INDUSTRIAL SAFETY AND PROTECTIVE SECURITY: A CHEESE & ONION FLAVOUR

Amplifying the value of collaborative working with likeminded diciplines

1. Introduction

Can an organisation's safety and security practitioners work together to help deliver the business plan objectives or organisational goals? Is there a conflicting mindset between the two tradecrafts and why does safety always appear more important than security? Is there a different mindset, or can the two converge to create an efficient strategy to provide a safe and secure working environment?

This article will explore the recent evolution of both the industrial safety and protective security professions, whilst assessing the merits associated with the safety based *Swiss Cheese Model* and the *Onion Skin Defence-in-Depth* concept. It will conclude by suggesting that an infused *flavour* may enhance the likelihood of business success.

2. The Evolution of Industrial Safety

The recent history of industrial safety evolution has seen significant advancements and changes in practices, regulations, and technologies. Here is a summary of some key developments:

2.1. Shift from Reactive to Proactive Approach. In recent years, there has been a shift in focus from reactive safety measures to proactive safety management. Organisations have recognised the importance of identifying and mitigating hazards before accidents occur, leading to the adoption of risk-based approaches, safety management systems, and proactive safety cultures.

2.2. Emphasis on Human Factors. There has been an increased recognition of the critical role of human factors in industrial safety. Understanding human behaviour, decision-making, and the impact of organisational factors on safety has become a prominent aspect of safety management. Human factors engineering, behaviour-based safety programmes, and training initiatives aim to reduce human errors and improve safety performance.

2.3. Integration of Technology. Technology has played a significant role in advancing industrial safety. The integration of sensors, automation, and data analytics has enabled real-time monitoring of hazards, predictive maintenance, and enhanced risk assessment capabilities. Internet of Things (IoT) devices, wearables, and digital platforms have facilitated improved communication, reporting, and analysis of safety data.

2.4. Regulatory Frameworks. Governments and regulatory bodies have strengthened industrial safety regulations and standards to ensure a higher level of safety in various industries. Compliance requirements and enforcement measures have been implemented to reduce accidents, protect workers, and minimise environmental risks. International standards, such as ISO 45001 for occupational health and safety management systems, have gained traction.

2.5. Safety Culture and Leadership. Organisations have recognised the importance of fostering a strong safety culture and leadership commitment to achieve sustainable

safety performance. Safety leadership training, employee engagement programmes, and safety recognition initiatives have become integral parts of safety management systems. Safety culture assessments and audits help identify areas for improvement.

2.6. Focus on Process Safety. Process safety management has received increased attention in recent years, particularly in high-hazard industries such as oil and gas, civilian nuclear power, chemicals, and manufacturing. Process safety standards, risk assessment methodologies, and safety critical elements have been developed to prevent catastrophic incidents and ensure the safe operation of complex processes.

2.7. Psychological Well-being. Mental health and psychological well-being have gained recognition as crucial aspects of industrial safety. Addressing stress, fatigue, and psychological risks in the workplace is now considered vital for maintaining a safe and healthy workforce. Companies have started implementing employee assistance programmes, stress management initiatives, and policies to support mental well-being.

These are some of the notable trends and developments in the recent history of industrial safety evolution. The focus on proactive approaches, human factors, technology integration, regulatory frameworks, safety culture, process safety, and psychological well-being reflects the ongoing efforts to continually improve safety practices and protect workers in industrial environments.

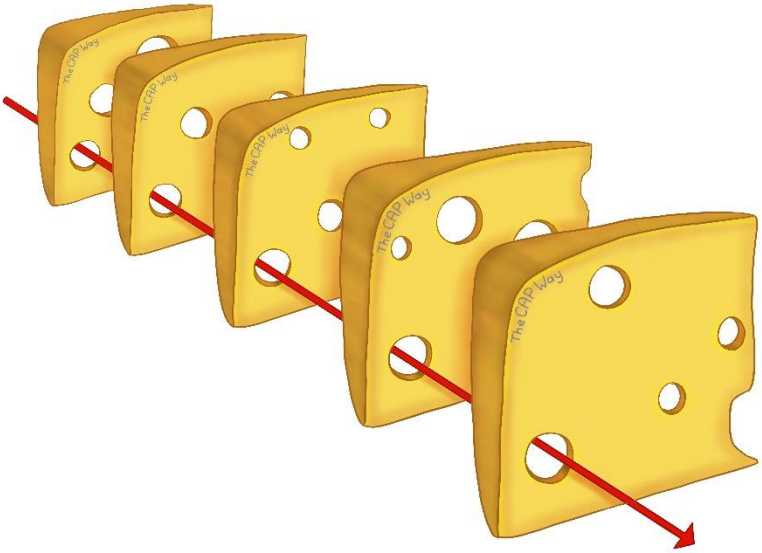
3. An Industrial Safety Mindset: The Swiss Cheese Model

The *Swiss Cheese Model*, also known as the "cumulative act effect" model, is a widely recognised conceptual framework used in the field of industrial safety. It was originally developed by James Reason, a prominent psychologist and expert in human error. The model provides a visual representation of how accidents or incidents occur in complex systems, emphasising the role of multiple latent and active failures.

The model is called the *Swiss Cheese Model* because it likens the layers of defence within a system to slices of cheese, where each slice represents a barrier or safeguard against accidents. In a well-functioning system, these layers align and create a robust defence, akin to a solid block of cheese without any holes. However, when an accident occurs, it is often due to the alignment of various failures or "holes" in these layers.

The *Swiss Cheese Model* consists of the following key components:

3.1. System Defences. These are the various layers of protection designed to prevent accidents. They can include safety policies, procedures, regulations, training programmes, safety equipment, and physical barriers.



3.2. Latent Failures. Latent failures are typically long-term and organisational in nature. They are often hidden within the system and can accumulate over time, potentially leading to accidents. Examples of latent failures include inadequate maintenance procedures, flawed designs, poor communication, or insufficient training.

3.3. Active Failures. Active failures are immediate or short-term failures that occur at the operational level. They are often triggered by human error, violations, or other unsafe actions. Active failures can include mistakes, lapses in concentration, rule violations, or poor decision-making.

3.4. Error Pathways. Error pathways represent the potential paths that an active failure can take to breach the system's defences and lead to an accident. These pathways arise when the layers of defence are misaligned or have weaknesses that allow errors to propagate through the system.

The *Swiss Cheese Model* suggests that accidents occur when multiple failures align or "line up" across various layers of defence, creating a clear pathway for an error to cause harm. The model highlights the importance of addressing both latent and active failures, as well as identifying and strengthening the system's defences to prevent accidents.

By understanding the *Swiss Cheese Model*, industrial safety professionals can analyse and improve safety systems by identifying weaknesses, enhancing training and communication, implementing effective safety measures, and reducing the likelihood of failures aligning to cause accidents.

4. The Evolution of Protective Security

In much the same way as the industrial safety journey, the recent history of protective security evolution has been shaped by various factors, including emerging threats, advancements in technology, and evolving security strategies. Here is a summary of some key developments:

4.1. Rise of Cybersecurity. With the increasing reliance on digital systems and the increased motivation and capability of cyber threat actors, cybersecurity has become a significant aspect of protective security. The evolution of cyber risks, such as

hacking, data breaches, and ransomware attacks, has led to the development of specialised cybersecurity measures, including firewalls, intrusion detection systems, encryption, and employee awareness training.

4.2. Enhanced Physical Security Measures. The evolution of physical security measures has focused on improving *deterrence*, *detection*, and *response* capabilities. Advanced surveillance systems, access control technologies, biometrics, and security screening technologies have become more sophisticated. Integration with digital systems and analytics has allowed for better adversarial threat detection and management.

4.3. Risk-Based Approach. There has been a shift towards a risk-based approach in protective security, where security measures are tailored to specific threats and vulnerabilities. Adversarial risk assessments, protective intelligence, and vulnerability management are used to identify and prioritise security risks. This approach helps allocate resources effectively and focus on the most critical protective security needs.

4.4. Increased Collaboration and Intelligence Sharing. The recognition of the interconnectedness of security threats has led to greater collaboration among organisations and intelligence sharing between private and public sectors. Information sharing platforms, public-private partnerships, and joint exercises have improved situational awareness and facilitated coordinated responses to security incidents.

4.5. Emphasis on Insider Threats: Organisations have increasingly recognised the potential risks posed by insiders, including employees, contractors, and partners. Insider threat programmes and monitoring systems have been developed to detect and reduce malicious activities or unintentional security breaches from within the organisation.

4.6. Integration of Artificial Intelligence and Automation. The advent of artificial intelligence (AI) and automation has brought new opportunities and challenges to protective security. AI-powered analytics, machine learning algorithms, and automation technologies are being utilised to enhance threat detection, video surveillance, access control, and incident response. However, the risks associated with AI, such as algorithmic biases and vulnerabilities, also need to be addressed.

4.7. Focus on Resilience and Business Continuity. Protective security has increasingly embraced the concept of *resilience*, emphasising the ability to withstand and recover

from security incidents. Business continuity planning, crisis management and emergency preparedness frameworks, and incident response exercises are integrated into protective security strategies to minimise the impact of disruptions and ensure the continuity of operations.

These are some of the notable trends and developments in the recent history of protective security evolution. The focus on cybersecurity, enhanced physical protection, risk-based approaches, collaboration, insider threats, AI and automation, and resilience reflects the ongoing efforts to adapt to emerging threats and protect people, property, and information in an evolving hostile landscape.

5. A Protective Security Mindset: The Onion Skin Defence-In-Depth Approach

The exact year when the onion skin defence-in-depth approach was first used in the protective security industry is difficult to determine as it has evolved over time and its origins are not attributed to a specific event or moment. However, the concept of layered defence, which forms the basis of the onion skin approach, has been employed in security practices for many years. While it is challenging to pinpoint the exact origin of the analogy, Bruce Schneier has extensively written about and advocated for the use of the *onion skin* metaphor to describe the layered defence approach in his books and articles.

The "*Onion Skin Defence-In-Depth*" is a concept used in protective security to describe a layered approach to safeguarding people, property, or information. It draws an analogy to the layers of an onion where each layer provides an additional level of protection. This approach aims to create multiple barriers to *deter* and mitigate threats, making it more difficult for adversaries to breach the security perimeter and reach valuable targets.

Here is an explanation of the *Onion Skin Defence-in-Depth* concept:

5.1. Outer Layer: The outermost layer represents the initial line of defence and serves as a *deterrent* to potential threats. It includes measures such as perimeter fencing, access control systems, signage, and visible security personnel. This layer is designed to create a visible presence and discourage unauthorised individuals from attempting to breach the security perimeter.

5.2. Middle Layer: The middle layer builds upon the outer layer and focuses on physical security measures. It includes elements such as reinforced doors, locks, barriers, surveillance cameras, and intrusion detection systems. This layer is aimed at *detecting* and *delaying* unauthorised access, giving security personnel or police officers additional time to *respond* to adversarial attacks.

5.3. Inner Layer: The inner layer represents the last line of defence and is primarily concerned with protecting specific assets, sensitive information, or critical infrastructure. It involves additional security measures such as access controls, biometric systems, security officers, encryption, firewalls, and other protective technologies. This layer is designed to reduce or minimise the impact of a security breach, providing a strong defence for the most critical elements of the protected entity.

The concept of *Onion Skin Defence-in-Depth* recognises that no single layer of security is fool proof. By implementing multiple layers of protection, each with its own unique characteristics and strengths, the overall security posture becomes stronger and more *resilient*. Even if one layer is breached, there are additional layers in place to impede further progress and increase the chances of *detection* or intervention.

The *Onion Skin Defence-in-Depth* approach is not limited to physical security measures but can also be applied to cybersecurity, information security, and other domains where protection of assets is crucial. In these contexts, layers may include firewalls, intrusion detection systems, encryption, access controls, security policies, employee training, and incident response plans.

The development of an appropriate security culture, where the right secure behaviours are adopted by an organisation's workforce can be an essential element of a protective security defence-in-depth. By adopting desired behaviours, the leadership, employees, contractors, visitors, and suppliers can be a huge force multiplier, at a relatively low cost, in strengthening the overall *resilience* to security events and adversarial attacks.

A Behavioural-Based Security (BBS) programme should be risk-based and concentrate on what a person needs to know to meet the organisation's security expectations. Workforce behaviour and staff vigilance are amongst the most off-putting factors for someone who is up to no good; it makes them think that they are being watched and that they are more likely to be *detected* and intercepted.

When workers support protective security through their behaviours, by being vigilant and report suspicious activities, they provide a *deterrent*, create an early warning mechanism, and assist in initiating an impactful and proportionate *response*. This reduces the likelihood of a security event, limits the negative consequence, and reduces the lost work time. By using the workforce eyes and ears, the chances of keeping an organisation's people and property safe are significantly enhanced.

By adopting a layered *Defence-in-Depth* concept —like that of an onion skin— organisations can enhance their overall security posture, *deter* potential threats, *detect* intrusions early, *delay* the adversary's attack plan, and minimise the potential impact of security incidents.

This layered approach provides a comprehensive and robust defence against a wide range of adversaries and attack vectors.

6. Does There Need to be a Difference Between the Industrial Safety and Protective Security Risk Management Approach?

Whilst the *Swiss Cheese Model* and the protective security *Onion Skin Defence-in-Depth* concept share some similarities in their approach to risk management and protection, they are primarily designed for different domains—industrial safety and protective security, respectively. Let's assess their synergies:

6.1. Layered Approach. Both models embrace a layered approach to risk mitigation. The *Swiss Cheese Model* emphasises the need for multiple layers of defence to prevent accidents, whilst the *Onion Skin Defence-in-Depth* concept focuses on creating multiple barriers to *deter* and mitigate threats in protective security. Both concepts recognise that relying on a single layer of defence is insufficient and that multiple layers increase the overall robustness of the system.

6.2. Multiple Defences. Both models recognise the importance of having multiple defences in place. The *Swiss Cheese Model* highlights the need for various safeguards, such as policies, procedures, training, and equipment. The *Onion Skin Defence-in-Depth* concept advocates for a combination of physical, technological, and behavioural measures to protect assets or information. In both cases, the idea is to have a range of overlapping defences that collectively enhance security or safety.

6.3. Human Factors. The *Swiss Cheese Model* emphasises the role of human error and organisational factors in accidents, highlighting latent and active failures. In contrast, while the *Onion Skin Defence-in-Depth* concept acknowledges human behaviours, it primarily focuses on physical and technological measures to *deter* and mitigate threats. The human element is still relevant, but it may not be as central as in the *Swiss Cheese Model*. Arguably, therefore, there is an opportunity to increase the human behavioural aspect within the *Defence-in-Depth* concept and take the learning from Reason's *Swiss Cheese Model.*

6.4. Domains of Application. The *Swiss Cheese Model* is primarily used in industrial safety and risk management, addressing accidents and hazards in complex systems. On the other hand, the *Onion Skin Defence-in-Depth* concept finds its application in protective security, such as safeguarding assets, facilities, or information from motivated and capable threat actors. While they share some underlying principles, their specific domains of application and contexts differ.

In summary, the safety focussed *Swiss Cheese Model*, and the protective security *Onion Skin Defence-in-Depth* concept share similarities in their layered approach to risk mitigation and the recognition of the need for multiple defences. However, they differ in their focus areas, with the *Swiss Cheese Model* primarily targeting industrial safety and the *Onion Skin* concept focusing on protective security. Does there need to be a difference, surely both are designed to safeguard an organisation's people, therefore a blended approach is better.

7. Would an Organisation Benefit from a Blended Approach?

It is advisable for an organisation to adopt both the *Swiss Cheese Model* and *Onion Skin* approach to creating *Defence-in-Depth* to safeguard its employees from both industrial hazards and adversarial attacks. These two concepts complement each other and provide a comprehensive approach to risk management and protective security.

By implementing the *Swiss Cheese Model*, the organisation can effectively address industrial hazards and safety risks. As previously mentioned, this model emphasises the identification and mitigation of latent and active failures within the system. It promotes a proactive approach to safety by implementing multiple layers of defence, such as safety policies, procedures, training programmes, and physical barriers. The *Swiss Cheese Model* helps identify and address potential weaknesses and vulnerabilities within the system that could lead to accidents or workplace hazards.

On the other hand, adopting the *Onion Skin Defence-in-Depth* concept enhances the organisation's ability to protect against adversarial attacks by motivated and capable threat actors. It involves the implementation of multiple layers of protective security measures, including physical, technological, and procedural [behavioural] defences. This approach makes it more challenging for adversaries to breach the site perimeter and reach valuable targets. By having a layered defence, the organisation can *deter* and *detect* potential attacks, *delay* adversaries' progress, and provide sufficient time to initiate a pre-planned and frequently rehearsed *response*.

Combining both the *Swiss Cheese Model* and *Defence-in-Depth* principles allows the organisation to create a robust and holistic approach to employee safety and security. It acknowledges the importance of addressing both accidental hazards and intentional threats, ensuring the well-being and protection of employees in various scenarios.

It is worth noting that the specific implementation of these models should be tailored to the organisation's unique needs, industry, and risk profile. Conducting a thorough workplace safety and adversarial risk assessment and engaging relevant experts can help determine the most appropriate measures and strategies for safeguarding employees from both industrial hazards and adversarial attacks.

8. Conclusion

Cannon Asset Protection Limited*™** advocates that organisations create a blended ***cheese and ***onion*** flavoured safety and security programme to safeguard their employees, visitors, and supply chain partners.

A converged directorate within an organisation's structure —comprising of safety, security, emergency preparedness, business continuity, protective intelligence, and business risk specialists— will provide the necessary organisational *resilience* to *deter*, *detect*, *delay*, and *respond* to industrial safety hazards, workplace accidents, and intentional adversarial attacks. Given the appropriate exposure to, and overt support from, the C-Suite, this *Protective Security and Organisational Resilience* directorate can increase the levels of certainty that an organisation can deliver against their business plan and achieve their goals.

This blended approach, to create and maintain a safe and secure working environment, is the cornerstone of ***The CAP Way*™** Behavioural Based Security (BBS) awareness programme that advocates that the protective security function should not become another 'silo' within a dysfunctional organisation. Impactful protective security programmes are achieved through collaboratively working with those departments who amplify the organisational Values, and by engaging, educating, encouraging, and influencing secure behaviours across the workforce. '*Security'* should not be shrouded in mystery, it is not a '*black art'*, and time should be spent recruiting advocates and ambassadors from across the organisation requiring protection.

THE CAP WAY™
CANNON ASSET PROTECTION