International Standard

ISO 5665

First edition
2024-04

Consumer incident investigation — Requirements and guidance

Analyse des incidents affectant les consommateurs — Exigences et recommandations

Reference number
ISO 5665:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Project Committee ISO/PC 329, *Consumer incident investigation guideline*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The objective of this document is to provide a process to any person or any organization of any size, whether it is public, private or not-for-profit, to investigate consumer incidents in order to prevent them from occurring in the future.

To prevent incidents from recurring, it is essential to conduct incident investigations that can lead to effective measures.

Some manuals and guides describing the principles and methods of incident investigation already exist in many fields (e.g. the aviation industry). Even though the fields are different, the literature have a common investigative purpose – to analyse the causal factors leading to the incident and propose preventative measures.

However, the development of effective incident investigation guidelines has yet to include incidents that affect consumers involving the use of products, services or facilities. These incidents can occur anywhere.

This document focuses on the investigation of consumer incidents. Thus, the incident investigation organization can trust other organizations conducting investigations according to this document. It would activate data sharing, respecting confidentiality policy or regulation, among organizations including full and complete data and related information on consumer incidents. This document encourages the full and complete sharing of information arising from an investigation, including the final report and all of the data developed during the investigation.

Consumer incident investigation — Requirements and guidance

1 Scope

This document provides general requirements and recommendations on the principles, procedures, and methods for investigating incidents where there have been injuries, illnesses, damage to health, fatalities to consumers, damage to property or environmental damage related to the use of products, services or facilities by consumers.

NOTE 1 These incidents can occur anywhere.

This document is applicable to any person or any organization of any size, whether it is public, private or community-based.

NOTE 2 This document is not limited to incidents while products, services or facilities are in use, but also includes incidents that occur when products, services or facilities are not in use, such as during transportation or storage by consumers.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
causal factor
condition, event, omission, deficiency or action that contributed directly to the incident

3.2
conflict of interest
situation where business, financial, family, political or personal interests can interfere with the impartial judgment of persons in carrying out their duties for the *incident investigation organization* (3.10)

3.3
consumer
individual member of the general public purchasing or using products, services or facilities for private purpose

[SOURCE: ISO 26000:2010, 2.2, modified —"property" was deleted from the definition "facilities" has been added to the definition.]

3.4
consumer incident
incident
occurrence, condition or situation that resulted in, or can result in injuries, illnesses, damage to health, or fatalities to *consumers* (3.3), damage to property, or an environmental damage related to use of products, services or facilities by consumers

Note 1 to entry: The term "accident" is used in some sectors as a synonym for incident but it is not used synonymously in this document.

3.5
consumer incident investigation
incident investigation
investigation
series of processes to collect as much *data* (3.6) as possible related to the incident to be investigated, to understand the events that occurred, to analyse the factors, to identify or estimate the causes and factors of the incident, and to develop and submit *recommendations* (3.13) on measures to prevent the incident from recurring

3.6
data
information collected during the course of an investigation for reference or analysis

Note 1 to entry: Data can be in, but is not limited to, the following forms: documents, records, dictations, interview transcripts, photographs, videos, materials, instruments, tools, statistical information, analytical results, research data, papers, hospital records and coroner's records, social media posts.

Note 2 to entry: Data can include discovery of non-incident related data that, although not directly related to the incident, can potentially pose a hazard or identify a deficiency.

[SOURCE: CSA Z1005-17:2017, 3.1]

3.7
direct cause
last *causal factor* (3.1) in the chain of causation leading to the incident

Note 1 to entry: There can be more than one direct cause.

3.8
harm
injury or damage to the health of people, or damage to property or the environment

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

3.9
human error
discrepancy between the human action taken or omitted, and that intended or required

[SOURCE: IEC 62740:2015, 3.1.10]

3.10
incident investigation organization
organization whose purpose is to conduct *consumer incident investigations* (3.5)

3.11
incident investigation team
people assigned by an *incident investigation organization* (3.10) to perform *consumer incident investigations* (3.5)

3.12
reasonably foreseeable misuse
use of a product or system in a way not intended by the supplier, but which can result from readily predictable human behaviour

[SOURCE: ISO/IEC Guide 51:2014, 3.7, modified — Notes 1 and 2 to entry have been deleted.]

3.13
recommendation
advice to the relevant department or organization regarding matters identified as needing to be corrected to prevent recurrence as a result of the incident investigation

Note 1 to entry: Corrective actions to remove potential for *harm* (3.8) and to reduce *risk* (3.14) can include, but are not limited to: additional product or facility redesign, instructions, warning statements, signage, service procedures, training for service providers and organizational management issues.

3.14
risk
combination of the probability of occurrence of *harm* (3.8) and the severity of that harm

[SOURCE: ISO/IEC Guide 51:2014, 3.9, modified — Note 1 to entry has been deleted.]

3.15
root cause
causal factor (3.1) or *underlying factor* (3.17) with no predecessor, that is relevant for the purpose of the investigation

Note 1 to entry: An incident normally has more than one root cause.

3.16
safety
freedom from *risk* (3.14) which is not tolerable

[SOURCE: ISO/IEC Guide 51:2014, 3.14]

3.17
underlying factor
condition, event, omission, deficiency or action that contributed indirectly to the incident

Note 1 to entry: Underlying factors are factors, if eliminated, that would not necessarily prevent the incident, but can help prevent future incidents.

Note 2 to entry: Underlying factors include management and organizational factors.

Note 3 to entry: Some documents apply the term “contributing factor” to this definition.

3.18
vulnerable consumer
consumer (3.3) who can be at greater *risk* (3.14) of *harm* (3.8) from products, services or facilities due to their demographic, level of literacy, physical condition or limitations, or inability to access product *safety* (3.16) information

[SOURCE: ISO 10377:2013, 2.30, modified — “services or facilities” has been added and “age” has been replaced by “demographic” in the definition.]

4 Principles of consumer incident investigation

4.1 General

The incident investigation process described in this document is shown in Figure 1. Each stage in the process is discussed in detail in the subclauses of Clause 4. Figure 1 includes the relevant clause numbers at each step to help find the relevant information.

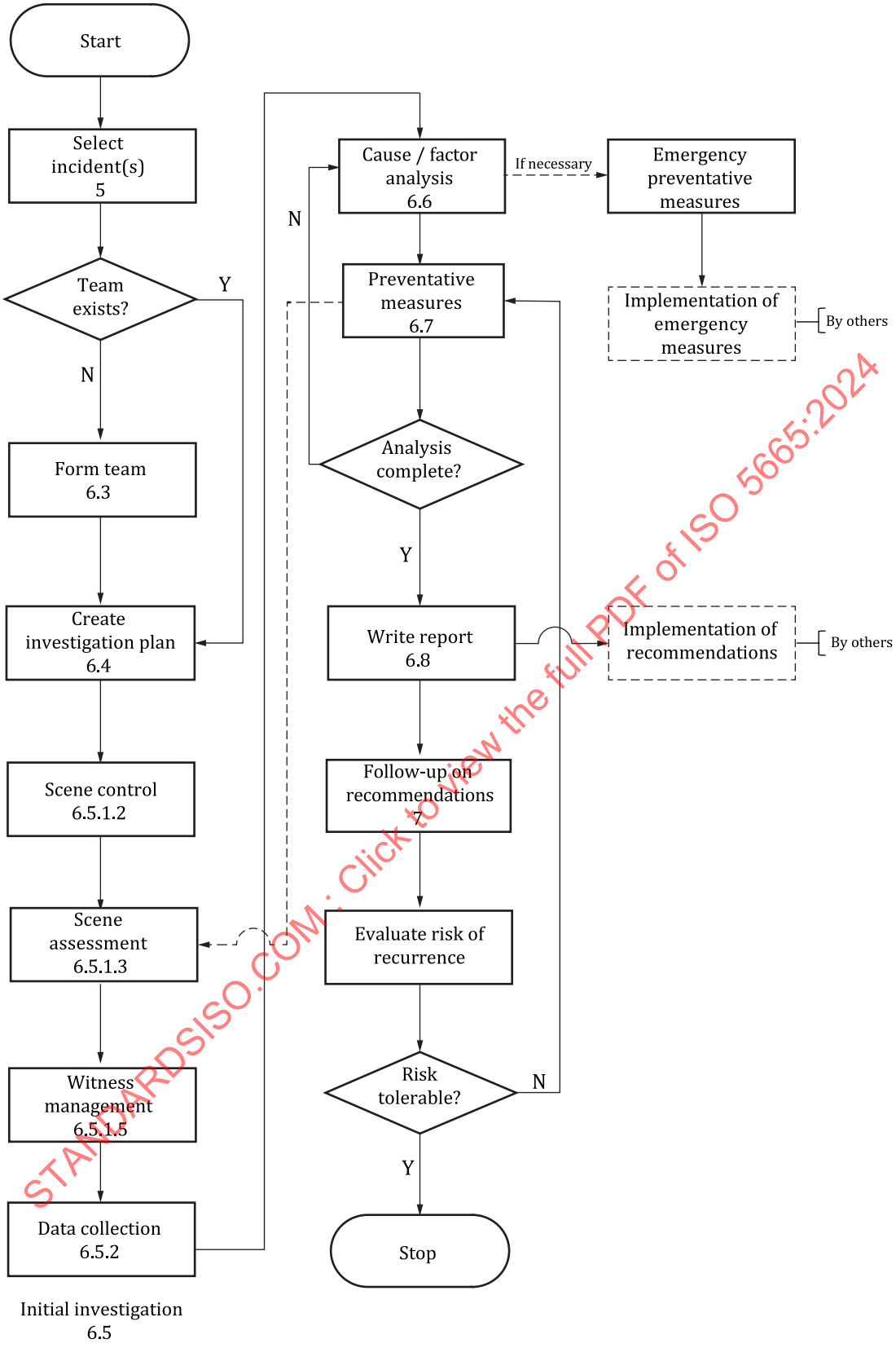


Figure 1 — Consumer incident investigation process

4.2 Objective

The sole objective of the investigation of an incident is the prevention of further incidents. It is not the purpose of this activity to apportion blame or liability.

4.3 Mission

The mission of an incident investigation team is the identification of hidden risk factors, improvement of the safety of the organization, prevention of the recurrence of incidents widely and ultimately to contribute to the advancement of safety in society.

The mission of the incident investigation team is encapsulated in these goals:

— the analysis of the causes and factors related to the incident under investigation,

— the determination of safety measures to prevent the recurrence or to reduce the severity of the same or similar incidents,

— to make recommendations to the organization, department regulatory authorities, standardization bodies and those involved in the incident where appropriate, and

— to verify the results after making recommendations.

Through these activities, the incident investigation can contribute to the improvement of consumer safety.

In addition to investigating the cause of the incident, the mission shall clarify the factors contributing to the increase in damage.

NOTE See ISO/IEC Guide 51:2014, 4.1 and 4.2 for guidance on the use of the terms “safety” and “safe”.

The incident investigation team shall achieve the mission goals by following the evidence as far as possible before coming to any conclusions.

Recommendations shall include at least one of the following two types:

a) measures to prevent recurrence in a narrow sense: measures to prevent the recurrence of the same or similar incidents based on the various factors constituting the cause of the incident;

b) measures to prevent recurrence in a broader sense: measures to eliminate organizational and system risk factors (dangerous events such as oversights, defects and the existence of triggers for human errors in various aspects from design to maintenance and operation) that revealed during the investigation, even if they are not related to the cause of the incident.

The conclusion of the incident investigation report shall reflect the purpose of the investigation.

4.4 Incident investigation organization and incident investigation team characteristics

4.4.1 General

Effective incident investigation organizations and incident investigation team share certain common characteristics. These teams shall have the minimum characteristics as described in 4.4.2 to 4.4.5.

4.4.2 Independence

The incident investigation team shall be independent.

The incident investigation team shall be able to conduct its own investigation and make its own judgments without influence from any source whose mission is different than described in this document. To ensure independence, the incident investigation team shall have the necessary authority to investigate the incident.

4.4.3 Impartiality

The incident investigation organization and the incident investigation team shall maintain impartiality during an investigation and the delivery of the investigation report.

To maintain impartiality, the incident investigation organization and team shall avoid influence by organizations or individuals who can have a stake in the outcome of the investigation.

The actions of the incident investigation organization and the incident investigation team during the investigation shall not raise any suspicion that such influence has occurred.

4.4.4 Expertise

The incident investigation team shall include members with the required expertise to conduct the investigation.

The expertise of incident investigation team members should include expertise in the following areas:

— relevant technical fields, e.g. product or service, sustainable development, economy,

— incident investigation techniques and methods,

— information collection,

— data analysis,

— human factors, and

— medical.

Over-reliance on expertise can lead to overlooking the perspectives and targets that are necessary for the investigation. To avoid these effects, the perspectives of non-experts, such as victims of incidents, should be taken into consideration during the investigation. See 4.5.

4.4.5 Resources

The incident investigation team shall be provided with sufficient resources to complete the investigation in an effective and efficient manner.

The resources can include:

— personnel,

— time,

— funding,

— technical and physical resources,

— access to the incident site,

— access to witnesses identified during the initial assessment of the incident,

— access to data and records related to the incident, and

— data and records from national and international sources.

4.5 Respect for victims and victims' families

The understanding developed through the incident investigation is not possible without the involvement of the victims in the incident. The victim's viewpoint is particularly useful in discovering factors leading to increased damage and in developing measures to reduce or eliminate it in future.

The victims and the families of the victims shall therefore be given the highest level of respect and they should be treated as important parties in the incident during the investigation.

Information and explanations should be provided to the victims and their families so that they do not feel alienated by the incident investigation team or the investigative processes used.

NOTE This subclause only addresses the respecting of the dignity of the victims, the victims' families and their unique insights.

5 Incidents to be investigated

The selection of incidents to be investigated shall take the following into consideration.

— Select consumer incidents in which the degree of harm is serious or likely to be serious, or in which a wide range of consumers have been or are likely to be harmed, even if the degree of harm is not serious. In the case of an incident caused by so-called "misuse" by a consumer, the scope of reasonably foreseeable misuse (see ISO/IEC Guide 51) should be considered as broadly as possible. Even in cases where products, services, etc. do not appear to present significant risk to consumers, beneficial findings can be obtained by conducting incident investigations to prevent the recurrence of incidents due to "misuse".

— Any recognized risk assessment methodology can be used to evaluate the risk associated with incidents being considered for investigation. These methods include all suitable quantitative or qualitative methodologies, e.g. risk matrices, risk graphs. Figure 2 is an example of a risk matrix.

			Harm level				
			Fatal	Hazardous	Severe	Minor	Negligible
			A	B	C	D	E
Probability	Extremely frequent	5	5A	5B	5C	5D	5E
	Relatively frequent	4	4A	4B	4C	D4	4E
	Not frequent	3	3A	3B	3C	3D	3E
	Rare	2	2A	2B	2C	2D	2E
	Extremely rare	1	1A	1B	1C	1D	1E

Key

risk level: high

risk level: medium

risk level: low

Figure 2 — Example of a risk matrix

6 Conducting an incident investigation

6.1 Terms of reference

The incident investigation organization shall set the terms of reference before assembling an incident investigation team.

The person designated to lead the incident investigation team shall ensure that the terms of reference are met.

The terms of reference shall include at least the following information:

— the authority to investigate incidents, i.e. who or what has granted the incident investigation team the authority to investigate the incident(s), e.g. consumer residences, medical records or other properties;

— the scope or jurisdiction of authority;

— a statement of independence and impartiality;

— resources available for investigative purposes and the authority to requisition the resources;

— the budget or financial constraints, if any;

— time constraints, if any, including any set term of existence for the incident investigation team;

— a list of stakeholders in the incident;

— the designation of incident investigation team members, including at least the incident investigation team leader; incident investigation team members may include co-leaders or deputy leaders as, appropriate, to facilitate administration and management of the investigation;

— the person or entity to which the incident investigation team reports.

The terms of reference shall be documented and included in the investigation file.

6.2 Investigation flow

The basic flow of the recommended incident investigation shall be as follows:

a) form an incident investigation team,

b) create of an incident investigation plan,

c) do initial incident investigation and data collection,

d) conduct cause and factor analysis,

e) formulate preventive measures,

f) prepare an incident investigation report.

6.3 Forming an incident investigation team

6.3.1 General

An incident investigation team with the necessary expertise, impartiality and neutrality shall be formed to collect relevant data, analyse causes and factors, and evaluate the results of the analysis.

The incident investigation team shall have the characteristics, expertise and qualifications as described in 6.3.

6.3.2 Expertise and skills of incident investigation team members

The incident investigation team members shall, where possible, have the expertise in the following areas:

— methods of information collection, analysis and trend analysis,

— knowledge of the concept of safety aspects,

— knowledge of risk assessment and risk management,

— knowledge of the concept of organizational and system incidents,

— knowledge of human factors,

— expertise on individual products and services related to the incident that occurred should be available, but can be sought outside the team, and

— knowledge about foreseeable misuse and the vulnerability of consumer.

Persons identified for potential membership in the incident investigation team shall provide the incident investigation team leader with their credentials as part of the selection process. The credentials of those selected for the incident investigation team should be included in the investigation file.

NOTE 1 Readily predictable human behaviour includes the behaviour of all types of human beings, e.g. the elderly, children and persons with disabilities. For more information, see ISO 10377.

NOTE 2 A trend is emerging to discard the term “misuse” in favour of the term “reasonably foreseeable use”.

6.3.3 Conflicts of interest

To help ensure that the incident investigation team is independent and impartial as required by 4.4.3, the people selected as incident investigation team members shall declare potential and explicit conflicts of interest.

When a prospective team member is found to have a conflict of interest with the investigation, that person’s membership in the incident investigation team shall not be accepted.

Where there are only few experts in the given field and they have a conflict of interest, the incident investigation team shall obtain knowledge of the field by interviewing said experts. The incident investigation report shall be reviewed and commented by said experts of the field. Their comments shall be included in the incident investigation report.

The criteria for the determination of a conflict of interest shall be determined in advance. The criteria for conflicts of interest shall be set by the incident investigation organization setting the terms of reference for the incident investigation team or by the incident investigation team leader.

The fact that an incident investigation organization receives a mandate from an interested party in the incident (e.g. the manufacturer, a competitor) does not constitute a conflict of interest.

6.3.4 Documentation

The incident investigation team leader shall ensure that a list of incident investigation team members is compiled. The list shall include at least the following information for each member:

— name,

— contact information (mobile phone number, email address),

— area(s) of expertise, and

— credential(s).

The list shall be documented and included in the investigation file.

6.4 Creating an incident investigation plan

The incident investigation team shall prepare an incident investigation plan specific to each incident. The plan can include, but is not limited to, identifying and managing the following elements:

a) incident scene access;

b) incident investigation team health and safety;

c) joint or concurrent investigations;

d) data requirements;

e) where and how the data will be obtained and maintained;

f) data preservation.

The incident investigation plan shall be documented and included in the investigation file.

6.5 Initial investigation and data collection

6.5.1 Scene management

6.5.1.1 General

If the incident site is not under the control of the incident investigation organization to which the incident investigation team belongs, such as private residence, there is a possibility that the incident investigation team can be required to coordinate the investigation with those who have control of the site. There is a possibility that scene management is unnecessary or impossible.

When an investigation in a private residence is foreseen, the incident investigation team shall obtain permission from the victim or the victim's family and the size of the team should be limited to the smallest size practicable.

NOTE Such an investigation can involve entering a private residence and obtaining personal medical information.

6.5.1.2 Scene control

The incident scene shall be effectively controlled, as much as possible. Scene control measures shall include at least the following.

a) Secure the scene and appropriately preserve all evidence.

b) One member of the incident investigation team shall be designated to control access to the scene. When appropriate, an additional team member may be delegated to provide relief to the primary scene control member.

c) All incident investigation team members who have reason to enter the scene to conduct their part of the investigation shall be permitted to enter the scene by the designated scene control member or their delegate.

d) The name and contact information, i.e. mobile phone number and email address, of each person entering the incident scene shall be logged by the designated scene control member or their delegate when the team members enter and exit the scene.

6.5.1.3 Scene assessment

The incident investigation team shall, if relevant, perform a scene assessment. If the initial scene assessment was done by others, a copy of the scene assessment documentation shall be obtained, if possible, and reviewed by the incident investigation team.

If no scene assessment was completed, or the scene assessment documentation is not available for any reason, this fact shall be noted in the incident investigation documentation.

If the scene assessment can be completed, it shall be documented and included in the investigation file.

The scene assessment shall at least include:

a) performing a hazard identification and risk assessment (see 6.5.1.4);

b) effectively controlling risk to ensure the safety of the incident investigation team;

c) verifying the initial incident information, and evaluating new, different or changing circumstances that can require additional or specialized resources to respond, and, if necessary, to modify the incident investigation plan.

6.5.1.4 Scene-specific risk assessment

The incident investigation team shall identify the hazards present at the scene and shall assess the risk to all aspects of the incident investigation team members' occupational health and safety, including:

— physical hazards,

— chemical hazards,

— biological hazards,

— psychological hazards,

— electrical hazards,

— radiation hazards, and

— fire and explosion.

Risks arising from the identified hazards shall be assessed in a documented risk assessment, and appropriate risk mitigation measures shall be used to protect the incident investigation team members (see Annex C).

6.5.1.5 Witness management and support

The incident investigation team shall, where possible, manage and support witnesses by:

— ensuring that witnesses are provided medical and psychological support as can be required;

— limiting interaction between witnesses to the greatest extent possible;

— limiting witness access to outside news sources or other sources of information or communication until they have been interviewed to prevent tainting their recollections;

— interviewing witnesses in a timely manner to help ensure that witness recollections of the incident are fresh, see 6.5.2.

Witness interviews shall, when possible, be conducted by incident investigation team members with expertise in interviewing techniques. The use of interview checklists can guide and support this process by ensuring that key points are covered. Interviews should not be limited by the content of any checklists used.

6.5.2 Data collection

The incident investigation team shall collect as much data as possible, relevant to the incident factors to objectively understand the events that have occurred.

The data collected can include:

— scene conditions,

— temporal conditions, e.g. time of day, year, season,

— environmental conditions, e.g. temperature, humidity, barometric pressure, weather conditions, altitude, pollutants,

— physical materials (products, equipment, tools, objects showing damage, etc.),

— interview records,

— documents and records related to the incident,

— photos and video recordings,

— statistical information, analysis data, research data, papers, etc.,

— type and vulnerability of consumer (intended or unintended user),

— information about foreseeable use or misuse from stakeholders,

— behaviour in incident, including protective behaviour,

— probability of exposure,

— incident history involving the product, service or facility in question, and similar products, service or facilities,

— documentation or test reports showing compliance to International Standards specific to the product, service or facility in question, and

— documentation of the risk assessment done by the organization responsible for that product, service or facility.

NOTE 1 Perishable or changeable evidence can require documentation and immediate preservation.

All evidence collected should be logged at the scene and maintained in safe custody for such a period as can be required for the purpose of the investigation.

NOTE 2 Since people's memories change over time due to news reports, conversations with others, etc., interviews with witnesses can require documentation as early as possible.

6.5.3 Data validation

Data shall be validated. Data validation shall, where possible, include at least the following:

a) examining the validity and accuracy of the data;

NOTE 1 Data can be validated by finding corroborating information or by examining conflicting data, where it exists.

b) identifying and documenting any assumptions and constraints related to the data;

NOTE 2 Assumptions can include the degree of confidence in the accuracy of the data.

c) addressing any gaps or deficiencies in the data and, where possible, obtaining additional data to close the gaps.

6.5.4 Experiments

It is recommended that experiments in relevant fields be conducted if they are deemed necessary or useful for cause and factor analysis.

The experiments conducted shall be documented in a report and shall contain as much detail as possible, including hypotheses, experimental method(s), experimental results and experimental data summary.

No additional harm should be caused by these experiments.

6.6 Cause and factor analysis

6.6.1 Perspectives on cause and factor analysis

An incident investigation can be described as an ex post facto risk assessment. The purpose of cause and factor analysis is to identify causes and factors that should be eliminated from various aspects. The causes and factors to be eliminated correspond to hazards (including hazardous situations and events) with risk that is not tolerable in risk assessment. See ISO/IEC Guide 51:2014, Figure 2.

Incident cause and factor analysis shall include all matters leading to the prevention of an incident. Therefore, it is essential to analyse the causes and factors of the incident as deeply and broadly as possible and analyse the complex factors, rather than just identifying the direct cause of the incident, such as human error, machine defects or malfunctions. In other words, it is crucial to extract not only the direct cause but also the causal factors, underlying factors and root causes. In this context, the analysis includes the events that occurred, human factors, organizational culture and rules, and industry practices, standards and regulatory requirements.

All possible causes and factors shall be considered without preconceptions. It is recommended that no conclusion shall be drawn until all the information has been analysed.

In the case of product incidents and incidents involving the use of facilities, in which consumer decisions and responses based on those decisions often intervene before an incident occurs, it is important to understand the actual conditions of use by consumers as they are, and to conduct analysis based on that understanding.

It is important to analyse not only the cause and the factors associated with the occurrence of the incident, but also the factors that led to the increased damage.

Even in the most seemingly straightforward incidents, seldom, if ever, is there only a single cause.

For example, an investigation that concludes that an incident was due to persons' carelessness, and goes no further, has failed to seek answers to several important questions such as:

— Was the person's attention distracted? If so, why?

— Were the safety procedures being followed? If not, why?

— Were the safety devices in order? If not, why?

— Was the product or device designed to take into account human factors, the challenges faced by vulnerable consumers and the foreseeable use?

— In the case of service providers and maintenance workers, were the workers properly trained? If not, why?

Humans tend to make errors even when they are paying attention. An investigation that answers these and related questions will, in most cases, reveal conditions whose correction will be easier and more effective, providing better solutions than simply attempting to prevent "carelessness."

An example of investigative failure is the conclusion that an incident was due to faulty equipment (e.g. a malfunctioning elevator), but the incident investigation team members fail to look further for underlying factors such as:

— Why was the fault not spotted during routine maintenance inspections?

— Were there any earlier symptoms of the fault?

— Were the symptoms of the fault reported? If so, why was the fault not corrected immediately?

These and any other relevant avenues shall be explored to ensure that the conclusions identify all causes and factors.

Similarly, in the case of an amusement park ride incident, an investigation will fail if the conclusion is simply that the incident was caused by operating the ride during adverse weather conditions. Avenues that should have been explored include:

— Why was management allowed to continue in such adversity?

— Why were no special supervision, equipment or other measures introduced to remove the risk to managing in such adversity?

NOTE See ISO/IEC Guide 51 for safety aspects, and ISO/IEC Guide 50 and ISO/IEC Guide 71 for addressing accessibility in standards.

6.6.2 Cause and factor analysis techniques

The data collected in 6.5.2 and 6.5.4, shall be analysed, taking into account the perspectives in 6.6.1.

a) Summarize the incident events and the overall events related to the incident, and organize the order of the events.

b) Select the methodology to be applied for the factor analysis; it is recommended to use several models for the analysis, not only one factor analysis model (see Annexes A and B).

c) Identify or estimate the direct causes or causal factors of the incident that shall be eliminated. One of the methods of factor analysis that can be used to find the direct causes and causal factors is the variation tree analysis (VTA), see Clause A.2.

NOTE Once the direct causes and direct factors are analysed, if it is necessary to implement emergency preventive measures to deal with them, a recommendation can be made to the relevant organization or department to implement the measures without waiting for the final report to be formulated. Emergency preventive measures can include product recalls, suspension of equipment used in services and suspension of use of facilities. The investigation process is then continued.

d) Identify or estimate the underlying factors. Examples of factor analysis methods that can be used to find the underlying factors are Why-why analysis and M-SHEL analysis. The analysis methods can be used singly or sequentially (see Clauses A.3 and A.4).

e) Root causes should be identified or estimated by expanding the perspective to include management factors and organizational factors in turn. An example of the root cause analysis method is J-RCA. This is a method for clarifying root causes by combining the above-mentioned VTA analysis, Why-why analysis and M-SHEL analysis (see Clause B.2).

Examples of organizational factors are listed below; their presence or absence depends on the type and scale of the business:

— business management factors;

— intermediate management factors;

— technical factors;

— climate and psychosocial factors;

— external environmental factors;

— individual and group factors;

— statutory, regulatory and market surveillance factors.

There can be more than one organization for which organizational factors are examined.

6.7 Risk reduction measures to prevent recurrence

Recommendations on preventive measures are made to encourage the organization to receive the recommendation to implement the risk reduction process in the risk assessment and risk reduction process flow. See ISO/IEC Guide 51:2014, Figure 2.

For each cause or factor identified in the analysis that needs to be eliminated, measures to reduce the risk shall be formulated, summarized and recommended, taking into account effectiveness, certainty, economy and permanence.

The risk reduction measures included in the recommendation should not be too concrete, since it is the organization receiving the recommendation that actually repeats the risk reduction process until that risk becomes tolerable.

The recommendation shall state that the risk reduction measures implemented by the organization receiving the recommendation shall apply the three-step method of ISO/IEC Guide 51 when they relate to the design of products, machinery, facilities, etc.

Recommendations for risk reduction shall be referred to the authority having jurisdiction or another appropriate body.

NOTE 1 Risk factors that are revealed in the process of analysis, can include, but are not limited to: oversights, inadequacies, defects, triggers for human error and others at each stage from design to maintenance, operation and management.

NOTE 2 In some cases, such as for small organizations, the investigation entity and the entity implementing the recommendations can be the same.

6.8 Incident investigation report

6.8.1 General

An incident investigation shall be documented in a report.

The report shall be compiled so that the purpose of the investigation, its contents, and recommendations for preventing recurrence are clearly and comprehensibly communicated to the incident stakeholders, including the victims of the incident and the organization responsible for implementing the recommendations.

The report shall:

— convey the purpose of the investigation and the significance of the selection of the incident to be investigated;

— identify the types of methods and models used in the analysis, explain the analysis process, and demonstrate their adequacy;

— provide conclusions about causes and factors;

— when there is insufficient scientific data on technical or other issues, point out the inadequacy of the data and indicate the scientific research agenda that is expected to be undertaken.

6.8.2 Structure of the incident investigation report

The incident investigation report shall include at least the following information, as applicable:

a) a synopsis of the investigation;

b) factual data including

   1) a description of the incident including date, time, location and preceding events,

   2) the incident investigation team member list and their credentials,

3) supporting documentation and records, where they can be found and if applicable,
4) either diagrams or photographs, or both,
5) assumptions and constraints, and
6) a list of all the evidence excluded from the investigation with rationale for the exclusion;

c) experimental description and results including
1) hypothesis,
2) experimental method,
3) experimental results, and
4) experimental data summary;

d) an analysis including
1) a description of the analysis process utilized,
2) direct causes, causal factors,
3) underlying factors, and
4) root causes;

e) results of and conclusions drawn from the investigation, including
1) conclusions about the factors of the incident, and
2) factors that need to be corrected (factors to be eliminated);

f) recommendations on preventative measures;

g) recommendations for corrective actions for each factor that needs to be corrected (removal of factors);

h) an annex containing the evidence log for all evidence used in the investigation.

The investigation report shall be included in the investigation file.

7 Follow-up on recommendations

The incident investigation team shall make sure that there is an entity in place (e.g. a dedicated organization or governmental authorities) to confirm whether the recommendations for preventing recurrence have been implemented, risks have been sufficiently reduced and the recommendations have sufficiently contributed to preventing recurrence and improving safety.

It is recommended to iterate until the risk of an incident occurring can be judged to be tolerable (see Figure 1).

Annex A
(informative)

Factor analysis methods

A.1 General

A wide variety of factor analysis methods are available. Most of those can be categorized as follows:

— Factor classification type: This is a method of identifying direct causes underlying factors in a certain format. It is suitable for relatively simple or small-scale incidents where the factors can be considered independently of each other. In the case of complex or large-scale incidents, it is recommended to combine it with another method for detailed analysis.

  Examples of the factor classification type: software, hardware, environment and liveware (SHEL) model, management-SHEL (M-SHEL) model and cognitive reliability and error analysis method (CREAM).

— Process-related type (tier type): This type focuses on the process that leads to the incident and to the changes in the relationships among factors, to aid in the assessment of the full scope of the events related to the incident. It is useful in uncovering important factors in delving further into the underlying factors, thus arriving at effective measures.

  Examples of process-related types (tier type): fault tree analysis (FTA), variation tree analysis (VTA), systematic approach to error reduction (Safer) and 5 whys or Why-why analysis.

This annex describes VTA, Why-why analysis and M-SHEL model, which do not require a high level of expertise and are relatively easy to apply. By using these three methods in this order to analyse a single incident, it is possible to find out not only direct causes an/or causal factors but also the underlying factors, and derive multiple preventive measures.

In addition, in the case of a relatively large or complex incident, when a retrospective analysis to determine the root cause, including organizational factors, is required, it is recommended to use the root cause analysis method, Japan institute of human factors-root cause analysis (J-RCA) (see Annex B). The J-RCA also uses the above three methods in its process.

A.2 Variation tree analysis

A.2.1 Overview

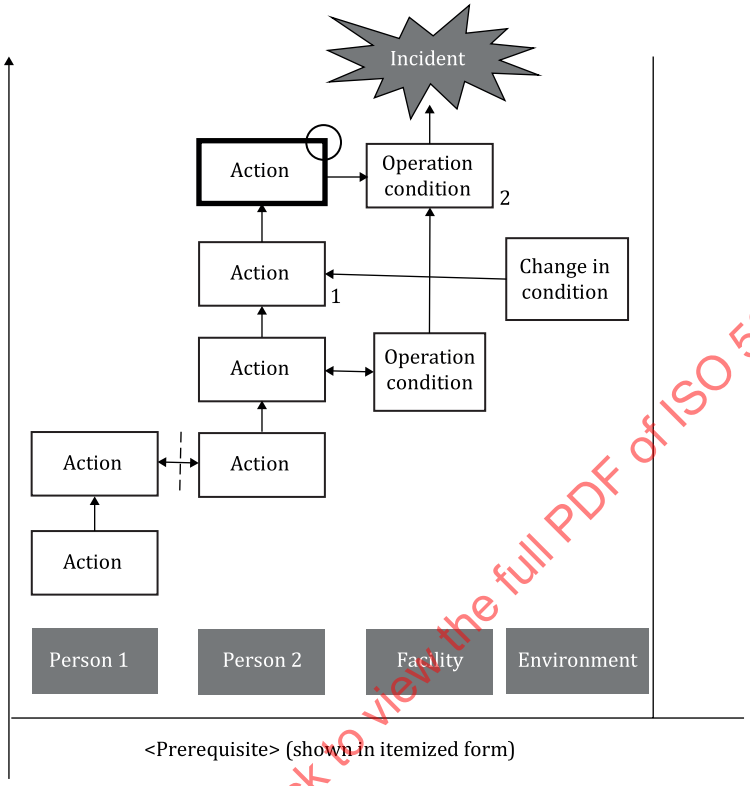
VTA is an analytical method based on the idea that unusual behaviours or conditions that occur are the factors that eventually lead to an incident or serious event. Events are shown in a tree-like diagram that follows the chronological course of time, and the overall process is visually understood and analysed. It is highly effective in understanding how factors interact with each other in a complex manner as time passes and in identifying the direct cause and/or causal factors.

However, it is difficult to develop countermeasures regarding complex events with VTA alone. It is to be combined with Why-why analysis (see Clause A.3) and M-SHEL analysis (see Clause A.4) as needed to further investigate the factors and arrive at effective countermeasures.

A.2.2 Structure of the VTA diagram

A.2.2.1 General

Based on the information gathered, the events that took place over time are written inside rectangles as nodes. The nodes are then positioned in chronological order and connected with arrows based on their relationships in order to create a VTA diagram.



<Explanation>

1 (Provide the corresponding supplemental explanation.)

2 (Provide the corresponding supplemental explanation.)

SOURCE: Human Factors - Creating a Safe Society, Japan, reproduced with the permission of the authors.

Figure A.1 — Basic VTA diagram

A.2.2.2 Vertical and horizontal axes

A.2.2.2.1 Items on the horizontal axis

Factors such as relevant entities, facilities, equipment or environment and other factors related to the incident to be analysed are placed along the axis. (The selection of pertinent factors should refer to the M-SHEL model explained in M-SHEL analysis for effectiveness, see Clause A.4.)

A.2.2.2.2 Items on the vertical axis

This is the time axis, in which passage of time is shown to start from the bottom upwards. If possible, enter the date or time (hour/minute/second, etc.).

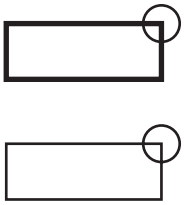
A.2.2.3 Nodes

Events and conditions related to the incident, such as the behaviour of a relevant entity, condition or change in relevant facility or condition or change in the environment are entered individually inside rectangular frames called nodes.

Text entered in each node should be as simple and objective as possible, to avoid the pursuit of liability of each individual entity. The text is written in present tense or as a concise set of words.

The types of nodes and how they are drawn are shown in Table A.1.

Table A.1 — Types of nodes

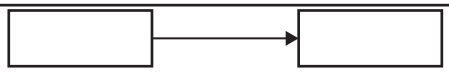
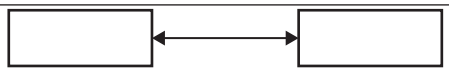
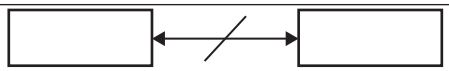
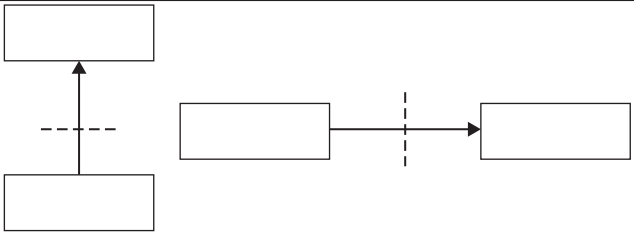
Type of node	Figure
Normal node (rectangle in thin line): Event or condition related to normal conditions	
Deviation node (rectangle in bold line): Event or condition that deviates from normal conditions	
Elimination node (marked with a circle at the top right of the node): Event or condition that is likely to be directly linked to the incident. Generally, a number of deviation nodes are classified as elimination nodes. However, there are cases in which a normal node can become an elimination node: — elimination node that is in the state of deviation (deviation node marked with a circle). — elimination node that is in normal condition (normal node marked with a circle).	
Assumption node (cell with a question mark (?) placed at left side of the node): When the event/condition is an assumption.	

A.2.2.4 Node connections

Nodes are connected with arrows in order to identify the causal relationships among nodes.

The types of nodes connections and how they are drawn are shown in Table A.2.

Table A.2 — Types of node connections

Type of node connection	Figure
If there is direction between events or conditions, they are connected with a unidirectional arrow.	
If events or conditions are interrelated, they are connected with a bidirectional arrow.	
If a problem is found in communication between nodes, a diagonal line is placed on the connecting arrow.	
Break (broken line). A broken line is placed perpendicular to the arrow of the node connection that would have prevented aggravation of the incident if the causal relationship or chain of events had been broken.	

A.2.2.5 Explanation

The description in each node should be as concise as possible. If the description is inadequate, a supplementary explanation marked with a number is added below the entire diagram (see Figure A.1).

A.2.2.6 Precondition

Matters shared by all of the items on the horizontal axis are entered below the said axis (see Figure A.1).

A.2.3 Process

The following steps make up the process.

a) Based on the information gathered, the events that took place over time are written inside rectangles as nodes. The nodes are then positioned in chronological order and connected with arrows based on their relationships.

b) Only one event is written concisely and objectively inside a node. If the description is inadequate, a supplementary explanation marked with a number is added at the right of the entire diagram.

c) An "assumption note" may be used in unavoidable cases, such as the absence of objective evidence.

d) A "deviation node" (an event or state that deviates from the norm) is identified and indicated by a bold frame.

e) An event or condition believed to be linked to the incident is designated an elimination node and is marked with a circle at the top right. An elimination node is a node highly likely to have prevented a critical event if eliminated. Generally, a number of deviation nodes are likely to become elimination nodes, but there are cases in which a normal node can become an elimination node. This is due to the fact that conduct regarded as normal can trigger an incident, depending on the conditions at that time.

f) A break (broken line) is placed at the point where the incident would not have occurred if the chain of events had not occurred from one node to the next, or between factors.

g) The elimination node in e) and the break in f) are direct causes.

A.2.4 Example

A scenario of an incident example is as follows (see Figure A.2).

— On a cold day in the middle of winter, the gas water heater in the home of an elderly person living alone broke down. The person asked for it to be repaired.

— The repair crew examined the water heater and found that the gas would not ignite due to a malfunction in the safety device.

— The repair required the replacement of parts. However, the repair crew did not have any replacement parts on hand. The person inquired with the company and found there was no inventory of the parts there.

— When told that it would be replaced at a later date, the elderly person pleaded, "I can't live without hot water in this season, please fix it somehow."

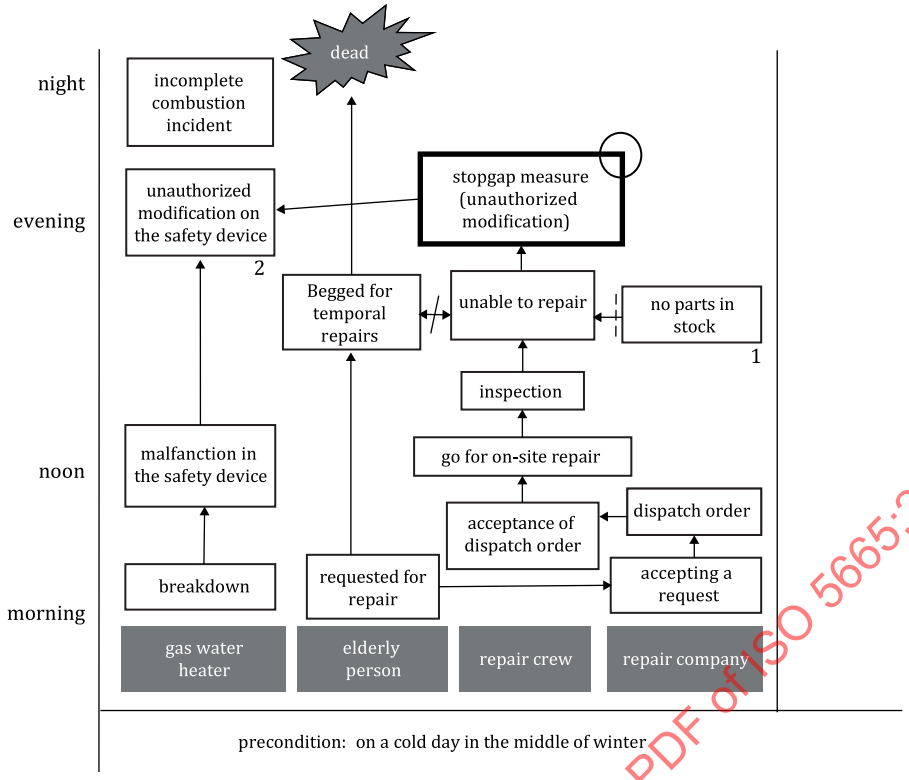
— The repair crew felt sorry for the elderly person and made an unauthorized modification by disabling the safety device, which allowed the gas to ignite and hot water to flow as a stopgap measure.

— That evening, the elderly person died from an incident caused by incomplete combustion.

The background information is as follows (see Figure A.2).

— A high frequency of safety device failure was reported for the particular model.

— The model was designed in a way that it was easy to make dangerous modifications to disable the safety devices.



Explanation

1 High frequency of safety device failure was reported for the particular model.

2 The model was designed in a way that it was easy to make dangerous modifications to disable the safety devices.

Figure A.2 — VTA diagram for the incident example

A.3 Why-why analysis

A.3.1 Overview

While VTA (see Clause A.2) is very effective in understanding events as objective facts and finding direct causes, Why-why analysis aims to reach the ultimate factor that cannot be considered anymore by repeating the step-by-step pursuit of "why" and "why not" for the underlying factors that are considered to have caused the event. If there are a number of underlying factors in an event, one should ask why each of them will result in a number of ultimate factors and require countermeasures.

A.3.2 Structure and process of the Why-why analysis diagram

In Why-why analysis, as shown in Figure A.3, the first question to be asked about an incident is "why (No. 1)," and the underlying factor to it is determined. Then, if it is not the final one considered, further underlying factor for it is found sequentially.

This is repeated a number of times to arrive at the ultimate factor. Depending on the complexity of the incident, it is desirable to limit the "why" to about five times:

— items on the vertical axis: the cause and effect are placed in a time series.

— items on the horizontal axis: if a single "why" uncovers multiple underlying factors, they are placed in the vertical direction.

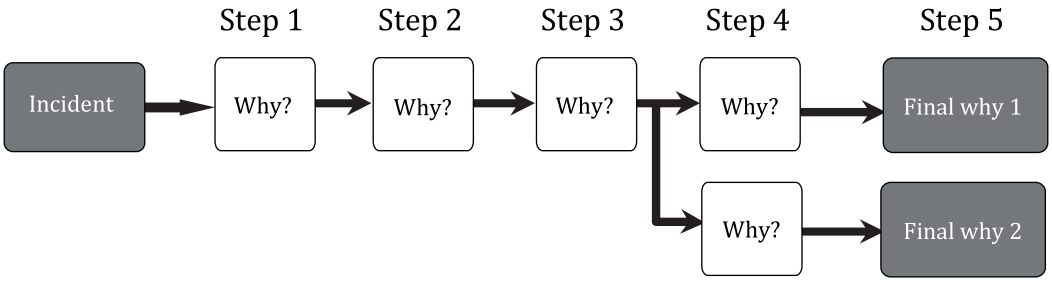


Figure A.3 — Basic form of the Why-why analysis diagram

NOTE By focusing on the M-SHEL items described in Clause A.4, i.e. management, software, hardware, environment, and liveware (person), it is possible to analyse without missing any important aspects.

Additionally, the validity of Why-why analysis can be confirmed by checking the flow of questions and answers in the opposite direction (from right to left) with the word "because", confirming that the explanation is logical and acceptable.

A.3.3 Example

The example in A.2.4 adapted to a diagram of Why-why analysis is shown in Figure A.4.

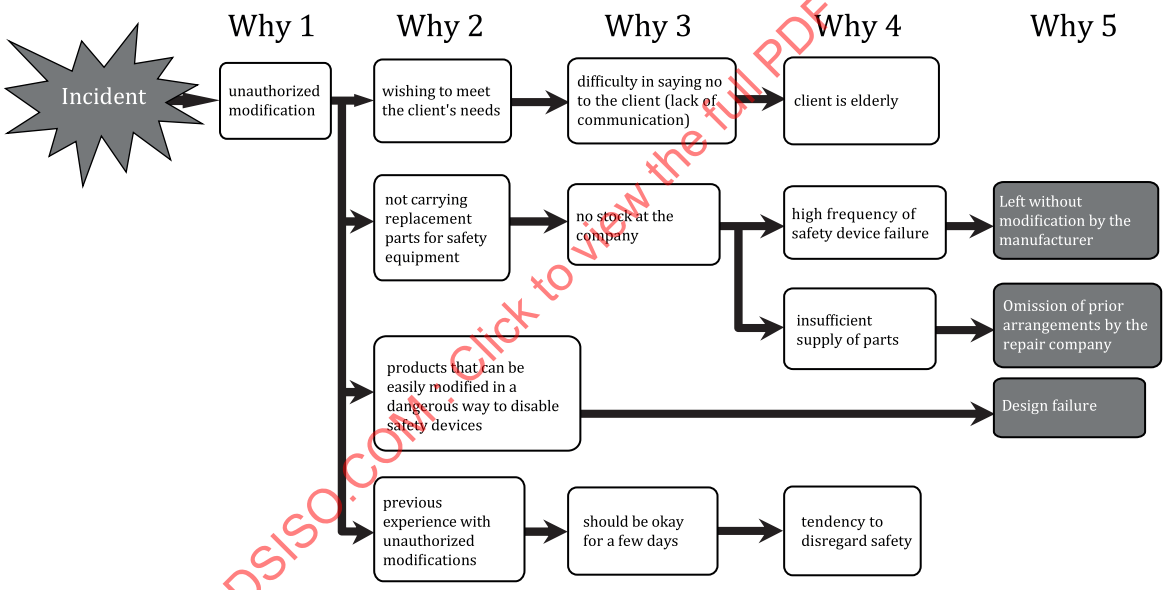


Figure A.4 — Why-why analysis diagram for the incident example

A.4 M-SHEL analysis

A.4.1 Overview

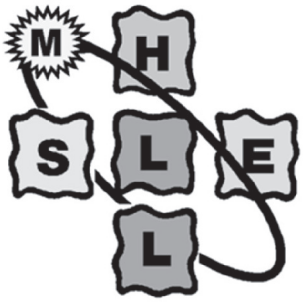
M-SHEL analysis is effective in examining incidents with human involvement. This analysis method employs a model in which the element of management (M) is added to the widely known SHEL method.

NOTE The M-SHEL analysis process includes countermeasure planning.

A.4.2 Structure of the M-SHEL model

In this analysis, the person (liveware) concerned in the incident (L) is positioned at the centre. The study is conducted by looking into what software (S) and hardware (H) were used at the time, what the environment

(E) was and how persons (L) other than the person concerned were involved, as well as how management (M) related to the incident was conducted (see Figure A.5).



SOURCE: Human Factors – Creating a Safe Society, Japan, reproduced with the permission of the authors.

Figure A.5 — M-SHEL model

The elements in the model indicate the following:

— M: basic concepts regarding safety, safety control system, organizational structure, etc.;

— S: regulations, policy, procedures, practice, information, etc.;

— H: machinery, products, tools, facilities, etc.;

— E: weather, temperature, humidity, noise, lighting, space (wide or narrow, near or far), etc.;

— Central L: person concerned or directly involved in the incident;

— Bottom L: person related to the person at the centre.

S, H, E and L are framed by wavy lines. The lines signify that the characteristics of each element change over time. If the elements are in contact with each other without any gap, it expresses visually that L at the centre is demonstrating the best possible performance.

On the other hand, if there is some kind of incompatibility between the elements, it can be considered as a situation where there is a gap in the contact surface, and this situation can easily cause human error.

M is shown as a satellite unlike other elements to suggest that it is closely connected to all of the other elements.

A.4.3 Process

A.4.3.1 Analysis

M-SHEL analysis is based on the basic idea of focusing on the person concerned and considering the relationship with the surrounding factors involved. When conducting the analysis, it is usually presented in a tabular format and the contents are filled in as appropriate.

— In M-SHEL analysis, L-S shows the relationship between the person and software (regulations, standards, etc.), L-H that between the person and hardware (facilities, products, tools, etc.) and L-E the relationship between the person and the environment (the surroundings at the time of the incident, customs and practices, etc.). Tables in a general format that are created when performing M-SHEL analysis are shown in Table A.3 and Table A.4.

— VTA by itself, or VTA and Why-why analysis in succession, makes it easier to fill in the M-SHEL table. In such a case, enter the elimination node or break of the VTA or the “last why” of the Why-why analysis in the cause and factor row of the table. Since the number of causes and factors is not necessarily one for each item, list the possible causes and factors based on each perspective in M-SHEL.

— In particular, for the "L" column, be careful not to use expressions that seek blame or liability. The description should be based solely on facts to help prevent recurrence.

Table A.3 — Table of basic information to be created as needed

Actions and/or conditions	Analysis target
(Fill in actions and/or conditions)	(Fill in the actions of the person involved and the condition of the objects that can be related to the occurrence of the incident.)

Table A.4 — M-SHEL analysis

M-SHEL	M	S (L-S)	H (L-H)	E (L-E)	L (L-L)	L
Causes and factors	(Fill in causes and factors in the management that contributed to actions and/or conditions.)	(Fill in causes and factors in the regulations, standards, etc., that contributed to actions and/or conditions.)	(Fill in causes and factors in the facility, equipment, etc., that contributed to actions and/or conditions.)	(Fill in causes and factors in the environment that contributed to actions and/or conditions.)	(Fill in causes and factors in the relationship between the person concerned and the related person that contributed to actions and/or conditions.)	(Fill in causes and factors of the person concerned that contributed to actions and/or conditions.)
Counter-measure	(Fill in countermeasure.)	(Fill in countermeasure.)	(Fill in countermeasure.)	(Fill in countermeasure.)	(Fill in countermeasure.)	(Fill in countermeasure.)

A.4.3.2 Countermeasures

In the "Countermeasures" column, describe the measures to be taken to solve the problems described in the "Causes and factors" column. Although countermeasures are basically developed to address each cause and factor, they do not necessarily fall into the "causes and factors" row. In some cases, whether it is a hardware or people problem, countermeasures are put under the "M" column. In some cases, the countermeasures can address a number of causes and factors at the same time. Depending on the situation, it is also effective to divide the measures into short-term, medium-term and long-term, and create an action plan for each of them.

A.4.4 Example

See Table A.5 for the example in A.2.4 adapted to a table of M-SHEL.

Table A.5 — Example of a M-SHEL analysis table for the incident

M-SHEL	M	S (L-S)	H (L-H)	E (L-E)	L (L-L)	L
Causes and factors	— The manufacturer did not revamp the safety device. (design failure) — The repair company did not arrange for the parts.	—	— The product was designed in a way that safety devices can be easily bypassed and disabled. — Frequent failures of safety devices.	— It was a cold winter night and hot water was needed. — A tendency to disregard safety.	Lack of communication.	He made unauthorized modifications.
Counter-measure	— The manufacturer improves the design of safety devices. — The repair company trains their employees on ethics.	—	The manufacturer changes the design of the product.	—	Careful explanation of risks.	Compliance with procedures.

Annex B
(informative)

Root cause analysis method

B.1 General

Root cause analysis (RCA) does not refer to a specific analysis method. RCA is a general term for a method of finding the ultimate cause (root cause) and formulating countermeasures by combining multiple methods of factor analysis and including the analysis of organizational factors at the end of the process of searching for underlying factors. While there are a variety of methods, Japan institute of human factors root cause analysis (J-RCA), which is relatively easy to analyse, will be presented in this annex.

B.2 Japan institute of human factors root cause analysis

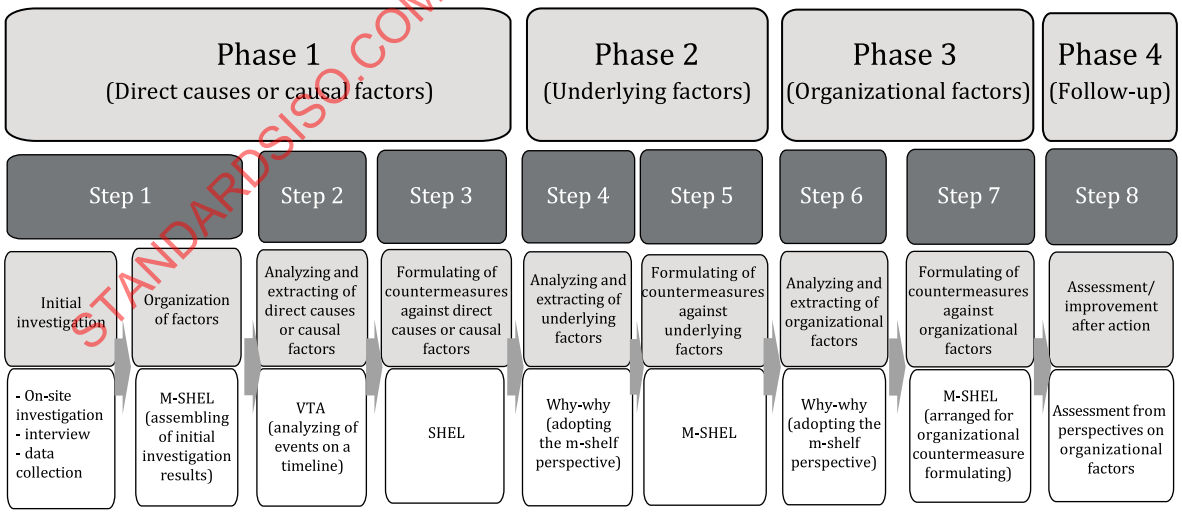
B.2.1 Overview

J-RCA is a combination of VTA, Why-why analysis and M-SHEL analysis described in Annex A. It aims to prevent the recurrence of incidents by developing emergency countermeasures, direct cause or causal factor analysis and countermeasures, underlying factor analysis and countermeasures, and organizational factor analysis and countermeasures. The J-RCA process includes the evaluation of countermeasures.

B.2.2 Structure of J-RCA

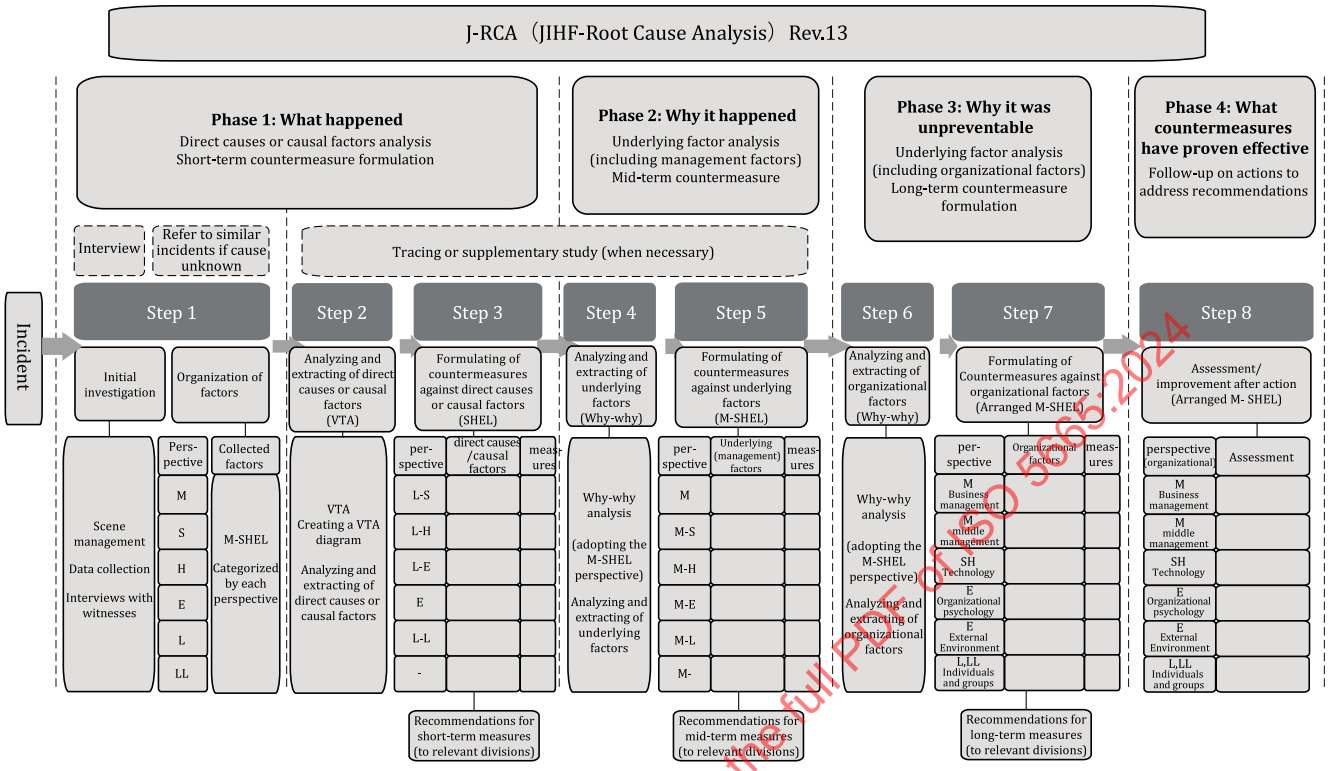
B.2.2.1 General

J-RCA consists of the following eight steps divided into four phases, starting with information gathering immediately after the incident, analysis and development of countermeasures and ending with follow-up action. The basic form is shown in Figure B.1 and a detailed form is shown in Figure B.2.



SOURCE: Human Factors - Creating a Safe Society, Japan (with some modifications), reproduced with the permission of the authors.

Figure B.1 — Basic form of a J-RCA



SOURCE: Human Factors - Creating a Safe Society, Japan (with some modifications), reproduced with the permission of the authors.

Figure B.2 — Detailed form of a J-RCA

B.2.2.2 Phase 1: What happened

Analyse direct causes or causal factors, formulate emergency or short-term countermeasures, and recommend implementation of countermeasures to relevant departments or organizations as necessary.

B.2.2.3 Phase 2: Why it happened

For the direct causes or causal factors identified in the first phase, analyse the underlying factors, each of them by adding a “management” perspective, formulate medium-term countermeasures, and recommend implementation of the countermeasures to the relevant departments or organizations.

B.2.2.4 Phase 3: Why it was unpreventable

Analyse the organizational factors involved in the incident, identify the root causes, formulate long-term preventive measures throughout the organization related to the incident, and recommend implementation of the measures to the relevant departments or organizations.