Indicative Guidelines for Chemical Safety and Security in Small and Medium-sized Enterprises to Foster the Peaceful Uses of Chemistry

OPCW
Organisation for the Prohibition of Chemical Weapons

Editors: N. Kojevnikov, L. Zhao, H. Mat Som, T. Zhang

Indicative Guidelines for Chemical Safety and Security in Small and Medium-sized Enterprises to Foster the Peaceful Uses of Chemistry

The Outcome of the Workshops on Developing Tools
for Chemical Safety and Security Management

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 PREFACE

At its Sixteenth Session, the Conference of the States Parties (hereinafter "the Conference") to the Convention on the Prohibition of the Development, Production, and Stockpiling and Use of Chemical Weapons and on Their Destruction (hereinafter "the Convention") adopted decision C-16/DEC.10 (dated 1 December 2011) on the "Components of an Agreed Framework for the Full Implementation of Article XI" of the Chemical Weapons Convention. In accordance with operative paragraph 2(a) of that decision, States Parties and the Technical Secretariat (hereinafter "the Secretariat") were required "to conduct, based on input from National Authorities and relevant stakeholders, a needs assessment on tools and guidance that would be helpful for promoting chemical safety and security".

In order to follow up on that decision and to systematically gather and make available the knowledge and practices shared by the States Parties, the Secretariat, since 2009, has continuously organised various workshops and training courses that have involved relevant governmental institutions, the National Authorities, the chemical industry, international organisations, and academic representatives to foster the exchange of best practices related to chemical safety and security (CSS). In addition, the Secretariat has issued a number of Notes that have formed the basis for it to conduct surveys that gathered information from States Parties about best practices, especially those relating to the chemical industry and laboratories; one of these was the "Needs Assessment and Compilation of Tools, Guidance, and Best Practices in Chemical Safety and Security Management" (S/1602/2018, dated 16 March 2018), which encouraged States Parties to voluntarily submit information relating to needs assessments and about existing tools, guidelines, and best practices.

Based on the resulting information, the Secretariat realised that it was crucial for it to develop tools for CSS management. To this end, the Secretariat, in March 2019, initiated a project to develop non-binding and indicative guidelines for CSS in order to foster a culture of the peaceful uses of chemistry, an initiative which would contribute to economic and technological development under Article XI and prevent the re-emergence of chemical weapons. In a statement to a workshop entitled "Developing Tools for Chemical Safety and Security Management" held in The Hague, The Netherlands, from 25 – 27 March 2019, the Deputy Director-General underscored the importance of this endeavour, which would "encompass a broad range of stakeholders" and which would entail the active involvement of the Organisation for the Prohibition of Chemical Weapons (OPCW).

The first step in this process has involved giving priority to the development of indicative guidelines for chemical safety and security in small and medium-sized enterprises (SMEs). The "Indicative Guidelines for Chemical Safety and Security in Small and Medium-sized Enterprises to Foster the Peaceful Uses of Chemistry" which follow were finalised by a multidisciplinary group of experts in chemical management (see Appendix C, page 53) at a second workshop held in Almaty, Kazakhstan, from 2 – 6 December 2019.

These indicative guidelines incorporate basic elements, such legal frameworks and selected institutional and technical capacities that can help to achieve chemical safety and security, and build on the resources, tools and guidance developed by international organisations dealing with public health and the environmental and safety aspects of chemicals. While highlighting the complementary relationships that exist among existing regulations and capacities and CSS measures, this document specifically addresses the needs of SMEs in States Parties whose economies are either developing or in transition and which have shared their existing best practices as they seek to enhance CSS management. Other stakeholders may also find these guidelines useful as they seek to promote CSS in order to foster the peaceful uses of chemistry.

2 TABLE OF ACRONYMS AND ABBREVIATIONS

AG	Australia Group
AI	Artificial Intelligence
AIChE	American Institute of Chemical Engineers
ASTM	American Society for Testing and Materials
CAS	Chemical Abstract Service
CCPS	Center for Chemical Process Safety
CCTV	Closed-circuit television
CDC	Centers for Disease Control and Prevention
CFATS	Chemical Facility Anti-Terrorism Standards
CSS	Chemical safety and security
CW	Chemical weapon
CWC	Chemical Weapons Convention
DHS	Department of Homeland Security
ECHA	European Chemicals Agency
EU	European Union
GHS	Globally Harmonized System of Classification and Labelling of Chemicals
ICCA	International Council of Chemical Associations
ILO	International Labour Organization
IPCS	International Programme on Chemical Safety
ISO	International Organization for Standardization
MCMT	Methylcyclopentadienyl manganese tricarbonyl
MoU	Memorandum of understanding
OECD	Organisation for Economic Co-operation and Development
OPCW	Organisation for the Prohibition of Chemical Weapons
OSHA	Occupational Health and Safety Administration
PPE	Personal protective equipment
REACH	Registration, Evaluation, Authorisation and Restriction of Chemicals
SDS	Safety Data Sheet
SMEs	Small and medium-sized enterprises
SOP	Standard operating procedure
STOP	Substitution, Technical measures, Organisational, and Personal protective equipment
TNT	Trinitrotoluene

UNECE	United Nations Economic Commission for Europe
UNEP	United Nations Environment Programme
WHO	World Health Organization

3 INTRODUCTION

Developing a culture of chemical safety and security (CSS) requires participation from all employees and stakeholders of a company that uses chemicals.[1] Furthermore, individuals across the chemical sector, including those in education, research and development, production, and regulation have a responsibility to promote CSS within and outside of their respective institutions.

Many chemists, chemical engineers, and/or practitioners working in the field of chemistry, especially in small and medium-sized enterprises (SMEs), have not received formal training in CSS. This reality shows the need for the chemical sector at large to redefine the important components of critical safety and security knowledge so that future chemists, chemical engineers, and other employees can be properly trained. Academia, government agencies, professional societies, accreditation bodies, and industry all have a role to play in the development of future employees in the chemical industry.

Companies and other organisations involved in the storage, manufacture, trade, sale, transportation, and/or disposal of chemicals are expected to implement best practices in chemicals management. In light of this requirement, a chemicals-management plan should be developed in accordance with a company's best practices; the recommendations contained in safety data sheets (SDS); health, safety, security, and environmental rules and regulations; and in line with generally accepted practices and legal provisions at both the local and international levels.

3.1 Role of the Employer

It is the duty of the employer to ensure that the development, implementation, and monitoring of CSS policies and programmes are in place. These policies shall include the designation of persons responsible for the overall execution of all such activities. Employers are also obliged to ensure the availability of a chemical emergency-response plan to mitigate the consequences of an accident or incident. The plan should include, but not be limited to, the provision of emergency-response equipment and the designation of trained emergency responders. It is required that all relevant staff shall receive training for chemical hazard information; that they implement the required procedures for chemical hazard communication management; that they participate in audits; and that they provide suggestions for improvement. However, in the final analysis, the responsibility for adequate safety and security policies rests with the employer and cannot be delegated.

All documentation, including training materials, shall be regularly updated and disseminated to employees and should include the following information:

a. changes made to chemical formulations;

b. data on new chemicals that have been introduced into chemical processes;

[1] All web-resources referenced in this document were accessed between 2 to 6 December 2019, unless otherwise noted.

c. changes that have been made to process conditions;

d. information about the substitution in the chemicals used; and

e. any other relevant information.

3.2 Role of the Employees

Although the ultimate responsibility for CSS rests with the employer, employees have a vital role to play as well. They need to comply with all policies, procedures, and programmes, including, but not limited to, the following: the safe use of chemicals and equipment; the proper utilisation of safeguards and safety/security devices; and procedures ensuring that they are taking the necessary steps to reduce risks. Employees are required to report all accidents/incidents and near misses occurring in the workplace, as well as initiating and promoting safe behaviours.

3.3 Protecting Communities

The implementation of CSS programmes is key to protecting surrounding communities and the environment from potentially dangerous impact, should an accidental or intentional release of hazardous chemicals occur. Carrying out risk assessments is the core principle underlying the implementation of this policy; such risk assessments identify potential safety and security scenarios and spell out site-specific measures that are appropriate and that can adequately protect the facility and surrounding communities.

3.4 What is Chemical Safety?

Chemical safety is the practice of handling chemicals in a manner that protects human health and the environment from accidents/incidents and their unintentional consequences.

Chemical safety is comprised of a spectrum of disciplines involving the occupational, public, process, environmental, consumer, storage, and distribution aspects of avoiding risks and accidents. Many of these are dealt with by international conventions and by several international organisations and agencies. According to the International Programme on Chemical Safety (IPCS) of the World Health Organization (WHO), "Chemical safety is achieved by undertaking all activities involving chemicals in such a way as to ensure the safety of human health and the environment. It covers all chemicals, natural and manufactured, and the full range of exposure situations from the natural presence of chemicals in the environment to their extraction or synthesis, industrial production, transport, use, and disposal."[2]

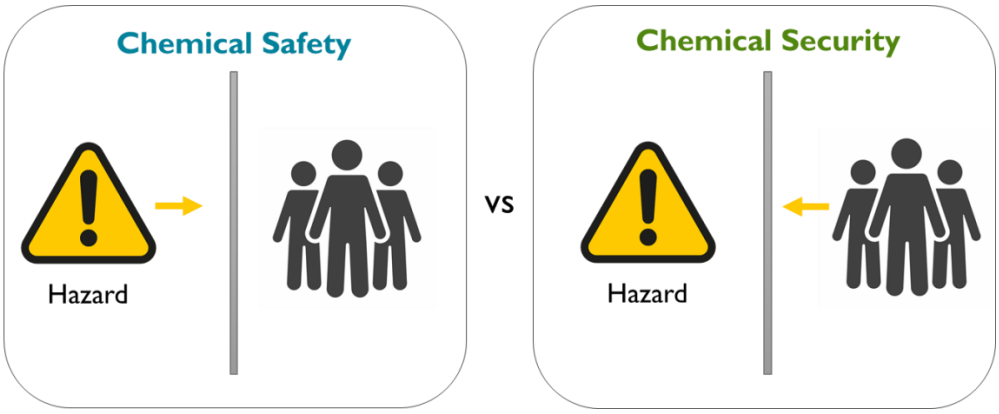
---

[2] World Health Organization, *Chemical Safety*, https://www.who.int/health-topics/chemical-safety#tab=tab_1 accessed 4 May 2021)

3.5 What is Chemical Security?

Chemical security refers to policies and practices to prevent malicious and/or illicit use of chemicals, as well as to mitigate the impact of these kinds of events, should they occur. Chemicals should be secured throughout their lifecycles from threats, including those posed by terrorism. Some chemical facilities possess materials that could be stolen and used to cause harm and/or damage. An attack on certain facilities could cause a significant number of deaths and injuries. The impacts of an accident or attack can be far-reaching and may occur in a variety of ways.[3]

Figure 1. Safety Barriers vs Security Barriers



Both types of barriers are placed between people and hazards (or assets); however, safety barriers are intended to protect people from chemicals and security barriers protect chemicals from the actions of people. [4]

3.6 Why Chemical Safety and Security Are Important for SMEs

Many SMEs require frequent or occasional use of hazardous or dual-use chemicals for a variety of reasons. Regardless of the reason for their use, hazardous and dual-use chemicals present a security and safety challenge to SMEs. In light of this, it is crucial that CSS programmes are put into place by all SMEs in order that they can assess and reduce potential risks, thus effectively and efficiently protecting:

a. employees and members of the surrounding communities from physical or psychological harm, injury, and/or death;

---

3 United States Cyberstructure and Infrastructure Security Agency, *Chemical Security*, https://www.dhs.gov/topic/chemical- security (accessed 4 May 2021)

4 Figure created by staff at the Global Chemical and Biological Security Group, Sandia National Laboratories: "Unintentional Versus Intentional Chemical Incidents", SAND2019-2822 TR, Sandia National Laboratories, Albuquerque, New Mexico, USA

b. infrastructure and other material resources within the facility and outside from damage, contamination, or destruction;

c. businesses from undesirable impacts, including interruption, reputation, and loss in consumer confidence;

d. direct and indirect financial impacts, such as lost workhours; cash flow problems; profit margins; possible penalties and fines; and increased insurance premiums;

e. business continuity and licences to operate (production and operations can be stopped by incidents);

f. companies from legal action (local, regional, national, or international) at the personal, civil, or criminal levels; and

g. resource allocation by avoiding increased scrutiny from government agencies, the surrounding communities, employees, and other stakeholders.

4 KEY CONCEPTS

Terms in relation to CSS, as found in this document, may have meanings that differ from how they are used in common, everyday language. It is, therefore, useful to define how various terms are utilised in this guidelines document in order to achieve precision and clarity.

Asset: The term "asset" refers to "an item of value from the perspective of either the owner or a potential adversary. The item may be dangerous, rare, valuable, or otherwise hard to replace, or it may cause an unacceptable delay in business if lost".[5] From a potential adversary's perspective, assets may include:

a. an item of current or future financial value, such as computers, equipment, valuable reagents, and chemical products with high resale value on the black market;

b. chemicals that can be used to make a weapon, such as explosives, toxic chemicals, or precursors to chemical weapons;

c. chemical precursors for the production of illicit chemicals;

d. information, including employee knowledge, trade secrets, proprietary information and

e. unpublished or unpatented scientific processes; and

f. a piece of equipment that could be used in weapons or for illicit drug production."[6]

Chemical accident: The term "chemical accident" refers to *"any unplanned event involving hazardous substances that causes or is liable to cause harm to health, the environment or property*, such as loss of containment of hazardous substances, explosions, and fires. These events are generally the result of unintended technological failures and/or human errors."[7]

---

5 Salerno, R. & Gaudioso, J, *Laboratory Biosecurity Handbook*, CRC Press: Boca Raton, 2007; p. 105

6 Nelson, Andrew Wyatt & Malcahy, Mary Beth, *Chemical Security Handbook: Security Risk Assessment for Laboratories*, United States, Department of Energy (June 2020, p. 12), https://doi.org/10.2172/1635333, (accessed 4 May 2021)

7 Organisation for Economic Cooperation and Development, *Guiding Principles for Chemical Accident Prevention, Preparedness and Response: Guidance for Industry (including Management and Labour), Public Authorities, Communities, and Other Stakeholders* (2nd edition, 2003, p. 18), http://www.oecd.org/env/ehs/chemical-accidents/Guiding-principles-chemical-accident.pdf (accessed 4 May 2021)

Chemical incident: A "chemical incident" refers to a chemical release "arising from technological incidents, natural disasters, conflicts, and terrorism."[8]

Controls: "Controls" refer to "measures, barriers, safeguards, or layers of protection. Controls are technical, operational, and/or organisational elements which either individually or collectively reduce the risk of an accident or incident. If an accident or incident occurs, controls can also minimise the severity of the consequences."[9]

Dual-use: The term "dual-use" refers to chemicals, equipment, knowledge, or software that can be used for legitimate purposes or misapplied for illicit purposes.[10]

Exposure: "Exposure", when referring to chemicals, refers to the "contact with a chemical by swallowing, by breathing, or by direct contact (such as through the skin or eyes). Exposure may be short term (acute) or long term (chronic)."[11]

Hazard: The term "hazard" refers to any agent that has the potential to cause harm. "Hazards can also be conditions or activities that, if left uncontrolled, may cause injury, loss of life, or damage to property or the environment."[12]

Table 1. Typical Hazards at Chemical Facilities[13]

Hazard	Examples
Physical	Explosive materials, flammable substances, pyrophoric solids or liquids, gases under pressure, electrical equipment, and energy sources
Health	Acute toxicity, carcinogenicity, mutagenicity and reproductive toxicology, or a respiratory sensitisation
Condition	Incompatible chemical storage (e.g., strong oxidizers such as nitric acid near hydrocarbons), high or low pressure, magnetic fields, extreme temperatures, or waste accumulation
Activity	Scale-up of a reaction or the addition of catalyst to a reaction, both activities which could increase the rate and quantity of heat and by-product generation, and the transportation of hazardous materials

8 World Health Organization, *International Programme on Chemical Safety, Chemical Incidents and Emergencies*, https://www.who.int/ipcs/emergencies/en/ (accessed 4 May 2021)

9 Nelson, Andrew Wyatt & Malcahy, Mary Beth, ibid, p. 12

10 Nelson, Andrew Wyatt & Malcahy, Mary Beth, ibid, p. 12

11 United States Agency for Toxic Substances and Disease Registry, *Glossary of Terms*, https://www.atsdr.cdc.gov/glossary.html#G-D- (accessed 4 May 2021)

12 Nelson, Andrew Wyatt and Malcahy, Mary Beth, op cit, p. 13

13 American Chemical Society, "Recognize the Hazards", https://www.acs.org/content/acs/en/chemical-safety/guidelines-for-chemical-laboratory-safety/resources-supporting-guidelines-for-chemical-laboratory-safety/recognize-hazards-c.html (accessed 4 May 2021)

Physical security: The term "physical security" refers to the physical protection of assets, whether in active use or in long-term storage; physical security includes site perimeter protection, as well as the protection of assets within the confines of the facility.

Risk: In the context of *chemical safety*, "risk" refers to the likelihood that a hazard will lead to a negative outcome and to the severity of any resulting consequences, should they occur. In terms of *chemical security*, "risk" refers to the likelihood that an adversary will intentionally cause harm and to the consequences stemming from that harm.

Safety data sheet: A comprehensive, standard document that chemical manufacturers and suppliers should provide to the end user; it should include information on physical and chemical properties, environmental hazards, health hazards, first aid measures, and accidental release measures.[14]

Threat*:* The term "threat" (can also be called an adversary) refers to "a person or group of persons with the motivation and capability to cause harm, either through theft, diversion, and/or sabotage of an asset. Threats can be people who are either unaffiliated with the institution (termed "outsiders") or people who are affiliated with or employed by the institution (termed "insiders"), or a collusion of insiders and outsiders. Insider threats can also be described as persons who have authorised access to a facility, which can provide them with extensive knowledge of the facility and assets."[15] Insiders making threats may voluntarily cooperate with outsiders, or they may be coerced, under duress, to assist outsiders posing a threat.

Vulnerability: The term "vulnerability" refers to a weakness in a safety or security system which can lead to chemical accidents or incidents, such as exploitation by adversaries for malevolent purposes.

---

14 United Nations, United Nations, *Globally Harmonized System of Classification and Labelling of Chemicals*, Chapter 1.5, p. 35, (7th edition 2017), https://unece.org/fileadmin/DAM/trans/danger/publi/ghs/ghs_rev07/English/ST_SG_AC10_30_Rev7e.pdf (accessed 4 May 2021)

15 Nelson, Andrew Wyatt & Malcahy, Mary Beth, op cit, p. 14

5 SAFETY AND SECURITY: MUTUAL SUPPORT AND POTENTIAL CONFLICT

The management of safety and security risks can be complementary. Sections of the management system that are complementary can cooperate to include inventory management, audit programmes, hazard reductions, and similar elements. For example, both safety and security risks can be reduced by the implementation of access controls. By limiting access to a hazardous working place to individuals with appropriate safety training, SMEs can reduce the likelihood of an accident. Similarly, by limiting access to a hazardous working place to authorised individuals only, SMEs can reduce the potential for security incidents. Although the motivation for these access control measures is different, they can be integrated.

There are fields where safety and security are independent of each other. For example, personal protective equipment (PPE) supports safety, but does not directly support security. Perimeter monitoring supports security, but does not directly support safety.

CSS controls can sometimes also be at odds with one another. Two critical areas where safety and security goals can conflict include physical security and information management. For example, securing chemicals or equipment from theft could lead to locking exit doors, but safety concerns require leaving doors open to ensure people can leave quickly should an emergency arise. Similarly, information protection may result in restricting signage and access to information on the chemical names, quantities, and locations, whereas safety concerns lead towards open information-sharing to prevent accidental exposures. These examples indicate that safety and security requirements need to be considered as a whole, so that potential conflicts can be addressed to balance the needs of emergency egresses (exits) and hazard communication against protecting assets within the facility.

6 CHEMICAL SAFETY AND SECURITY RISK-MANAGEMENT SYSTEM

CSS risk management systems share many features, but can conflict with one another. There are numerous publications on risk-management systems, ranging from theoretical approaches to governmental requirements and to international standards. Each publication caters to a different audience and varies in its purpose; makes use of varied terminology; and often utilises a different structure. The guidance iterated in the following sections is based on the following:

a. input from international experts;

b. procedures contained in established risk-management systems;

c. international standards described in the International Organization of Standardization's guidelines ISO 45001 and ISO 35001;

d. governmental guidelines published by the Occupational Safety and Health Administration (OSHA) in the United States, entitled "Occupational Safety and Health Program Management Guidelines"; and

e. recommendations from the American Institute of Chemical Engineers (AIChE), found in two publications: "Guidelines for Risk-Based Process Safety" and "Guidelines for Analysing and Managing the Security Vulnerabilities of Fixed Chemical Sites".[16,17,18,19]

At the basic level, each of these references suggests safety and security risk management systems that are grounded in four domains:

a. management and employee commitment to safety and security;

b. understanding the hazards, assets, threats, and risks;

c. managing risks; and

d. learning from experience to improve.

At the end of these OPCW guidelines is a compilation of case studies that focus on different CSS scenarios (see Appendix A, page 46).

---

16 International Organization for Standardization, ISO 45001:2018 , "Occupational Health and Safety" (2018), https://www.iso.org/iso-45001-occupational-health-and-safety.html (accessed 4 May 2021)

17 International Organization for Standardization, ISO 4500135001:2019, "Biorisk management for laboratories and other related organisations" (2019), https://www.iso.org/standard/71293.html (accessed 4 May 2021)

18 United States Occupational Safety and Health Administration, "Safety and Health Program Management Guidelines" (2015), https://www.osha.gov/shpmguidelines/SHPM_guidelines.pdf (accessed 4 May 2021)

19 American Institute of Chemical Engineers, *Guidelines for Risk-Based Process Safety*, DOI: 10.1002/9780470925119

7 MANAGEMENT AND EMPLOYEE COMMITMENT TO SAFETY AND SECURITY

The first step to any robust CSS programme is making both management and employees aware of the importance of safety and security and encouraging their commitment to making the workplace safer and more secure. Common risk-management approaches aim to increase management and employee commitment through a number of elements. The most important aspects of this are described below.

7.1 Management Participation and Commitment

Because management serves as a role model for all individuals in the worksite, including employees, contractors, and visitors, its visible commitment to safety and security is a strong indicator that these are integral elements of the workplace. For this reason, participation and commitment by management to CSS is paramount. Managers of SMEs in particular exercise great influence over the success of safety and security programmes, as they can directly influence how safe and secure a company is. The aspects listed below are key elements that will ensure that management succeeds in its efforts to make the workplace more safe and secure:

1. **Accountability**: Management should define expected safety and security roles and responsibilities at every level for employees, contractors, and visitors. Once these have been specified, management should hold everyone accountable to these roles and responsibilities to ensure that safety and security programmes function as intended.

2. **Authority**: Because management is generally responsible for hiring, promoting, rewarding, penalising, and dismissing employees, it should clearly demonstrate a commitment to safety and security so that employees, contractors, and visitors will report safety or security concerns without fear of retaliation.

3. **Finances**: Because management needs to constantly increase the productivity or quality of its products, the pressures related to this may unintentionally compromise safety and security goals; however, safety and security measures should be included as critical functions that are necessary investments and expenditures for the sustainability of the business.

4. **Infrastructure**: Management should make timely decisions on the maintenance, investment, and procurement of those components related to major safety and security infrastructure (e.g., ventilation or fences).

5. **Policies**: Management should raise everyone's awareness of the importance of developing, implementing, enforcing, and auditing all policies related to safety and security.

7.2 Employee Participation and Accountability

Participation by employees in safety and security programmes is equally important, and all necessary steps should be taken to ensure that all staff understand and are committed to CSS. There are a number of ways for employees to contribute to and be involved such programmes, including the following:

1. **Mentoring programmes**: Employee participation in mentoring programmes can take place within or outside SMEs. For example, more senior and/or experienced employees should help train junior, less experienced employees. Similarly, SMEs could consider arranging mentoring programmes in collaboration with other companies in order to enable staff members to learn about and disseminate best practices.

2. **Briefings**: Before the beginning of each shift, it is recommended that employees spend a few minutes discussing relevant safety and security issues.

3. **Meetings**: Safety and security debriefs can be integrated into regular meetings so that employees and management can discuss lessons learned, best practices, or issues that need to be addressed.

4. **Training and certification programmes**: Employees should be trained and certified, continuously and regularly, in safety and security policies in order for them to improve their performance. In addition, safety and security performance should be factors that are weighed when employees are being considered for promotion.

5. **Committees**: Employees should be encouraged to participate in safety and security committees within SMEs, industry, and trade associations (e.g., Responsible Care®), or national or international task forces.

7.3 Promotion of a Safety and Security Culture

The promotion of a culture of safety and security encourages employees to understand and follow safety and security practices, even when they are working unobserved. Although approaches to developing these policies are varied, the following steps can foster a stronger safety and security culture:

1. Define realistic safety and security goals (e.g., SMART goals[20]);

---

20 SMART Goals are: "**S**pecific, **M**easurable, **A**chievable, **R**elevant, and **T**ime-Bound", *SMART Goals: A How to Guide*, https://www.ucop.edu/local-human-resources/files/performance-appraisal/How%20to%20write%20SMART%20Goals%20v2.pdf (accessed 4 May 2021)

2. Communicate and enforce safety and security goals transparently. Management should foster open communication among all levels of employees working in SMEs;

3. Establish peer-exchange sessions, where best practices and lessons learned from near misses, incidents, and/or accidents can be shared; and

4. Establish systems that reward commitment to safety and security practices that are culturally relevant and appropriate.

Penalties or disciplinary actions should only be used when they are warranted, commensurate with the incident, and culturally appropriate. Care should be taken to avoid penalising employees who voice safety or security concerns, as this may result in employees being afraid to report important information. Management should do everything possible to foster a culture of communication and transparency, including:

1. Developing mechanisms to contract only with qualified (and, if appropriate, licensed or certified) suppliers, service providers, and other business partners;

2. Joining professional organisations, industry and trade associations (e.g., Responsible Care®), or national or international task forces and their training/educational programmes. Such membership will allow SMEs to access information on best practices regarding safety, security, and the environment; and

3. Promoting The Hague Ethical Guidelines (see Appendix B, page 53).

7.4 Compliance

It is important for leaders of SMEs to follow existing regulations, standards, codes, and polices related to safety and security. Compliance with these measures helps reduce liability in the event that a chemical accident or incident occurs and allows for systematic auditing to determine the performance of safety and security programmes at a facility. The table below describes some of the measures that can be adopted:

Table 2. Regulations, Standards, Codes, and Policies

Term	Definition	Organisation/Example
Regulations	Laws and requirements established at the local, national, or international level	European Chemicals Agency (ECHA)/Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) UN/Chemical-related multi-lateral agreements and instruments
Standards	A non-binding set of guidelines set forth by a consensus-based organisation that are "an agreed way of doing things"	International Organization for Standardization (ISO) American Society for Testing and Materials (ASTM) International
Codes	A series of principles and guidelines set forth by a professional society, trade and industry association, or corporation	OPCW (e.g., The Hague Ethical Guidelines) International Council of Chemical Associations (ICCA) /Responsible Care®
Policies	Guidelines and rules set forth by the company that employees are required to follow	Environmental, safety, security, and health guidelines and rules

7.5 Outreach

SMEs should consider the safety and security of their employees, contractors, and visitors. as well as the safety and security of the surrounding communities.[21] Through outreach programmes, companies can:

1. Better understand the resources, situation, and concerns of a community (for example, first-response capabilities, levels of crime, information on water usage, etc); and

2. Build positive relationships and confidence within the communities. The importance of such activities during normal operations and during crises cannot be overstated. However, care should be taken to not reveal sensitive information in any outreach efforts.

21 United Nations Environment Programme, "Awareness and preparedness for emergencies at local level (APELL)", https://www.unenvironment.org/explore-topics/disasters-conflicts/what-we-do/preparedness-and-response/awareness-and-preparedness

8 UNDERSTANDING THE HAZARDS, ASSETS, THREATS, AND RISKS

At the most basic level, understanding safety and security risks involves answering the following questions:[22]

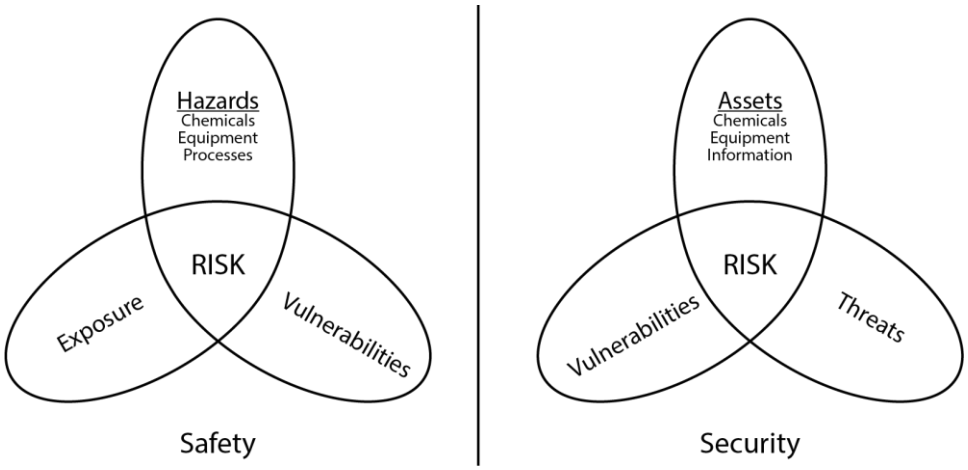
a. What can go wrong?

b. How likely is it?

c. What are the potential impacts?

Figure 2 below describes some of the relevant safety and security factors.

Figure 2. Safety and Security Risk Factors[23]



Safety risk is the intersection of exposures, vulnerabilities, and hazards. Security risk is the intersection of assets, threats, and vulnerabilities.

A risk assessment is the structured process that answers these questions by:

1. Identifying hazards, threats, assets, and vulnerabilities (Figure 2);

2. Analysing and evaluating the likelihood and consequences of an incident/accident (Figure 3, below), as well as vulnerabilities by assessing the effectiveness of existing controls; and

3. Identifying and prioritising risk-mitigation controls.

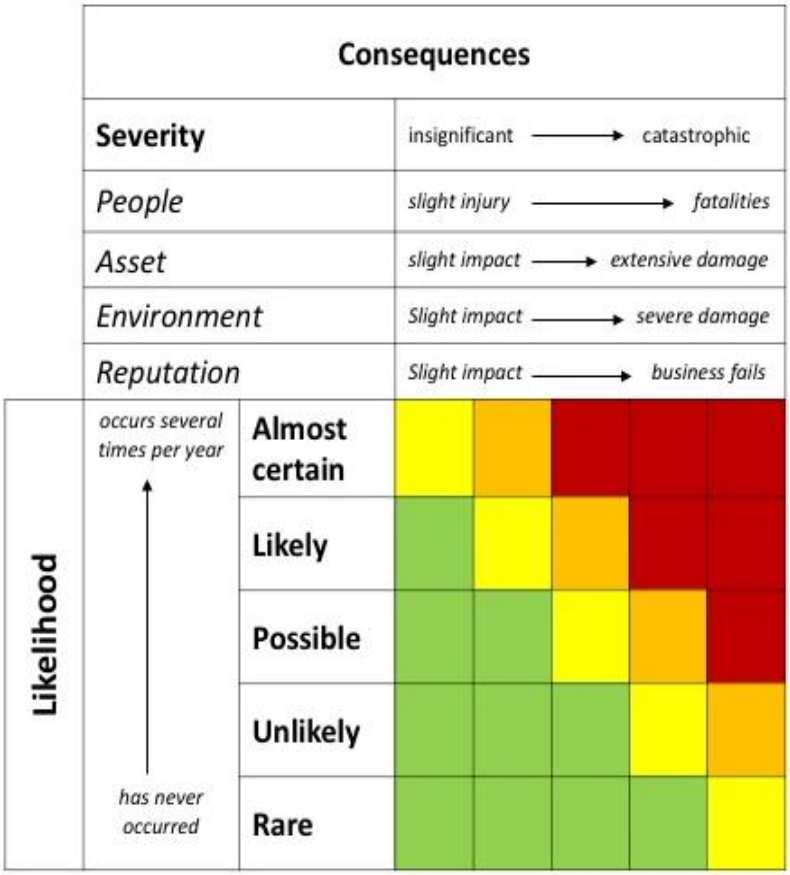
---

22 Kaplan S, & Garrick BJ, "On the Quantitative Definition of Risk", *Risk Analysis*, Vol. 1, No. 1, 1981

23 Figure created with Adobe Illustrator CC 2019 during the "Workshop on Developing Tools for Chemical Safety and Security Management" held in The Hague, the Netherlands, from 25 – 27 March 2019.

Resources for controlling safety and security risks at most SMEs are limited. Thus, it is important that risks are systematically prioritised, so that resources are used most efficiently and in a manner that improves and enhances control. An example is shown in the table below. A risk assessment should be the basis for such a process. It can identify when risks are unacceptable and justify the need to implement additional control measures that can be used to reduce those risks.

Figure 3. Sample Risk Matrix Table



The text in italics represents example frequencies or severities. SMEs should develop site-specific criteria.
Red represents the highest risk; orange represents medium-high risk; yellow represents medium-low risk; and green represents the lowest risk.[24]

[24] Figure created with Adobe Illustrator CC 2019 during the "Workshop on Developing Tools for Chemical Safety and Security Management" held in Almaty, Kazakhstan, from 2 - 6 December 2019.

Risk assessments have the added benefit of providing information on related aspects of risk management, including, whether the enterprise is:[25]

a. complying with governmental regulations;

b. planning for preventative maintenance;

c. regularly updating emergency plans;

d. systematically recording accidents and incidents;

e. identifying training and supervision needs;

f. evaluating the workflow with other units and processes;

g. justifying space and equipment needs;

h. evaluating procedural changes; and

i. carrying out advanced planning for facility renovations.

Ultimately, risk assessments help SMEs identify their risk tolerance by providing a systematic approach to determining if a risk is acceptable or unacceptable. Risk acceptance criteria can be researched from information found in country regulations or set by the SME itself. These criteria can be of a qualitative, semi-quantitative, or quantitative nature, depending on the potential severity of the event under analysis.[26,27,28,29,30]

---

25 Astuto-Gribble, Lisa M & Caskey, Susan Adele, "Laboratory Biosafety and Biosecurity Risk Assessment Technical Guidance Document", United States, https://www.osti.gov/servlets/purl/1171429 (accessed 4 May 2021)

26 Brazil, São Paulo State Regulation CETESB P4.261, Attachment H, pages 112-113, https://cetesb.sp.gov.br/wp-content/uploads/2013/11/P4261-revisada.pdf (accessed 20 May 2021)

27 United States Department of Labor, Occupational Safety and Health Administration, "Final Rule on Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents", Federal Register 57, no. 6356 (24 February 1992), https://www.osha.gov/laws-regs/federalregister/1992-02-24 (accessed 4 May 2021)

28 American Institute of Chemical Engineers, Center for Chemical Process Safety (CCPS), "Security Vulnerability Analysis", https://www.aiche.org/ccps/security-vulnerability-analysis (accessed 4 May 2021)

29 American Institute of Chemical Engineers, Center for Chemical Process Safety, "Risk Analysis Screening Tool (RAST) and Chemical Hazard Engineering Fundamentals (CHEF)", https://www.aiche.org/ccps/resources/tools/risk-analysis-screening-tool-rast-and-chemical-hazard-engineering-fundamentals-chef (accessed 4 May 2021)

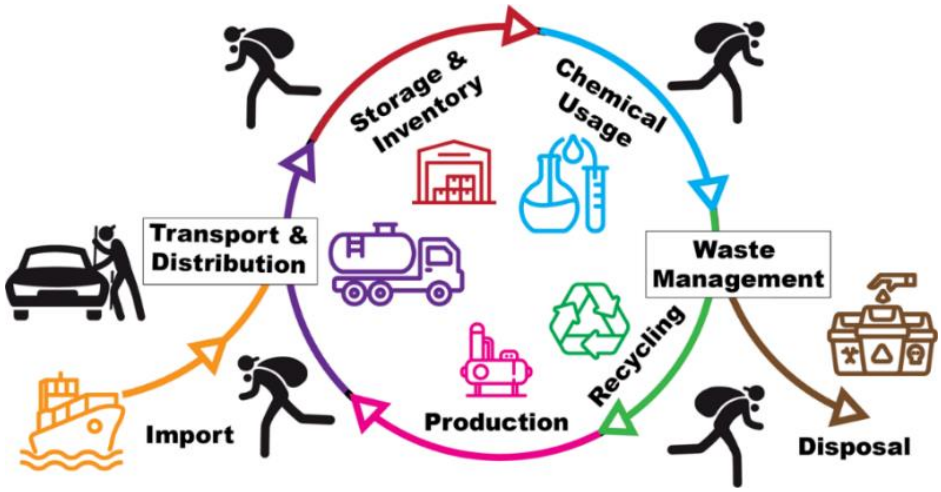
30 United States Environmental Protection Agency, "Guidance for Facilities on Risk Management Programs (RMP)", https://www.epa.gov/rmp/guidance-facilities-risk-management-programs-rmp (accessed 4 May 2021)

8.1 Performing a Risk Assessment

A risk assessment, that is, the systematic evaluation of potential risks, is a multi-step, iterative process. To accurately identify hazards, assets, and threats at a facility, employees in multidisciplinary teams at all levels need to actively participate and contribute to the evaluation. Risk assessment teams should be aware that chemical hazards and threats to assets can exist at all stages of the chemical lifecycle (Figure 4, below). Therefore, each stage of the lifecycle should be considered for the unique risks it presents.

SMEs should perform an initial risk assessment before production has started, but ongoing assessments are important as well, since risk levels can vary over time. In the absence of changes, periodic risk assessments enhance employees' risk awareness and identify unintended deviations in work practices. Revalidations and review of previous risk assessments should identify, evaluate, and suggest controls for any new hazards. After review of the results of any risk assessment, SMEs should update control measures to address unacceptable risks.

Figure 4. Chemical Lifecycle CSS Vulnerabilities[31]



8.2 Identifying Assets, Hazards, and Threats

Safety and security risk assessments start by defining the situation. This involves identifying, for the purposes of evaluation, a SME's assets, hazards, threats, and safety and security measures.

31 Sandia National Laboratories, "Security Concepts", SAND2020-6798 TR, Albuquerque, New Mexico, USA

8.3 Screening Hazards and Assets

SMEs may possess a few, hundreds, or even thousands of chemicals, but not all of them pose a significant safety or security risk. To reduce overall risk at a facility, SMEs should prioritise resources for chemicals and other assets which are most hazardous. Chemicals, equipment, or information may have safety or security concerns if they have properties of toxicity, explosivity, flammability, monetary value, and utility in relation to illicit drug or chemical weapons production.

Prioritisation should be guided by the potential impact of the chemicals present in SMEs on health, safety, environmental, financial, and reputational concerns. When prioritising chemical hazards and assets, an enterprise should consider it important to ask what would make these chemicals either hazardous (*safety concerns*) or valuable to an adversary with an intent to cause harm (*security concerns*). The following questions may guide this prioritisation:

1. Is the chemical highly toxic (*safety and security)*?
2. Is the chemical chronically toxic (safety)?
3. Is the chemical flammable and/or explosive (safety and security)?
4. Is the chemical known to be used for illicit purposes (security)?
5. Is it a precursor to a chemical weapon, illicit drug, or explosive (security)?
6. Is the chemical expensive (security)?

In order to identify whether chemicals pose safety or security concerns, it is recommended that the user consult publicly available resources, such as:

a. national legislation;

b. SDSs, available from suppliers, from the GESTIS substance database,[32] or from PubChem;[33]

c. the Globally Harmonized System of Classification and Labelling of Chemicals (GHS);[34]

---

32 Institute for Occupational Safety and Health of the German Social Accident Insurance, GESTIS Substance Database, "Information System on Hazardous Substances of the German Social Accident Insurance, GESTIS Substance Database (accessed 4 May 2021)

33 United States, Department of Health and Human Services, National Center for Biotechnology Information, PubChem, https://pubchem.ncbi.nlm.nih.gov/. (accessed 4 May 2021)

34 United Nations, *Globally Harmonized System of Classification and Labelling Of Chemicals* (7th edition, Chapter 1.5, p. 35), New York and Geneva (2017), https://unece.org/fileadmin/DAM/trans/danger/publi/ghs/ghs_rev07/English/ST_SG_AC10_30_Rev7e.pdf (accessed 4 May 2021)

d. the Convention's Annex on Chemicals;[35]

e. the Australia Group (AG) Export Control List: Chemical Weapons Precursors;[36]

f. the European Union (export control legislation) (EU)[37]; and

g. the US Department of Homeland Security (DHS) Chemical Facilities Anti-Terrorism Standards Chemicals (CFATS), Appendix A, Chemicals of Interest (COI).[38]

Equipment: Chemical equipment may pose greater safety risks than chemicals or may increase the risks of the chemical—for example, equipment can raise temperatures of chemicals that do not react under ambient conditions to temperatures that make them highly hazardous (e.g., exceeding flashpoints and boiling points).

Furthermore, equipment that causes strain to the human body or that results in unsafe (or insecure) procedures could harm the musculoskeletal system (falls, crushes, etc.), or increase the exposure to employees of dangerous substances (venting gasses, dusty procedures, etc.).

Another crucial factor that SMEs need to consider is the dual use of equipment. Equipment is a critical component which is not only needed by legitimate businesses, but which can also be used for the production of chemical weapons, explosives, and illicit or recreational drugs. Therefore, equipment may be targeted for theft or sabotage. The AG has developed a reference handbook for employees working to control biological and chemical weapons proliferation.[39] The handbook provides lists of CW precursors; of dual-use chemical manufacturing facilities; and of equipment, as well as related technologies.

---

35 Organisation for the Prohibition of Chemical Weapons, "Annex on Chemicals", from the Chemical Weapons Convention, https://www.opcw.org/chemical-weapons-convention/annexes/annex-chemicals/annex-chemicals

36 Australia Group, "Export Control List: Chemical Weapons Precursors", https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/precursors.html (accessed 4 May 2021)

37 European Commission, Council Regulation (EC) No 428/2009 of 5 May 2009, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0428 (accessed 4 May 2021)

38 Cyber Security &Infrastructure Security Agency, Chemical Facilities Anti-Terrorism Standards Chemicals (CFATS), Appendix A, Chemicals of Interest (COI), https://www.cisa.gov/appendix-chemicals-interest (accessed 4 May 2021)

39 Australia Group, Common Control List Handbooks, https://australiagroup.net/en/controllisthandbooks.html (accessed 20 May 2021)

A number of countries, complying with United Nations (UN) Security Council Resolution 1540 (2004), which states that "All States shall refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes,"[40] established regulations for the control of exports of dual-use equipment, including software and technology, which can be used for both civilian and military purposes. The European Union (EU) has also passed a regulation setting up an EU regime for the control, transfer, broking and transit of dual-use items that includes a list of such equipment and technology.[41]

Used chemical equipment may be attractive to individuals with malicious intentions. SMEs should be mindful that such individuals may target used or unwanted equipment, either through in-person exchanges, online purchases, or by collecting the equipment from waste bins or waste that has been discarded or left in piles. Therefore, enterprises should take care and exercise oversight when disposing of, selling, or trading obsolete equipment.
The dismantling of equipment presents safety risks that are often neglected or overlooked. It is imperative that any equipment is thoroughly drained, cleaned, and decontaminated prior to disposal, sale, or trade, so that no hazardous chemicals or chemical residues remain. Experienced and trained employees or contractors should carry out and oversee these processes and certify their completion. Such attention to detail is important for the protection of any downstream users who may further dismantle the equipment by cutting, crushing, grinding, recycling, or salvaging scrap materials; these individuals may not have an adequate understanding of the chemical hazards or of the appropriate protection measures (PPE, engineering controls, etc.) that should be taken.

8.4 Information for Security Purposes

The theft or release of information is often overlooked when a security-risk assessment is being carried out. Release of information can occur across multiple platforms, including emails, social media, written documents, and press releases. The types of sensitive information that may be included in such a risk assessment are:[42]

a. unpublished research materials;

b. inventories of chemicals;

---

40 United Nations (UN), UN Security Council Resolution 1540 (2004), https://www.un.org/disarmament/wmd/sc1540/ (accessed 20 May 2021)

41 European Commission, "Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (recast)", https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF

42 Nelson, Andrew Wyatt & Malcahy, Mary Beth, op cit, p. 23

c. the personal identification information of employees or other persons with access to the facility;

d. business plans;

e. security protocols;

f. facility blueprints or designs;

g. the location of high-risk chemicals; and

h. building occupancy.

The information listed above should be protected, as it could help adversaries identify the amount and location of valuable assets; highlight security vulnerabilities; or enable them to threaten the well-being of employees.

8.5 Identifying Security Threats

Once hazards and assets have been prioritised, potential threats by adversaries can be identified. Such threats might include (but not be limited to) researchers and/or companies, that are competitors to the enterprise; criminals looking for items to sell; disgruntled employees; and terrorists or other extremists. The motivations of these different groups or persons vary widely; for example, they can have the intent to[43]:

a. inflict casualties;

b. make a political statement;

c. cause damage or destruction;

d. profit from their activities;

e. spread fear;

f. destroy or gain proprietary information;

g. carry out some form of protest; and

h. retaliate against a perceived wrong.

It may be advisable/necessary to collaborate with local law enforcement agencies to exchange relevant information. Alternatively, organisations can draw up a list of potential/theoretical adversaries with attributes covering a spectrum of motivations and capabilities; this set will allow SMEs to conduct various kinds of analyses that can assist them to assess their security vulnerabilities.

8.6 Safety and Security Measures

43 Nelson, Andrew Wyatt and Malcahy, Mary Beth, op cit, p. 14 and p. 27

Protective security measures are formulated to protect people, information and assets from being lost or compromised through the application of various preventive techniques. It is, therefore, recommended that facilities should employ the following strategies to mitigate safety and security risks:

Table 3. Preventive Strategies to Deter, Detect, Delay, and Respond (Defend/Recover)

Strategy	Description	Example
Deter	Substitute or eliminate the hazard to make it less attractive to an adversary or increase the number of barriers to discourage an adversary from attempting to steal or sabotage an asset.	**Safety**: Signs and notices in work areas may reduce risk by alerting employees about hazardous conditions and limiting their access to hazardous areas. **Security**: Fences and closed-circuit television (CCTV) cameras around the perimeter of facility may discourage adversaries from attempting to break in.
Detect	Increase the ability of staff (through training) to identify unauthorised individuals (adversaries) attempting to access the facility. The goal is to detect unauthorised access as quickly as possible. Increase the ability of staff to identify risks or control the system in order to identify process deviations or upsets and then take corrective actions, human and/or automated, to prevent the event from progressing.	**Safety**: Low-pressure alarms can indicate a leak in equipment or obstruction in a pipeline. High-level transmitters can indicate a potential for overflow and close an automated valve on the reed pipe or shut down the feed pump before a leak happens. **Security**: Motion detectors will sound an alarm in the event of unauthorised access.
Delay	Increase barriers to slow down an adversary and the progress of a harmful event until responders can assess and intervene.	**Safety**: Spill containment measures (such as curbs, dike wall systems, and pits) can prevent chemical spills from spreading throughout the facility or into the surrounding environment. **Security**: Measures, such as locked doors, closed gates, and tire spikes, can be put in place to allow time for security guards to arrive.
Respond (Defend)	Increase the speed, number, or effectiveness of the approach responders to stop an adversary or protect employees and the surrounding community.	**Safety**: Emergency response teams can stop continuing spills, collect waste for disposal, and clean up the spills. **Security**: Security guards or local police/agents should be alerted as quickly as possible in order that they can arrest adversaries.

8.7 Additional Considerations

SMEs sometimes operate in industrial parks in close proximity to other plants. The hazards arising from each of these plants may require different levels of safety and security measures, resulting in a patchwork within the industrial park. Coordination and communication with other industry representatives could help address the overall risk profile of the industrial park and may provide standard safety and security measures at a reduced cost. For instance, an industrial park should have a single, centralised emergency preparedness and response team for CSS incidents, whose infrastructure, operations, and maintenance costs are shared by all the companies in that park.[44]

44 United States Occupational Safety and Health Administration, "Safety and Health Program Management Guidelines" (2015), https://www.osha.gov/shpmguidelines/SHPM_guidelines.pdf (accessed 4 May 2021)

9 MANAGING RISKS

Below is a summary of common concepts and elements found in most safety and security risk management systems.

9.1 Protection and Control of Hazards and Assets

Application of risk treatments should follow four basic principles; they should be:

1. Balanced;
2. Layered;
3. Graded; and
4. Hierarchy-based.[45]

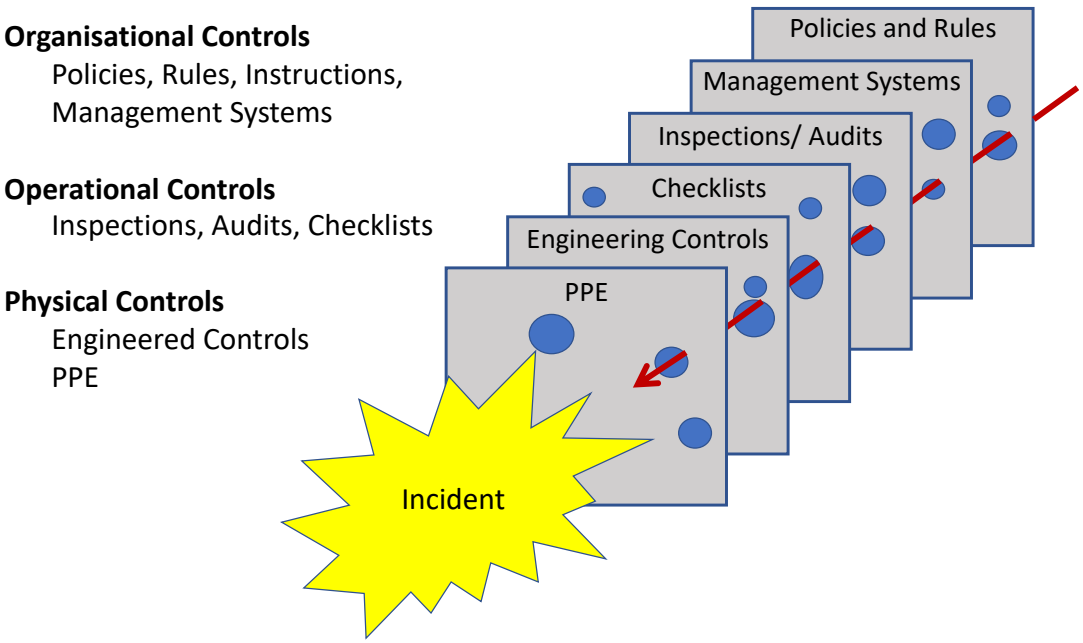
Safety and security measures should not be addressed piecemeal, but should be examined as a whole. This means they should be *balanced*, that is, based on the particular needs and situation of the SME concerned. In some SMEs, safety concerns may be greater than security concerns, whereas in others, security concerns are of more importance; therefore, the level of controls should reflect these concerns.

No risk mitigation control will be absolutely reliable. Every control measure has the potential to fail, as illustrated by the figure of the "Swiss Cheese Model" (see Figure 5 below), an assessment tool for risk analysis and risk mitigation which is widely used in diverse areas (for example, in chemical processes). This model visualises SME safety and security risks as layers of Swiss cheese stacked next to each other, and illustrates that a mistake in one hole or slice (level) can be prevented from affecting other slices or layers by the removal of the vulnerabilities (holes) in each slice. According to this model, risks are best mitigated by a *layered approach*, that is, one that uses multiple, independent layers of protection.

---

45 Garcia, Mary Lynn, *Design and Evaluation of Physical Security Systems* (2nd edition, 2007), DOI: 10.1016/C2009-0-25612-1

Figure 5. "Swiss Cheese Model" for Multiple Layers of Controls to Mitigate Risks[46]



Consequently, the implementation of a combination of organisational, operational, and physical controls will provide a more reliable system (see Table 4 below). From a safety perspective, this can mean that the enterprise adopts a fully automated action to shut down a process (should the need arise) and also installs an alarm requiring that, should the alarm sound, an operator responds to stop the event from progressing. From a security perspective, this can mean limiting various points of access to employees, contractors, and visitors as areas become progressively more sensitive.

Table 4. Types of Control: Organisational, Operational, and Physical

Control Category	Description	Example
Organisational	Creating policies, rules, instructions, and management systems	**General**: Placing limitations on speed limits for cars. **Chemical safety**: Establishing policies and standard operating procedures (SOPs) as to how PPE should be used and how staff should respond to emergencies and/or critical incidents (when alarms sound). Require all personnel to have safety training and training in the use of PPE.

46 Figure created by contributors to this document.

Control Category	Description	Example
		Chemical security: Putting into place a policy restricting access to sensitive areas to authorised employees only.
Operational	Carrying out tasks such as creating procedures, carrying out inspections and audits, and drafting checklists for employees	**General**: A police officer who enforces the speed limit. **Chemical safety**: Creating standard operation procedures (SOPs) for how to use PPE and how to respond to respond to emergencies and/or critical incidents (when alarms sound) . **Chemical security**: Establishing a schedule for inspections of the site perimeter, to be carried out by security guards.
Physical	Purchasing and using physical objects that can contain, prevent, or separate exposure to chemicals, theft, or sabotage	**General**: Building speed bumps that can slow down the movement of cars. **Chemical safety**: Encouraging the use of alarms, fume hoods, sprinklers, PPE, automated interlocks, pressure-relief devices, dikes, and foam generation systems. **Chemical security**: Building alarms, fences, doors, and walls.

A *graded approach* suggests that risk-mitigation measures should be risk-based. Higher-risk materials, processes, and work sites should be safeguarded by more layers of protection and by more rigorous controls than those which pose a lower risk. For example, access to a public space like a cafeteria may require someone's passing through an unlocked door, while access to a high-hazard area may require the presentation of identification to a security guard; a special key to enter the building; and the use of CCTV-monitoring of the worksite. This concept of graded risk control also improves safety by restricting unqualified and unauthorised individuals from entering more hazardous areas of the facility.

An important concept used in chemical safety for the selection of control measures is the *hierarchy of controls* [47] or the "STOP" principle ("**S**ubstitution, **T**echnical measures, **O**rganizational, and **P**ersonal protective equipment"[48]). These concepts define a hierarchy that ranks the effectiveness of possible controls to reduce risks; analogies can also be made using the STOP principle for security control hierarchies.

Table 5. The Hierarchy of Controls[49]

Measure	Description	Example
Elimination	Elimination is the process of removing the hazard from the workplace. It is the most effective way to control a risk because the hazard is no longer present. It is the preferred way to control a hazard and should be used whenever possible.	Removing unwanted and unused chemicals, devices, or equipment from facility. Note: This approach directly supports safety and security goals.
Substitution	Substitution occurs when a hazardous chemical, process, or piece of equipment is replaced with one that is less hazardous. The risk is not completely eliminated, but is lowered.	Replacing organic solvents with water-based solvents. Note: This approach often supports safety and security goals; however, some substitutions intended to lower security risk may inadvertently increase safety risks and vice versa.
Engineering (Technical measures)	Engineering controls are methods that are built into the design of a plant, equipment, or process to minimise hazards. They are a very reliable way of controlling employees' exposures, as long as the controls are designed, used, and maintained properly.	Safety and security process control. Enclosure and/or isolation of hazardous substances. Ventilation of hazardous gases, fumes, etc.

47 United States Centers for Disease Control and Prevention, "Hierarchy of Controls", https://www.cdc.gov/niosh/topics/hierarchy/default.html (accessed 20 May 2021)

48 Deutsche Gesetzliche Unfallversicherung (DGUV), STOP principle, http://nano.dguv.de/en/prevention/stop-principle/ (accessed 20 May 2021)

49 Material in this table has been quoted and drawn from "Health and Safety Programmes, Hazard Control", by the Canadian Centre for Occupational Health and Safety, www.ccohs.ca/oshanswers/hsprograms/hazard_control.html (accessed 20 May 2021)

Measure	Description	Example
Administrative	Administrative controls improve safety and security through implementation and enforcement of policies and administrative actions. These control measures do not directly affect the hazard or asset itself, but moderate expectations and/or behaviours of the people around hazards and assets.	Restricting access to a work area. Restricting the task only to those competent or qualified to perform the work. Using job-rotation schedules that limit the amount of time an individual is exposed to a substance. Defining which chemicals should be secured at a facility; establishing access policies and procedures to monitor use of hazardous chemicals.
PPE	PPE includes items that "provide a barrier between the wearer and the chemical or material." However, PPE "should never be the only method used to reduce exposure because it may fail (stop protecting) with little or no warning." PPE is the last line of defence.	Respirators, protective clothing (such as gloves, face shields, eye protection, and footwear). Note: A good analogy for security is situational awareness. Individuals who are aware of what is happening around them can help identify security "red flags" as they arise.

9.2 Operating Procedures for Safety and Security

Creating comprehensive documentation of operating procedures is a critical step towards establishing a safe and secure facility. Accidents and incidents can arise when an employee, contractor, or visitor does not understand the language in which the safety and security procedures have been drafted, and thus has difficulty with following those procedures. SMEs should ensure that all employees can understand written procedures and are aware that each stage of the lifecycle presents unique CSS risks that should be managed. Below is a description of each portion of the lifecycle and some key safety and security considerations:

Table 6. Operating Procedures for and Security Throughout the Chemical Lifecycle

Lifecycle Stage	Description	Safety and Security Considerations
Procurement	Due diligence in the selection of a reliable and credible chemical supplier can affect safety and security at the plant on all levels, local and global.	**Safety**: Ensuring the use of reliable and credible suppliers will reduce the likelihood of poor-quality materials or mislabelled ingredients. **Security**: Unreliable suppliers may directly or indirectly support local criminal operations or in some cases rogue nations.
Storage	The safe and secure storage of chemicals can reduce the likelihood of chemical theft, sabotage, fires, explosions, spills, or adverse reactions. Proper storage provisions can be requested from the manufacturer or supplier of chemicals, and the labels and SDS should contain information.	**Safety**: Chemicals should be separated when required and stored in appropriate containers. SDSs for each product should be available in the warehouses or at storage facilities at all times. **Security**: Chemicals that potentially might pose a security risk should be adequately protected.
Inventory	Regular and systematic inventories of the chemicals and record-keeping are important components of a well-established CSS management programme. Monitoring may include gathering and maintaining information, such as, but not limited to: • CAS numbers • Storage requirements • Quantities • Manufacture and expiration dates of chemicals • Potential hazards • PPE requirements	**Safety**: Updated and maintained lists of chemicals and their quantities on site can assist first responders in the event of a spill or release. **Security**: Inventory databases should be secured and treated as sources of sensitive information, as they can provide information to possible adversaries on what can be stolen or sabotaged at a facility. Every removal of chemicals should be recorded (which employee removed the chemical and in which quantities).
Usage/Production	SOPs, checklists, and/or other forms of documentation should be developed and used for all relevant activities.	**Safety**: Documentation for all relevant activities should include safety processes and protection protocols that employees are expected to use or follow.

Lifecycle Stage	Description	Safety and Security Considerations
		Security: Documentation for all relevant activities should include security protocols and practices that all employees should follow.
Waste Management	Companies should review existing applicable national legislation on the proper identification, characterisation, handling, and disposal of wastes; those wastes should always be identified and described as waste products. The company should work with and hire reliable and credible waste contractors. If products can be recycled or reused, care should be taken to accurately document protocols to maintain safety and security.	**Safety**: Documentation should be provided on the compatibility of mixing wastes. **Security**: If theft or sabotage of waste is a concern, wastes should be adequately secured. Waste contractors should be selected through due diligence for reliability and credibility. **Equipment:** Care should also be taken to ensure that used chemical equipment is disposed of properly and not diverted to individuals without appropriate background and safety checks being carried out. The company should always ensure that equipment does not get into the hands of individuals with malicious intentions (thus maintaining security).
Transportation	Companies should ensure that materials are appropriately packaged for safe and secure transport (as outlined in the SDS). Appropriate SDSs should be provided with all shipments.	**Safety**: Documentation should include specifications for the correct type of vehicles to be used for transporting chemicals; load limits for the vehicles; and safe practices to be applied during the loading and unloading of chemicals. **Security**: Reliable and credible transport contractors should be selected. When possible and when appropriate, physical security measures should be applied to shipments (e.g., tamper-evident locks, GPS tracking for critical products, etc).
Sales/Distribution	Protocols should exist to determine whether sales of chemicals and new or used equipment are used for their intended purpose. These protocols are commonly	**Safety**: The potential hazards of chemicals and equipment should be documented and provided to customers. **Security**: Care should be taken during the sales of hazardous or dual-use chemicals and/or equipment to customers. Suspicious sales should be carefully considered and reviewed prior to the delivery of products. If in doubt, the company should refuse to sell.

Lifecycle Stage	Description	Safety and Security Considerations
	referred to as "Know Your Customer."[50]	Severe cases should be reported to law-enforcement bodies.

9.3 Safe and Secure Work Practices

To ensure the safety, security, and reliability of the workplace, a number of structural and administrative measures need to be put into place, specifically:

a. ensuring the integrity and reliability of the facility;

b. guaranteeing that the facility is safe by design;

c. setting up industrial/occupational hygiene programmes;

d. appointing chemical safety and security officers;

e. providing medical surveillance programmes;

f. managing/overseeing contractors;

g. managing change effectively;

h. drawing up emergency-management plans; and

i. giving due consideration to human factors.

9.3.1 Ensuring the Integrity and Reliability of the Facility

The overall facility where chemicals are manufactured and stored should be properly maintained, and be safe and secure. The maintenance and routine inspection of equipment, materials, and facilities (i.e., that is, "good housekeeping" and good business practice) help to ensure the integrity of the infrastructure and identify vulnerabilities before accidents and incidents arise. Where appropriate, the environment should be controlled to prevent vegetation from obscuring the facility perimeter. If useful, service contracts for equipment should be drawn up in a manner that ensures the reliability of equipment.

50 United States Department of Homeland Security, "If You See Something, Say Something"™ (p. 2), https://www.cisa.gov/sites/default/files/publications/see-say-chemical-security-trifold-508.pdf (accessed 4 May 2021)

9.3.2 Guaranteeing that the Facility Is Safe and Secure by Design

Before a facility is built, the design should include planning for CSS measures. This concept is often referred to as "Safe by Design" and "Secure by Design".[51] Regardless of whether safety or security measures were originally built into the facility, the risk profile of that facility will change over time, so changes or upgrades of safety and security features may be needed.

9.3.3 Setting Up Industrial / Occupational Hygiene Programmes

SMEs should consider consulting industrial (occupational) hygienists to help them to mitigate against and prepare to respond to identified chemical safety concerns. Industrial (occupational) hygiene is a science devoted to the identification, evaluation, and control of occupational conditions that cause sickness and injury.[52] Some of the typical activities that should be present in an industrial hygiene programme are:

a. monitoring of the concentrations of toxicants in the air and eliminating or reducing them as needed; and

b. monitoring and reducing the exposure of employees to physical hazards in the workplace, such as noise, heat, radiation, and other physical factors that affect their health.

9.3.4 Appointing Chemical Safety and Security Officers

SMEs should consider appointing CSS officers to routinely assess the safety and security conditions in the facility. SMEs can consider adding safety and security responsibilities to those personnel whose duties currently involve the areas of the environment, compliance, and auditing. In any case, sufficient resources (workhours, budget) should be devoted to CSS by management.

9.3.5 Providing Medical Surveillance Programmes

According to national and international guidelines, SMEs should strive to provide medical surveillance programmes for all employees.[53] Consideration should be given to scenarios or specific tasks where employees may be chronically or acutely exposed to toxic chemicals; to hazardous and repetitive work conditions (ergonomics concerns); and to stressful working conditions (psychosocial concerns). Medical care should be provided to employees suffering from occupational exposures or injuries.

---

51 United States Centers for Disease Control and Prevention, Prevention through Design (2013), https://www.cdc.gov/niosh/topics/ptd/default.html (accessed 4 May 2021)

52 Crowl, Daniel A. & Louvar, Joseph F, *Chemical Process Safety Fundamentals with Application* (2nd Edition, p.63, 10.2478/s11532-012-0131-1)

53 International Labour Organization, "Medical and health surveillance" (2004), https://www.ilo.org/legacy/english/protection/safework/cis/products/safetytm/chemcode/13.htm (accessed 4 May 2021)

9.3.6 Managing/Overseeing Contractors

Contractors are commonly hired by chemical companies. In some cases, contractors work at facilities on a daily basis, in many ways carrying out tasks usually performed by regular employees. In other cases, contractors visit the facility on a periodic basis only, for example to deliver shipments of raw materials. Contractors should receive, on a needs basis, information, resources, and/or training with respect to safety and security. SMEs should clearly spell out to contractors what safety and security training they are required to have and should request documentation proving that contractors have achieved the desired specific level of CSS competency. The table below highlights some examples of safety and security considerations with respect to contractors:

Table 7. Examples of Safety and Security Considerations for Contractors

Safety	Security
Transportation: Check that drivers have appropriate and valid licences; that they have appropriate PPE; and that they understand the relevant regulations. **Waste management:** The company should provide contractors with appropriate information on chemical waste composition and on potential hazards and processes at the plant. It should also validate that contractors dispose of hazardous wastes at adequate and approved treatment facilities. **Production line**: Training on emergency protocols being used at the facility should be provided.	**Unknown background**: Because SMEs often know less about contractors than about their own employees; it can, therefore, be more difficult for them to assess their backgrounds. It is advisable that SMEs carry out thorough background checks of contractors, as far as is permitted. **Unfamiliarity with security protocols**: Contractors may inadvertently leave materials unprotected if they have not received training in relation to security requirements.

9.3.7 Managing Change Effectively

Companies should expect that changes will occur over time in the chemical industry; these may arise for a number of reasons, such as innovations; employees leaving or retiring from the company; equipment replacement; and regulations being modified and new regulations being introduced. As these conditions fluctuate, it is natural that operational factors and the risks they pose will also change. It is therefore important for SMEs to manage these changes and that they react promptly and appropriately to them. Below are some common areas that should be monitored and updated routinely:

a. business plans;

b. SOPs;

c. SDSs;

d. engineering drawing and technical plans (site plans; process and instrumentation diagrams; maps/plans of process and rainwater drainage and collections systems, etc.);

e. inventories (their quantity and location, etc.);

f. documentation detailing the facility and its layout;

g. personnel records (such as the results of security and background checks);

h. emergency-response plans;

i. information on relevant laws and regulations;

j. copies of and information about international standards and conventions published by international organisations and governments (the GHS; the ICCA; the ILO; the ISO; the OPCW; the OECD; the United Nations Economic Commission for Europe (OECD); the United Nations Environment Programme (UNEP); and the WHO).[54]

9.3.8 Drawing Up Emergency-Management Plans

Companies that have put into place emergency-management plans are more likely to make correct, life-saving choices in stressful emergency situations. In light of this, it is critical that SMEs develop and practice emergency-management plans and responses. In some cases, drills may require support from fire departments, from law enforcement, and from other external agencies. Some suggestions as to how a company should develop its emergency-response plans and strategies are listed below. The company should:

a. develop and periodically review and update all emergency-response plans that involve chemical safety and security;

---

54 Organisation for Economic Cooperation and Development (OECD). Publications that are particularly relevant include: *OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response* (2nd edition, 2003).
Page 32 at the end of Chapter 1, entitled "General Principles", provides information that specifically addresses the needs of SMEs, http://www.oecd.org/env/ehs/chemical-accidents/Guiding-principles-chemical-accident.pdf. OECD, *Corporate Governance for Process Safety: Guidance for Senior Leaders in High Hazard Industries* (2012), OECD Environment, Health and Safety, Chemical Accidents Programme, https://www.oecd.org/env/ehs/chemical-accidents/corporate%20governance%20for%20process%20safety-colour%20cover.pdf.
OECD, *Guidance on Change of Ownership in Hazardous Facilities* (2018), OECD Environment, Health and Safety Series on Chemical Accidents, No. 31

b. inform and provide training to any individuals before they enter the premises; they should be told what to do and whom to contact in case of an emergency;

c. confirm that all emergency contact information is accurate and up-to-date;

d. undertake regular exercises and drills of plans and procedures;

e. make sure that all equipment and resources needed for any emergency response is available;

f. ensure that appropriate memoranda of understanding (MoUs) or resource-sharing plans are in place with local fire departments, with law enforcement, and with other companies, as necessary;

g. arrange for local fire departments and law enforcement to periodically visit the site;

h. develop an appropriate plan for the "use-of-force", should it become necessary during a security response.[55]

9.3.9 Giving Due Consideration to Human Factors

The management of risks needs to take into account ergonomics, that is, the influence of human factors and their impact on engineering and the design of products, systems, and processes.[56] Decisions or behaviours undertaken by humans can lead to accidents and incidents, particularly in systems (including software systems) that were not designed with human psychology and physiology in mind. The goal is, therefore, to reduce errors; increase safety and security; and increase productivity and comfort by considering the interaction of humans with technology and the work environment.

If human factors are not considered, it is likely that employees will find shortcuts or workarounds that undermine and short-circuit the safety and security measures that are in place. For example, if physical security systems result in long delays when an employee enters or exits the facility, employees may leave a locked door open. Similarly, if the climate or working conditions are too hot for staff to wear PPE, employees may choose to remove PPE for comfort, even when this decision increases their potential exposure to hazardous chemicals.

---

55 University of Geneva, "Use of Force in Law Enforcement and the Right to Life: The Role of the Human Rights Council" (2016), https://www.geneva-academy.ch/joomlatools-files/docman-files/in-brief6_WEB.pdf

56 Information obtained during personal communications with the Human Factors Department of the Sandia National Laboratories, 5 December 2019.

Some questions that companies need to ask when addressing the issue of the impact of human factors are:

1. Is the individual working in this job qualified to conduct the work independently?

2. Has s/he received adequate safety and security training for the tasks?

3. Are there aspects of the working conditions that may negatively impact the ability of employees to carry out tasks related to safety and security (the environment is too loud, too noisy, too crowded, too cold, too hot, or too sunny).

4. Do employees have the time and/or resources available to adequately perform their duties? Are employees required to perform multiple tasks at the same time?

5. Do the sheer number (or inefficient) safety and security requirements negatively affect productivity or disrupt employees from performing their other tasks?

10 LEARNING FROM EXPERIENCE

The remaining critical components of a safety and security risk-management system should be those dedicated to the company's learning from experience and from the chemical community, so that the company can continually improve its safety and security measures. Four crucial areas on which an enterprise should focus are:

a. performance evaluation;

b. accident and incident reports and investigations;

c. auditing and drafting corrective actions; and

d. education and training.

10.1 Performance Evaluation

To determine whether safety and security measures are effective, SMEs should gather information on the safety and security performance indicators that are relevant to their companies. The OECD and other organisations can provide guidance on how to choose indicators that are relevant to local conditions and situations.[57,58]

Table 8 below lists some examples of safety and security performance indicators that companies should consider implementing:

Table 8. Safety and Security Performance Indicators

Safety Indicators	Security Indicators
Safety controls have been defined and implemented for each major hazard. The major consequences that can ensue from safety lapses have been defined and well understood by all employees. The severity of the consequences of and likelihood of occurrence of adverse events have been identified for each potential hazard.	Security controls have been defined and implemented for each major asset. The consequences of theft from and sabotage to the facility have been explained and understood by employees and by management. The likelihood of an adverse event occurring and its potential consequences have been identified for each asset.

57 Organisation for Economic Cooperation and Development, *Guidance on Developing Safety Performance: Indicators related to Chemical Accident Prevention, Preparedness and Response for Industry* (2nd edition, 2008), https://read.oecd-ilibrary.org/environment/guidance-on-developing-safety-performance-indicators-for-industry_9789264221741-en#page1

58 United States Chemical Safety Board, https://www.csb.gov/

Safety Indicators	Security Indicators
Reduction in near misses (chemical accidents). The levels of injuries, accidents, and/or fatalities at the facility have been reduced. Emergency-response times have been reduced.	The number of thefts from the facility have been reduced and the levels of materials unaccounted for have been lowered. The response times needed by security staff have been reduced. The incidence of security violations has been reduced.

10.2 Accident and Incident Reports and Investigations

Accurate and timely accident and incident reporting and investigations can help SMEs identify vulnerabilities; the causes of accidents/incidents; and the corrective actions that need to be taken as a result. In addition, companies should not overlook the importance of the reporting and investigation of near misses, that is, incidents that could have potentially caused harm or injury, but did not because the danger was averted. Because near misses indicate that there are crucial safety and security vulnerabilities that should be addressed, staff should be encouraged to report these events, so that the company can carry out investigations and avoid the likelihood that such incidents will occur.

Similarly, near-miss investigations provide an opportunity for the company to understand which safety and security measures performed well and why, thus helping to avert the any exposure or release of hazardous materials. After any accident, incident, or near miss, SMEs should share lessons the learned with the relevant stakeholders.

10.3 Auditing and Corrective Actions

Auditing provides an opportunity for SMEs to determine whether the facility and operations are in compliance with standards, codes, and/or regulations. Thus, internal and external audits inform SMEs whether the safety and security management system is working as intended. Detailed information and tools for auditing can be found through a variety of organisations, including the ISO[59] and the Occupational Health and Safety Administration (OSHA) in the United States.[60]

---

59 International Organization for Standardization, ISO 19011:2018, "Guidelines for auditing management systems" (2018), https://www.iso.org/standard/70017.html (accessed 4 May 2021)

60 United States Department of Labor, "Recommended Practices for Safety and Health Programs, Explore Tools" (2016), https://www.osha.gov/safety-management/explore-tools (accessed 4 May 2021)

Management should carefully review audit-and-corrective action reports and respond to them by formulating actions plans that set deadlines; that assign persons who will be responsible for carrying out the recommendations; and that track implementation until completion.

10.4 Education and Training

SMEs should provide employees with adequate and accurate information about the hazards posed by chemicals; about how those hazards can be controlled and managed; and about any other CSS concerns. A risk assessment can help guide management to determine which information should be shared with the employees. Training and education should be provided to new employees as part of the onboarding (organisational socialisation) process and on a recurring schedule for all employees.

Numerous resources exist for safety and security training that can be readily accessed for free on the internet.[61, 62] Other resources that offer information and training in relation to safety and security include local academic institutions, private consulting companies, government authorities, and trade or professional societies. There is no prescribed format for information-sharing and capacity-building. Training records should be kept on file for auditing purposes.

---

61 American Chemical Society, "Chemical and Laboratory Safety", https://www.acs.org/content/acs/en/chemical-safety.html (accessed 4 May 2021)

62 United States National Academies of Sciences, Engineering, and Medicine, "Chemical Laboratory Safety and Security, A Guide to Prudent Chemical Management", http://dels.nas.edu/global/bcst/Chemical-Management (available in English, French, Arabic, and Indonesian)

11 EMERGING CYBER-SECURITY RISKS

Emerging information technologies (ITs) and automated industrial control systems offer the possibility of increased automation, interconnectivity, and productivity for SMEs; however, these tools also present cyber security risks which must be managed.[63,64] Before introducing new technologies, such as artificial intelligence (AI), cloud computing, or blockchain,[65] SMEs should assess the risks and identify mitigation plans. Similar to guidance for chemical and equipment management, cyber and computing resources should be assessed periodically to ensure they are working as intended.

Review of prior cyber-attacks involving ransomware and other malicious programmes, such as WannaCry,[66] Stuxnet,[67] Spectre,[68] Meltdown,[69] and Foreshadow[70] can help SMEs understand the consequences of and their vulnerabilities to malicious attacks; however, cyber technologies are changing rapidly, and thus vulnerabilities to new cyber-attacks should be expected. Data targeted by cyber-attacks may include:

a. digital control systems for plant operations;

b. inventories;

c. customer and price lists;

d. emails;

---

63 International Organization for Standardization, ISO 27001, "Information Security Management", https://www.iso.org/isoiec-27001-information-security.html

64 United States National Institute of Standards and Technology, *Cybersecurity,* https://www.nist.gov/cybersecurity (accessed 19 May 2021)

65 *Pence,* Harry *E, "Blockchain: Will Better Data Security Change Chemical Education?",* Journal of Chemical Education *2020, 97, 7, 1815-1818,* DOI: 10.1021/acs.jchemed.9b00560

66 United States National Cybersecurity and Communications Integration Center, "What is WannaCry/WannaCryptor?", https://www.us-cert.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf (accessed 4 May 2021)

67 Kushner, David, "The Real Story of Stuxnet", IEEE Spectrum (Volume 50, Issue 3, March 2013), https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet (accessed 4 May 2021)

68 "Meltdown and Spectre", https://meltdownattack.com/ (accessed 4 May 2021)

69 Ibid

70 "Foreshadow, Breaking the Virtual Memory Abstraction with Transient Out-of-Order Execution", https://foreshadowattack.eu/ (accessed 4 May 2021)

e. patented recipes and lists of ingredients; and

f. and other sensitive business documents.

In light of this, SMES should take a proactive approach to cyber-security by employing the following precautionary measures (this list is not exhaustive):

1. Consult with cyber-security experts, as needed;

2. Follow announcements from hardware and software suppliers; and

3. Ensure that they stay current on hardware and software updates.

A unique challenge presented by the shift to digital systems is that companies often contract with IT providers to assist them with this process. Companies should attempt to select reliable and credible IT contractors (refer to section 9.3.6 above on the oversight of contractors).

APPENDIX A: CASE STUDIES

A.1 Safety

Note: Different detailed examples of case studies, investigations, and recommendations can be found on the US Chemical Safety Board site.[71]

Threat Type	Example of Event
Spillage	*Description of incident*: A release of approximately one cubic metre ($1m^3$) of diesel fuel occurred at a fuel station when a transfer hose from a tank truck became detached during the filling of a storage tank. The spill resulted in contamination of the local soil, which was collected for disposal. The cause of the incident was the fact that the parking platform was not paved; hence the spillover material leached into the soil, resulting in environmental contamination. *Cause*: Because there was no proper hose connection from the tank truck to the storage tank, refilling was carried out directly through the insertion of the transfer hose through an open manhole on top of the storage tank. The transfer hose had simply been tied to the manhole with a piece of rope during the filling operation. The rope failed and the transfer hose became detached from the tank truck, causing the spillage. *Lessons learned*: • The absence of a leak-proof, permanent goose-neck system of piping, combined with a dry-coupling hose connection, resulted in a loose and unreliable connection. • The tank truck parking spot was not paved nor curbed for spill collection and/or containment, and so the liquid leaked directly into the soil. • SOPs had not been properly developed or implemented; these should have included specific instructions for visual inspections to be carried out of diesel transfer hoses before each use.
Chemical Handling and Transportation Procedures	*Description of incident*: A 200-litre drum containing a toxic and corrosive material had been placed on a wooden pallet onto a flat-bed truck; when the plastic stretch which was used to restrain the drum was cut by the logistics operator, the pallet fell to the ground and the contents were spilled. The release resulted in a liquid pool on the pavement, which evaporated, generating a toxic cloud that dispersed without any further ensuing consequences. The residual material on the pavement was flushed with firewater and collected for final disposal. *Cause*: Unknown to the logistics operator, a second operator on the opposite side of the truck, while unloading the cargo, had pushed the drums forward while trying to grab them with forklift clamps, resulting in the instability of

[71] United States Chemical Safety Board, www.csb.gov

Threat Type	Example of Event
	the unrestrained drums. Operating procedures in place at that time did not include precise instructions on how this kind of operation should be carried out, nor were procedures/instructions in place ensuring communication and coordination between the two operators during the execution of all tasks. *Lessons learned*: • The plastic wrapping around the drums should not have been cut prior to the removal of the pallets. • SOPs in force during the incident did not include step-by-step instructions on how such a procedure should be carried out, nor did they stress the need for continuous communication between operators.
Process Design	*Description of incident*: A powerful explosion and subsequent chemical fire killed four and injured 32 employees. It destroyed the facility, a solvent-blending operation. The explosion damaged buildings within one-quarter of a mile of the site. At the time of explosion, ethyl cyclopentadienyl manganese tricarbonyl (MCMT, CAS# 12108-13-3) was being manufactured. Following a report of a cooling problem by the process operator, one of the owners went to the control room to assist. A few minutes later, the reactor burst, then the contents exploded, killing the owner, the process operator, and the two operators who were exiting the reactor area. *Cause*: The investigation team discovered that a runaway exothermic reaction occurred during the first (metalation) step of the MCMT process. The batch recipe was tested to determine the most likely failure scenario. It was likely that the lack of sufficient cooling during the process resulted in the runaway reaction, leading to a rise in uncontrollable pressure and a temperature rise in the reactor. The pressure caused the reactor to explode, causing the contents to explode, and creating an explosion equivalent to 640 kilograms of TNT. *Lessons learned*: • The investigation team identified the root cause as the company's lack of awareness of the runaway reaction hazard associated with the MCMT it was producing. The investigation team also identified the following contributing causes: • The cooling system employed by the company was susceptible to single-point failures, due to a lack of design redundancy; and

Threat Type	Example of Event
	• The MCMT reactor relief system was incapable of relieving the pressure from a runaway reaction. The investigation team recommended that the subject of hazard awareness be added to the chemical engineering curriculum.

A.2 Security

Threat Type	Example of Event
Theft	*Case 1*: *Description of incident* Around 50 pallets of drugs (worth US $75 to 80 million) were stolen when thieves broke into a pharmaceutical warehouse. At the time of the incident, the building was shut down. There was no security fence and no security guard, but there were cameras and motion sensors in the facility. The thieves were able to get onto the roof; rappelled their way into an unmonitored area of the warehouse; and accessed the control room. They disabled the existing security system and lifted the boxes with drugs and loaded them into a tractor-trailer, which was parked at the loading bay in an area not covered by the surveillance cameras. *Lessons learned*: • Physical security systems should be strengthened (e.g., the company should increase its security fencing). • Additional surveillance cameras with expanded coverage should be put up (to cover all areas of the facility and its perimeter); these cameras should be manned. • In addition to surveillance cameras, human surveillance and security should be provided, especially during the hours when the facility is closed. • Sensitive and non-sensitive information which could be used during a robbery (such as floor plans and the location of control and computer rooms) should be protected and secured. *Case 2: Description of incident:* A driver of a truck filled with drums with different chemicals (including triethanolamine (CAS Registry Number® # 102-71-6) parked his truck near his house. Upon returning to his vehicle, the driver discovered that his truck had been stolen.

Threat Type	Example of Event
	Lessons learned: • Clear transportation procedures should be given to the logistical personnel of hazardous or scheduled chemicals (truck not be left unattended, etc.), so that personnel are aware of procedures. • The company should ensure that operators understand and follow the procedures related to chemical transportation, i.e., the company should ensure that personnel can perform/carry out the procedures. • The company should consider placing location-tracking equipment (GPS) and possibly dashboard cameras (dashcams) on its vehicles, especially on those carrying hazardous materials.
Terrorism	*Description of incident*: The incident occurred in a chemical facility producing strategic commodities. A group of terrorists, believed to have prior knowledge about the site plan, raided the employees' dormitory and the central processing facility. Explosive devices were planted by the terrorists throughout the periphery of the facility, and they then threatened to blow up the whole site if their demands were not met. The assailants, it would appear, were operating with previous knowledge about the company, and engaged in door-to-door searches looking for targeted employees. The attack resulted in loss of life of several employees. *Lessons learned*: • All employees and contractors working on site need to undergo background checks, and be screened for any previous criminal records and behavioural problems. • Rigorous and updated security-risk assessment tests need to be performed regularly and security protocols need to be updated and re-evaluated regularly in order to minimise potential risks and enable a quick and rapid response to any security attacks and/or abuses.
Trade-Secret Theft Cyber Crime	*Description of the incident*: An international chemical company lost millions of dollars due to the theft of confidential information through its former employees. A technology consultant contacted former employees in order to obtain relevant and detailed information about the plant and the chemical processes it used. Some of these former employees still had accurate information from the work they had previously carried out for the enterprise, particularly in terms of production processes. Based on the information that had been obtained, new chemical plants and processes were built and developed by the competitor, which exploited this confidential and valuable information, enabling it to obtain significant contracts and substantially increasing its profits.

Threat Type	Example of Event
	The chemical company sued the competitor. The individuals involved were convicted of economic espionage, possession of trade secrets, and cyber-attacks. *Lessons learned*: • Access to confidential information should be restricted and secure. • Varying levels of accessibility, that is, the classification of data in terms of its confidentiality, should be put into place and important information related to processes should be subject to layered controls. These levels should be graded and names and ultimately tied to how it will be protected, used, and transmitted. • In accordance with a country's legislation and company policies, human resources personnel should apply all relevant, security-related policies, including carrying out criminal background checks.
Sabotage	*Description of incident*: A chemical company was shut down for maintenance. At the same time the maintenance was being carried out, management decided to upgrade the CCTV in the plant site and some of the CCTVs were shut down. One night, an employee from Administration Branch, who assumed the CCTVs were shut down, entered the production area. He intentionally tore a bag that contained a chemical substance sensitive to air and moisture. He left the production area immediately after that. A few hours later, the chemical ignited and caused a fire in the production area, which resulted in a large loss to the company. The investigation revealed that the employee had been paid by a third party to tear the chemical bag in order to sabotage the facility. *Lessons learned:* • Monitoring of unauthorized personnel into the production area needs to be strengthened. • Guidelines for authorised staff also need to be strengthened to define who is allowed to go where and when. "Off-limits" areas should be strictly indicated. • The company should ensure that strict safety measures be followed, such as the proper storage of chemicals (in appropriate, sealed containers) and their separation.

Threat Type	Example of Event
	• Several layers of protection/control must be implemented in order to subject the materials to strict control and protection. Redundancy in security measures is recommended.
Know Your Customer	*Description of incident*: Drums of precursor chemicals were found at an illegal laboratory. Upon investigation, the police traced and identified the chemical supplier that had sold the chemical to a laboratory address. This supplier regularly conducts background checks on its customers, according to which it carries out financial checks and personal visits to ascertain whether the request for the product is legitimate, etc. It emerged that the chemicals had been purchased via the internet and that the customer had made a false declaration to the chemical supplier company. The precursor chemicals had been purchased for illegal purposes. *Lessons learned*: • The customer-checking system should be expanded to include analyses related to the use of the internet for purchasing dual-use chemicals. The capability of the company to detect suspicious sales over the internet should be enhanced through the definition of criteria and by making it mandatory for the company to refuse to make a sale if suspicions arise that the chemical might be used for illegal purposes. • The chemical supplier needs to strengthen its procedures related to risk assessment and customer background checking before precursor chemicals can be sold. • Highly suspicious cases should be reported to law enforcement bodies or agencies.
Attempt to Commit Robbery	*Description of incident*: Two burglars, apparently thinking that something valuable must be inside a one-meter-high safe, used an oxyacetylene cutting torch to burn through a metal and concrete barrier. The safe was filled with commercial-grade fireworks. As the heat from the torch went through the metal into the safe, the temperature rose until the safe violently exploded, sending lethal shards of shrapnel into the air and creating a violent and booming shockwave. The explosion was so massive that it caused the safe to soar through the air, ripping through the building before it landed outside. The two robbers died. *Lessons learned*: • Physical security should be strengthened, including adding additional perimeter protection to the site. Correct and specific information about highly hazardous chemical storage should be clearly posted in order to

Threat Type	Example of Event
	to discourage and deter any attempt to circumvent security systems to gain access to protected chemicals.
Online Purchases	*Description of the incident*: An individual was not only able to buy 3150 castor beans on the internet, but was also able to obtain detailed instructions how to produce ricin (CAS Registry Number® #9009-86-3) from the castor beans. He was able to buy equipment (every day kitchen items) to process the beans. When the police raided his home, they found 84.3 mg of ricin and the ingredients for a makeshift bomb, consisting of 250 metal balls, sharp glass objects, and pyrotechnical substances. They also found emails on his computer indicating that he had gathered information about in the properties of ricin and had tested the ricin on a hamster. The amount of ricin corresponds to roughly several hundred lethal doses, depending on the method of dispersal. He was caught because intelligence services had been monitoring his online purchases of a large quantity of castor beans from different sources. *Lessons learned*: • Online businesses are especially vulnerable to enabling the purchases of dual-use goods (because of the anonymity provided by internet sales). • It is essential that sales staff receive rigorous training in relation to spotting questionable transactions.

APPENDIX B: THE HAGUE ETHICAL GUIDELINES

B.1 Background

The **Hague Ethical Guidelines** were published in October 2015 in order to promote a discussion, on all levels of education, research, and practice, about the vital role that ethics play in relation to chemical disarmament and the promotion of the peaceful uses of chemistry. To promote a culture of responsible conduct in the chemical sciences and to guard against the misuse of chemistry, a group of chemical practitioners from around the world formulated a set of ethical guidelines that were based on the requirements of the Chemical Weapons Convention.[72]

The **Hague Ethical Guidelines** are intended to serve as the basis for the development of ethical codes and as discussion points for ethical issues related to the practice of chemistry under the Convention.

The OPCW encourages all stakeholders to refer to and promote the guidelines when debating the vital dimension of ethics in relation to chemical disarmament and non-proliferation and the broader issue of responsible scientific conduct.

B.2 Components of the Guidelines

Key elements: Achievements in the field of chemistry should be used to benefit humankind and protect the environment.

Sustainability: Chemistry practitioners have a special responsibility for promoting and achieving the UN Sustainable Development Goals of meeting the needs of the present without compromising the ability of future generations to meet their own needs.

Education: Formal and informal educational providers; enterprises; industry; and civil society should cooperate to equip anybody working in chemistry and others with the necessary knowledge and tools to take responsibility to work for the benefit of humankind; for the protection of the environment; and to ensure relevant and meaningful engagement with the general public.

Awareness and engagement*:* Teachers, chemistry practitioners, and policymakers should be aware of the multiple uses of chemicals, specifically their potential to be used as chemical weapons or as precursors. They should promote the peaceful applications of chemicals and work to prevent any misuse of chemicals; scientific knowledge; tools and technologies; and any harmful or unethical developments in research and innovation. They should disseminate relevant information about national and international laws, regulations, policies, and practices.

---

72 Organisation for the Prohibition of Chemical Weapons (OPCW), *The Hague Ethical Guidelines*, https://www.opcw.org/hague-ethical-guidelines

Ethics: To adequately respond to societal challenges, education, research, and innovation must respect fundamental rights and apply the highest ethical standards. Ethics should be perceived as a way of ensuring high quality results in science.

Safety and security: Chemistry practitioners should promote the beneficial applications, uses, and development of science and technology while encouraging and maintaining a strong culture of safety, health, and security.

Accountability: Chemistry practitioners have a responsibility to ensure that chemicals, equipment, and facilities are protected against theft and diversion and are not used for illegal, harmful, or destructive purposes. Chemical experts should be aware of applicable laws and regulations governing the manufacture and use of chemicals, and they should report any misuse of chemicals, scientific knowledge, equipment, and facilities to the relevant authorities.

Oversight: Chemistry practitioners who supervise others have the additional responsibility to ensure that chemicals, equipment, and facilities are not used by other employees for illegal, harmful or destructive purposes.

Exchange of information: Chemistry practitioners should promote the exchange of scientific and technical information relating to the development and application of chemistry for peaceful purposes.

APPENDIX C:LIST OF MULTIDISCIPLINARY EXPERTS[73]

Name	Title, Organisation, and Country
Adrian, Sven	Project Assistant, *Wuppertal Course on Loss Prevention and Safety Promotion in the Chemical Process Industries*, Germany
Aytbay, Aiday	Chief Ecologist, Sodium Cyanide Production, *Talas Investment Company*, Kazakhstan
Akmaral, Kenzhebayeva	Chief Quality Manager, *Kazphosphate*, Kazakhstan
Aluoch, Austin Ochieng	Lecturer, *Technical University of Kenya*, Kenya
Araya Barrantes, Juan José	Professor, *University of Costa Rica*, Costa Rica Member of the Drafting Committee
Arman, Karagaliyev	Environmental Specialist, *Kazphosphate*, Kazakhstan
Ashok, MID	Chemical Inspector, *National Authority*, Sri Lanka
Cooreman, Werner	Chief Security Officer, *Solvay Group*, Belgium
Dennehy, Mariana	Professor, *Universidad Nacional del Sur*, Argentina
Djibo Saley, Boubacar	Environment Section Head, *CNPC Niger Petroleum S.A.*, Niger
Fontejon Enarle, Gretchen	President, *Chemical Industries Association of the Philippines (SPIK), Sustainability Leader, Atlantic Coatings, Inc.*, Philippines Member of the Drafting Committee
Han Gi-Kim, Stephan	Vice-President, *Global Talent Management Institute*, Republic of South Korea
Gregoris, João Carlos	Process Safety Technology Leader, *Dow Chemical Company*, Brazil
Gulnar, Ilmaliyeva	Head of the Department of Chemical and Pharmaceutical Industry, *Ministry of Industry and Infrastructure Development of the Republic of Kazakhstan*, Kazakhstan
Hesselnberg, Lisa	Project Assistant, *Wuppertal Course on Loss Prevention and Safety Promotion in the Chemical Process Industries*, Germany
Kearns, Peter	Principal Administrator (Retired), *Organisation for Economic Co-operation and Development* (OECD) Member of the Drafting Committee
Kidwai, Syed Iqbal A.	Secretary General and CEO, *Pakistan Chemical Manufacturers Association*, Pakistan
Leech, Douglas	Technical Director, *Chemical Business Association* (CBA), United Kingdom of Great Britain and Northern Ireland

[73] Positions held by the contributors as at the end of 2019.

Name	Title, Organisation, and Country
Leksin, Alexey	Project Director, *Wuppertal Course on Loss Prevention and Safety Promotion in the Chemical Process Industries*, Germany
Männig, Detlef	Chairperson of the Chemical Industry Coordination Group OPCW/ICCA, *International Council of Chemical Associations*, Managing Director, *Männig Consulting*, Germany Member of the Drafting Committee
Nahar, Luftun	Staff Officer (Chemist), *Bangladesh Navy and Former Staff Officer, National Authority for Implementation of the Chemical Weapons Convention*, Bangladesh
Nelson, Andrew Wyatt	Senior Member of the Technical Staff, *Sandia National Laboratories*, United States of America Coordinator of the Drafting Committee
Pomares, Miguel Juan Albaladejo	Chemist & Chemical Engineer, *Head of Fire Brigade-Hazmat Unit, Leganés*, Spain
Quiblier, Pierre	Programme Officer, *United Nations Environment Programme* (UNEP) Member of the Drafting Committee
Ranghieri, Massimo Claudio	Consultant, *National Research Council*, Italy Member of the Drafting Committee
Reniers, Genserik	Professor, *Delft University of Technology*, Belgium
Sany, Mohamed Noor	Chairperson of the Safe Road Committee, *Chemical Industry Council*, Malaysia
Sehailia, Moussa	Senior Research Scientist/Team Leader, *Centre de Recherche Scientifique et Technique en Analyses Physico-Chimiques (CRAPC)*, Algeria
Tang, Cheng	Chairperson, OPCW Scientific Advisory Board, China Workshops Facilitator and Member of the Drafting Committee
Yerlan, Kudashev	Head of Ammonia Production, *KazAzot*, Kazakhstan
Yernar, Kuanyshbayev	Expert of the Department of Chemical and Pharmaceutical Industry, *Ministry of Industry and Infrastructure Development of the Republic of Kazakhstan*, Kazakhstan
Zuber, Muhammad Setyabudhi	Secretary-General and Senior Executive Director, *Responsible Care® Indonesia (RCI) and Vice-Chairperson for International Affairs Federation of the Indonesian Chemical Industry (FIKI)*, Indonesia Member of the Drafting Committee

- - - o - - -

OPCW

Organisation for the Prohibition of Chemical Weapons