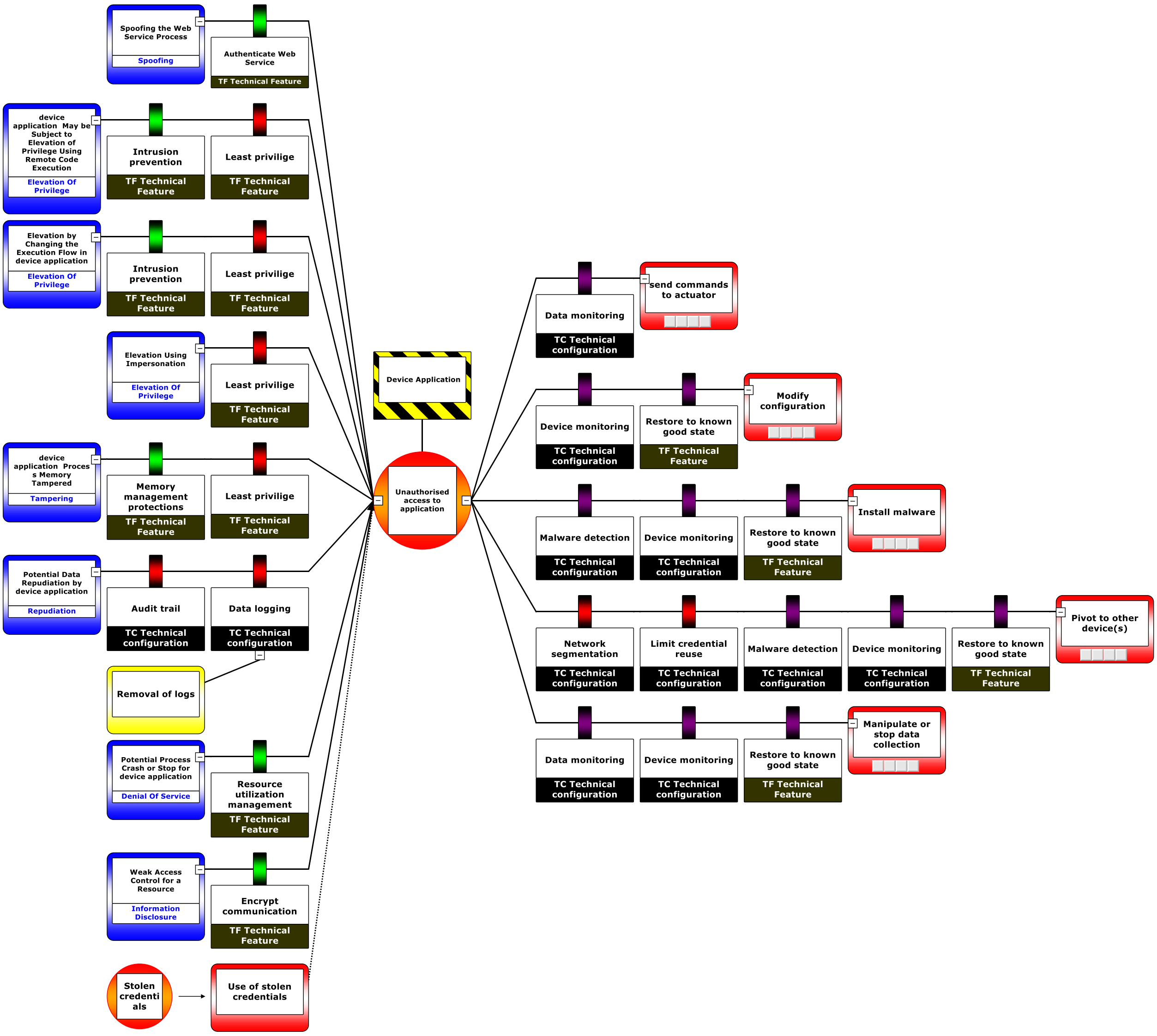


Figure 11 - Barrier function type colour coding
(The shape of this diagram, represents the reason for the name bowtie, due to the similarity to the shape of a type of neck tie, called a bowtie)

Threat property, barrier type and chaining

Figure 12 introduces three other bowtie features, namely properties, barrier type and chaining. STRIDE categories imported as part of the threat list are shown as properties to provide context to the threat. Below each barrier is a barrier type layer. *Technical feature* – inherent in the software – and *Technical configuration* – requires configuration after installation – are user defined barrier types. Barrier type in this context allows the security practitioner to understand what is required to implement and maintain the barrier. In the context of this example a software (technical) feature inherent in the software is preferred over a software (technical) configuration option that must be implemented in addition to the default installation of the application. Additional layers can be defined in BowTieXP for accountability including association with a management system, responsibility and activity assignment (de Ruijter & Guldenmund, 2016).



Spoofing the Web Service Process
Spoofing
Authenticate Web Service
TF Technical Feature
device application May be Subject to Elevation of Privilege Using Remote Code Execution
Elevation Of Privilege
Intrusion prevention
TF Technical Feature
Least privilige
TF Technical Feature
Elevation by Changing the Execution Flow in device application
Elevation Of Privilege
Intrusion prevention
TF Technical Feature
Least privilige
TF Technical Feature
Elevation Using Impersonation
Elevation Of Privilege
Least privilige
TF Technical Feature
device application Proces s Memory Tampered
Tampering
Memory management protections
TF Technical Feature
Least privilige
TF Technical Feature
Potential Data Repudiation by device application
Repudiation
Audit trail
TC Technical configuration
Data logging
TC Technical configuration
Removal of logs
Potential Process Crash or Stop for device application
Denial Of Service
Resource utilization management
TF Technical Feature
Weak Access Control for a Resource
Information Disclosure
Encrypt communication
TF Technical Feature
Stolen credenti als
Use of stolen credentials
Device Application
Unauthorised access to application
Data monitoring
TC Technical configuration
send commands to actuator
Device monitoring
TC Technical configuration
Restore to known good state
TF Technical Feature
Modify configuration
Malware detection
TC Technical configuration
Device monitoring
TC Technical configuration
Restore to known good state
TF Technical Feature
Install malware
Network segmentation
TC Technical configuration
Limit credential reuse
TC Technical configuration
Malware detection
TC Technical configuration
Device monitoring
TC Technical configuration
Restore to known good state
TF Technical Feature
Pivot to other device(s)
Data monitoring
TC Technical configuration
Device monitoring
TC Technical configuration
Restore to known good state
TF Technical Feature
Manipulate or stop data collection

Figure 12 - Threat list items as a bowtie with barrier type.

The third feature chaining, enables the security practitioner to associate and navigate between events. In Figure 12 (lower left) the *Stolen Credentials* event (Figure 14) is linked to the *Unauthorised Access to Application* event by the *Use of Stolen Credentials* consequence. Figure 13 highlights the chaining feature, where four bowties are chained together by a consequence of the hazard/event pair from initial threat to business impact of the failed equipment. One benefit of chaining is to navigate and consequently explore the paths through which a cybercriminal could potentially compromise a system. With a base understanding of the features of bowtie, the next step is apply a bowtie to risk management activities.

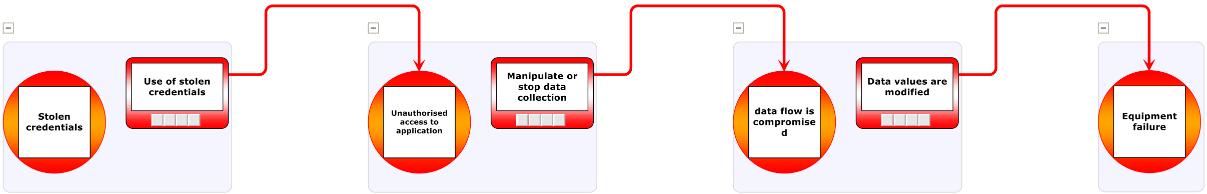

Stolen credentials
Use of stolen credentials
Unauthorised access to application
Manipulate or stop data collection
data flow is compromise d
Data values are modified
Equipment failure

Figure 13 - Hazard/event chaining

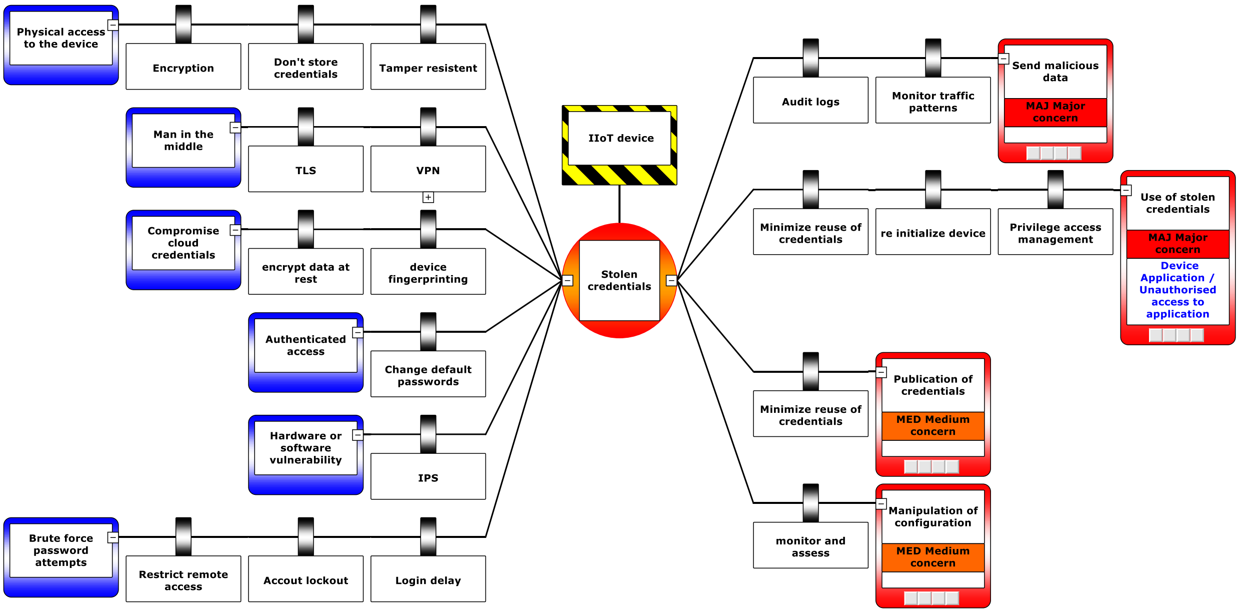
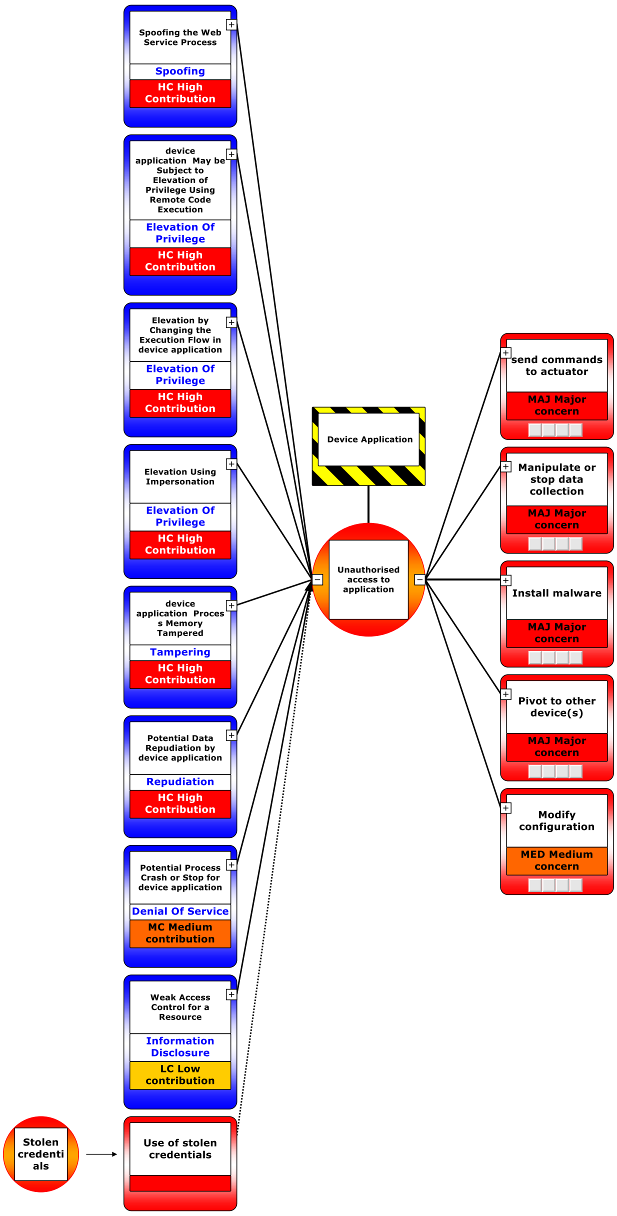


Figure 14 - Stolen credentials bowtie

RISK ANALYSIS AND RISK EVALUATION

How can bowtie diagrams aid risk analysis and evaluation? Level of risk determination as defined in ISO/IEC 27005 specifies incidents, consequences, business impacts and likelihood as inputs (ISO/IEC, 2011). For this scenario likelihood – the chance of something happening – is replaced by threat – potential to cause harm. Thus, for this discussion, likelihood is not evaluated and could impact an overall risk assessment. To determine the level of risk, elements of analysis and evaluation can be incorporated into the bowtie. Firstly, for analysis not all threats are the same and a threat level can either be quantitatively or qualitatively defined. Table 5 identifies a qualitative threat level that uses a theoretical industrial organization's risk criteria. Threats categorized by STRIDE are mapped to the CIA model and assigned a risk level based on the risk criteria. Consequently, threats can be associated with a risk level using the STRIDE category (Figure 15). The *Weak access control for a resource* threat is an information disclosure event that is associated with a *Low Contribution* level as represented in the bowtie diagram.

One other aspect of risk for this scenario is consequence. The BowTieXP application defines by default (customization is available) three consequence categories. A category is qualitatively assigned to each consequence in the bowtie based on real and perceived consequences (Figure 15).



Spoofing the Web Service Process
Spoofing
HC High Contribution
device application May be Subject to Elevation of Privilege Using Remote Code Execution
Elevation Of Privilege
HC High Contribution
Elevation by Changing the Execution Flow in device application
Elevation Of Privilege
HC High Contribution
Elevation Using Impersonation
Elevation Of Privilege
HC High Contribution
device application Proces s Memory Tampered
Tampering
HC High Contribution
Potential Data Repudiation by device application
Repudiation
HC High Contribution
Potential Process Crash or Stop for device application
Denial Of Service
MC Medium contribution
Weak Access Control for a Resource
Information Disclosure
LC Low contribution
Stolen credenti als
Use of stolen credentials
Device Application
Unauthorised access to application
send commands to actuator
MAJ Major concern
Manipulate or stop data collection
MAJ Major concern
Install malware
MAJ Major concern
Pivot to other device(s)
MAJ Major concern
Modify configuration
MED Medium concern

Figure 15 – Threat and consequence levels

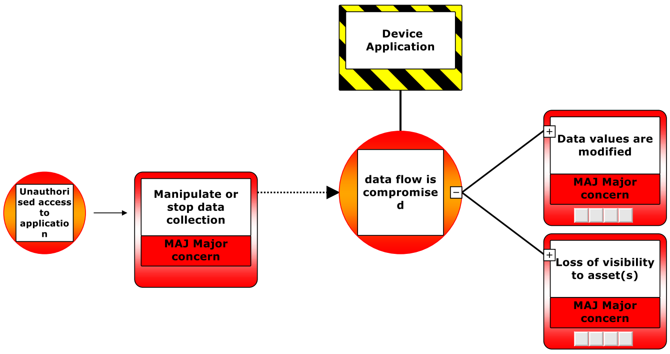
Threat Contribution	Weight	Definition
High (HC)	1	Integrity – Escalation of privilege, Spoofing, Tampering, Repudiation
Medium (MC)	0.75	Availability – Denial of Service, Escalation of Privilege
Low (LC)	0.5	Confidentiality – Information disclosure

Table 5 - Threat level

There are several observations that can be drawn from applying bowtie to risk analysis and evaluation. Firstly, the bowtie provides a visual analysis and evaluation tool for threat and consequence level to identify risk. The diagram clearly indicates how threats relate in terms of criticality, the consequences they relate to and the consequence level as it pertains to the organization. Secondly, there is no list of risks (the combination of threat and consequence) and their associated levels. The assignment of risks and levels would assist with the prioritization and reporting to facilitate risk evaluation. (Note: this capability may be available as part of applications that utilize bowties and was not researched for this paper.) A risk report may be possible by exporting and correlating the bowtie data, however was not incorporated into the research for this paper. Weights defined in Table 5 could facilitate the risk level or prioritization process. In addition, organizational risk criteria can be used as part of the risk evaluation process as shown by the inclusion of CIA model into the prioritization of threat. Finally and to reiterate an earlier point, the risk analysis presented is threat and consequence, instead of likelihood and consequence, where likelihood could be an additional bowtie property or layer highlighting the flexibility of bowties.

RISK TREATMENT

Unacceptable risk identified through the risk assessment process can be analysed to determine relevant risk treatment options to modify the risk level (ISO/IEC, 2011). The CIA model applied to an industrial setting for this scenario positions integrity as a key business objective. Figure 17 lists the consequences of one integrity event where data flow from a device application, which in turn is from a sensor, has been compromised. Two consequences have been identified and due to the relevance of integrity, they are marked as *Major Concern*. Reducing the risk in this scenario is through the implementation of controls, or barriers as defined in the bowtie method.

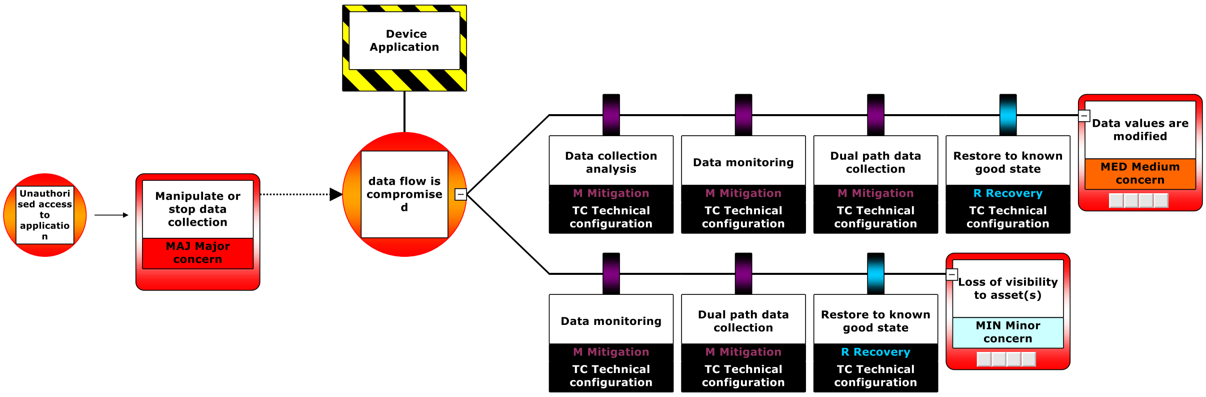


Unauthori sed access to applicatio n
Manipulate or stop data collection
MAJ Major concern
Device Application
data flow is compromise d
Data values are modified
MAJ Major concern
Loss of visibility to asset(s)
MAJ Major concern

Figure 16 - Consequences for an event

Risk treatment options can be identified and compared using bowties. Figure 17 lists a set of barriers for the two potential consequences of the data compromised event. The data analysis barrier is an example of an algorithm or process that evaluates data as it is received from the device. Analysis of data could identify step changes or data behaviour this is not expected or relevant for the device or sensor through machine learning, analysis or calculation methods. For this to be effective, data analysis must occur remote from the device. Remote analysis is required due to the previous chained event indicating the application and device may have been compromised. The data monitoring barrier is the ability to identify changes in data collection, for example a gap in received values that could indicate connectivity issues or be an indication of a security related event.

Implementation of one or more barriers is dependent on the cost and benefit. For the sake of this scenario, the organization has determined that the risk treatment options outlined are required. Consequently, Figure 17 lists these barriers along with updated residual risk values for the consequences reducing them to medium and minor from major. Visual representation of risk enables review of an event including verifying that each consequence incorporates a recovery control as shown in Figure 17.



Device Application
Unauthori sed access to applicatio n
Manipulate or stop data collection
MAJ Major concern
data flow is compromise d
Data collection analysis
M Mitigation
TC Technical configuration
Data monitoring
M Mitigation
TC Technical configuration
Dual path data collection
M Mitigation
TC Technical configuration
Restore to known good state
R Recovery
TC Technical configuration
Data values are modified
MED Medium concern
Data monitoring
M Mitigation
TC Technical configuration
Dual path data collection
M Mitigation
TC Technical configuration
Restore to known good state
R Recovery
TC Technical configuration
Loss of visibility to asset(s)
MIN Minor concern

Figure 17 - Mitigation and recovery barriers for data flow compromised consequences

EVALUATION OF BOWTIE METHOD

"*All models are wrong, some are useful*" (Box, 1976).

To evaluate bowties, a baseline is required that defines bowties and the relevant risk management activities. The bowtie method (also referred to as bowtie model) enables the visual representation of threats and consequences for given events with risk treatment options (CGERisk, 2015). The risk assessment process incorporates identification, analysis – consequence, likelihood and level of risk – and evaluation of risk. Risk treatment is the process used to modify risk (ISO, 2009).

Identification of risk is an optional benefit from the use of bowties. While a key benefit of bowties is visualization, in addition, communication, brainstorming and discussion could facilitate the identification of new risks. During the exercise to create and review sample bowties, barriers identified for one threat were identified to be relevant for other threats. Consequently increased reuse, knowledge sharing and areas for improvement can be realised. Care should be taken not to attempt to make a bowtie represent every scenario, as this level of complexity would detract from the visual benefits of bowties (CGERisk, 2015; de Ruijter & Guldenmund, 2016). Bowties can be created to represent higher level or more detailed level events as required for the audience and connected together as appropriate through chaining.

Flexibility is a key feature of bowtie use that can benefit from governance. There are a number of areas where guidelines could be applied to bowties to enable consistent implementation. Firstly, subjectivity and bias should be minimized through peer review, group discussion and quantitative analysis (CGERisk, 2015). Secondly, there is no inherent consistency in the bowtie method which could complicate validation and verification (de Ruijter & Guldenmund, 2016). Finally, context and terminology are important since there is no defined industry specific standard, for example, to identify hazard and event pairs. Inconsistent risk representations could occur if practitioners mix threats with events making it difficult to connect and understand bowties created by different practitioners. This raises the question as to the complexity, training and required skill level to effectively implement bowties.

Barriers and chaining of bowties can facilitate more in depth risk analysis and treatment. In Figure 18 four events are joined together enabling analysis of a multi layered threat-event-consequence scenario to more realistically reflect the path of a cybercriminal. A similar example was shown in (Figure 13). Representing risk as a bowtie enables the security practitioner to contrast the threats and consequences with risk treatment (barrier) options. Failure analysis of barriers can easily be done with the visual representation of barriers for a threat or consequence. Identification of multiple instances of a specific barrier could impact risk treatment decision making, whereby a commonly used barrier maybe more viable that a lesser used barrier on a lower priority risk. Barriers need to be used carefully and may give a false sense of security. The security practitioner should explain to the bowtie audience that it is possible that one or all of the barriers could fail and whether the barrier is proposed, planned, implemented or under management. Barrier layers and properties are supported in BowTieXP. Barriers can be linked to management systems to provide a chain of responsibility and identify the implementation state.

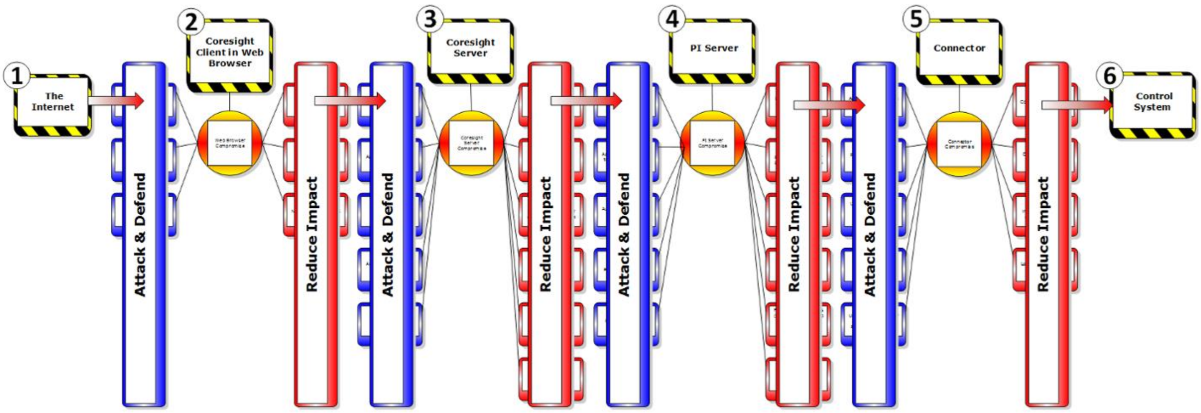


Figure 18 - Bowtie chaining example for OSIsoft application (Paul, 2016)

Qualitative or quantitative risk evaluation is possible using the bowtie method. While not explicitly researched in this paper, literature review identifies several bowtie implementations that utilize each method. Both methods can be applied to barriers, however quantification is not the main goal of the bowtie (CGERisk, 2015). Quantification may be complicated for barriers due to the occurrence of multiple barriers for a single threat or consequence. Additionally, quantification may require combining two or more threats (or consequences) to identify the probability which is not how the bowtie is structured (de Ruijter & Guldenmund, 2016). While the bowtie does not enable the calculation of probability as a native feature, the practitioner is able to see the threat and risk treatment options in one view.

Implementation of the bowtie method to visualise IIoT security risk scenarios enabled several activities. Firstly, the ability to visually represent software threat models associated with events, consequences and potential controls. In addition, the association of individual events through chaining to identify a potential path of a cybercriminal from stolen credentials to equipment failure. Thirdly, by assigning barriers to consequences, visually recalculate and update the consequence risk level. Assigning barrier types enabled auditing to identify relevant controls. Finally, as integrity of data was a key business priority in this scenario, the identification of controls that include tamper proof devices and data analysis to detect malicious manipulation of sensor data.

BOWTIE GUIDELINES FOR CYBER SECURITY RISK

Guidelines were identified based on literature review and the use of the bowtie method for this paper. As for any risk management task, include subject matter experts and stakeholders that can provide context and question aspects of the risk process including for example the analysis of risk. Consider the top event in relation to the audience of the bowtie, for example a top event for a developer may not be relevant for a DevOps administrator or Process Engineer. In general terminology should be defined, understood and followed for a consistent use of categories, types and labels. Context is key so that the audience is aware of the purpose and limitations of the bowtie. Additional recommendations are included in material from CGERisk (2015).

FUTURE RESEARCH

Four areas for further research have been identified. Firstly, how to manage the connection between constituent parts of the system, associated hazards and events to validate that all relevant items are identified and connected. A key question for an organizational implementation is how to integrate with project management solutions that enable governance of the risk treatment decisions, maintain consistency and manage ongoing updates to bowties. This area of research can benefit from existing bowtie implementation in other industries. Thirdly, map features to bowtie attributes including implementation state, responsibility, effectiveness and prioritization. Finally, identify how a quantitative risk management approach could integrate with the bowtie method using approaches from practitioners including Freund and Jones (2014) and Hubbard and Seiersen (2016).

CONCLUSION

The Industrial Internet of Things (IIoT) empowers organizations on a digital transformation journey. Bowties enable the communication of risk through the visual representation of hazards, events, threats, consequences and risk treatment options. In addition, context, threat types, qualitative and quantitative assessment can be incorporated into bowties. Risk assessment and risk treatment activities can utilise bowties as an aid to empower the risk management process. The flexibility of the bowtie is a strength and also an area to be addressed through governance and a shared understanding of how to interpret the bowtie. Risk management processes can benefit from the use of the bowtie. The bowtie method is a tool that can complement a security practitioner’s toolbox, especially for the shared understanding and discussion of risk, including risks to the Industrial Internet of Things.

REFERENCES

Box, G. E. P. (1976). Science and Statistics. *Journal of the American Statistical Association, 71*(356), 791-799. doi:10.1080/01621459.1976.10480949

CGERisk. (2015). *Bowtie Methodology Manual [PDF file]*

de Ruijter, A., & Guldenmund, F. (2016). The bowtie method: A review. *Safety Science, 88*, 211-218. doi:https://doi.org/10.1016/j.ssci.2016.03.001

Freund, J., & Jones, J. (2014). *Measuring and managing information risk: a FAIR approach*: Butterworth-Heinemann.

Glenn, C., Sterbentz, D., & Wright, A. (2016). *Cyber Threat and Vulnerability Analysis of the US Electric Sector*. Retrieved from https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf

The History of the Bowtie. (n.d.). Retrieved from https://www.cgerisk.com/knowledge-base/risk-assessment/the-bowtie-methodology

Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*: John Wiley & Sons.

Industrial Internet Consortium. (2017). Industrial Internet Reference Architecture. Retrieved from http://www.iiconsortium.org/IIRA.htm

ISO. (2009). IEC 31010—Risk Management: Risk Assessment Techniques. *International Organization for Standardization.* Retrieved from http://www.iso.org

ISO/IEC. (2011). Information technology -- Security techniques -- Information Security Risk Management (ISO/IEC 27005:2011). Retrieved from http://www.iso.org/

Lewis, S., & Hurst, S. (2005). Bow Tie An Elegent Solution? Retrieved from http://www.cgerisk.com/images/Knowledge_base/Strategic%20Risk.pdf

Lewis, S., & Smith, K. (2010). *Lessons learned from real world application of the bow-tie method.* Paper presented at the Prepared for Presentation at American Institute of Chemical Engineers-6th Global Congress on Process Safety San Antonio.

NIST. (2003). 800-53. *Recommended Security Controls for Federal Information Systems*, 800-853.

Pagliery, J. (2014). Hackers attacked the U.S. energy grid 79 times this year. Retrieved from http://money.cnn.com/2014/11/18/technology/security/energy-grid-hack/

Paul, H. (2016). Bow Tie for Cyber Security (0x03): Attack Path of Least Resistance? Retrieved from https://pisquare.osisoft.com/groups/security/blog/2016/08/16/bow-tie-for-cyber-security-0x03-attack-path-of-least-resistance

Plósz, S., Farshad, A., Tauber, M., Lesjak, C., Ruprechter, T., & Pereira, N. (2014). *Security vulnerabilities and risks in industrial usage of wireless communication.* Paper presented at the Emerging Technology and Factory Automation (ETFA), 2014 IEEE.

Scandariato, R., Wuyts, K., & Joosen, W. (2015). A descriptive study of Microsoft's threat modeling technique. *Requirements Engineering, 20*(2), 163-180. doi:10.1007/s00766-013-0195-2

Thiagarajan, D. (2016). *Analysis of the current state of Industrial Internet of Things (IIoT) adoption.* Massachusetts Institute of Technology.

Top 5 CIS Controls. (n.d.). Retrieved from https://www.cisecurity.org/critical-controls.cfm