*energies*

MDPI

*Article*

# Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management

**Kazimierz T. Kosmowski [1], Emilian Piesik [1,*], Jan Piesik [2] and Marcin Śliwiński [1]**

[1] Faculty of Electrical and Control Engineering, Gdansk University of Technology, G. Narutowicza 11/12, 80-233 Gdansk, Poland; kazimierz.kosmowski@pg.edu.pl (K.T.K.); marcin.sliwinski@pg.edu.pl (M.Ś.)
[2] Michelin Polska Sp. z o.o., St. W. Leonharda 9, 10-454 Olsztyn, Poland; jan.piesik@michelin.com
* Correspondence: emilian.piesik@pg.edu.pl

**Abstract:** This article outlines an integrated functional safety and cybersecurity evaluation approach within a framework for business continuity management (BCM) in energy companies, including those using Industry 4.0 business and technical solutions. In such companies, information and communication technology (ICT), and industrial automation and control system (IACS) play important roles. Using advanced technologies in modern manufacturing systems and process plants can, however, create management impediments due to the openness of these technologies to external systems and networks via various communication channels. This makes company assets and resources potentially vulnerable to risks, e.g., due to cyber-attacks. In the BCM-oriented approach proposed here, both preventive and recovery activities are considered in light of engineering best practices and selected international standards, reports, and domain publications.

**Keywords:** functional safety; cybersecurity; BCM; Industry 4.0; information technology; industrial control system



**Citation:** Kosmowski, K.T.; Piesik, E.; Piesik, J.; Śliwiński, M. Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. *Energies* **2022**, *15*, 3610. https://doi.org/10.3390/en15103610

Academic Editor: Marko Mladineo

Received: 17 March 2022
Accepted: 12 May 2022
Published: 15 May 2022



## 1. Introduction

Industrial companies nowadays, including those implementing Industry 4.0 smart technologies, face potential safety and security problems due to their use of open systems and networks for communication and control [1–3]. The same concerns exist with respect to the energy systems within critical infrastructure such as power plants for producing electricity and/or heat from various energy sources, including coal, oil, natural gas, biogas, and renewable energy sources.

In order for power plants and distributed industrial systems to be economically effective, they should be reliable in continuous operation mode, or with the highest achievable availability when their operation is required on demand (e.g., during peak load of the electrical grid or during an abnormal state due to dependent or cascade failure leading to emergency conditions). These issues can be considered from a business continuity management (BCM) [4,5] point of view.

A traditional RAMS&S (reliability, availability, maintainability, safety, and security) methodology [6,7] can support elements of BCM in the life cycle, however, it insufficient due to its need to consider various impact factors, including the human and organizational factors. Certain aspects of BCM can be analyzed regarding performability engineering, as analysed and emphasised by Misra [8]. An interdisciplinary review of business continuity issues from the perspective of information systems, directed towards proposing an integrated framework, was published by Niemimaa [9]. These issues are lately of increasing attention to insurance companies [10,11].

Relatively new aspects in BCM analysis are connected to information and communication technology (ICT) and industrial control systems (ICS) that operate within computer systems and networks using wired or wireless communication channels. These systems

and networks have been considered in several publications and research reports from the perspective of systems engineering [12–15] and cyber-physical systems [16,17]. Several research projects have been undertaken concerning the integrated analysis of ICS safety and security [18,19]. Interesting research works have been published concerning business continuity management, for instance an article [20] and monograph [21]. The functional safety and cybersecurity issues of industrial automation and control systems (IACS) have lately been emphasized as especially important in the design and operation of hazardous industrial plants and critical infrastructure systems [22–25].

Several security-related issues of the industrial automation and control system (IACS) have been considered in the context of protection solutions proposed for improving IACS security as proposed in the IEC 62443 standard [26]. The dependability and safety integrity of the safety-related part of the ICS are discussed with regard to the generic functional safety standard IEC 61508 in [27].

The remainder of this article is structured as follows. Section 2 provides a basic overview of functional safety and cybersecurity aspects related to business continuity management and the basic requirements in the context of risk evaluation within the life cycle; in addition, a BCM framework is proposed for business continuity planning in industrial companies. Section 3 outlines an integrated dependability, safety, and security management framework for industrial companies, including BCM aspects. In Section 4, a case study is presented to demonstrate the application of the proposed integrated approach. In the conclusions, the significance of adequately treating ICT and IACS within BCM activities in Industry 4.0 is emphasized.

## 2. Brief Presentation of the Framework and Components

### *2.1. Overview of IT and OT Systems and Their Convergence*

The convergence of information technology (IT) and operational technology (OT) creates both new opportunities and new challenges. The data flows outside and into plant networks inevitably lead to additional threats and increased security-related risks. One of the biggest challenges facing the industrial sector is understanding the risks involved in potential cyberattacks, which are already being observed; these risks can emerge when companies adopt Industry 4.0 technologies, including Industrial Internet of Things (IIoT) technologies and tools. The management staff of industrial companies are becoming more aware about the magnitude of the gap between the priorities recognized by teams responsible for operational technology (OT) and those recognized by information technology (IT) professionals. This gap often impacts new cybersecurity initiatives.

In order to explain the issues involved, it is necessary to begin with a model industrial system. The traditional reference model is based on the ISA99 series of standards derived from the generic model of ANSI/ISA-95.00.01 (Enterprise-Control System Integration), and represents the manufacturing system using five functional and logical levels (Figure 1). These levels are often assigned to two classes, namely, Operational Technology (OT) and Information Technology (IT), with their own relevant security zones. The zero level defines the actual physical processes. The first level of activities involved in sensing and manipulating physical processes include intelligent devices. The second level includes control systems (e.g., Programmable Logic Controllers). The third level, site manufacturing and control, includes an ICS/SCADA system with a relevant Human–System Interface (HSI) and the Manufacturing Execution System (MES). The fourth level, enterprise business planning and logistics, comprises an Enterprise Resource Planning (ERP) system for effectively management and coordination of the business and enterprise resources required for manufacturing processes. Finally, the fifth level is the enterprise network for business and logistics activities, which can now be supported using applications based on Cloud Technology (CT) [28,29].

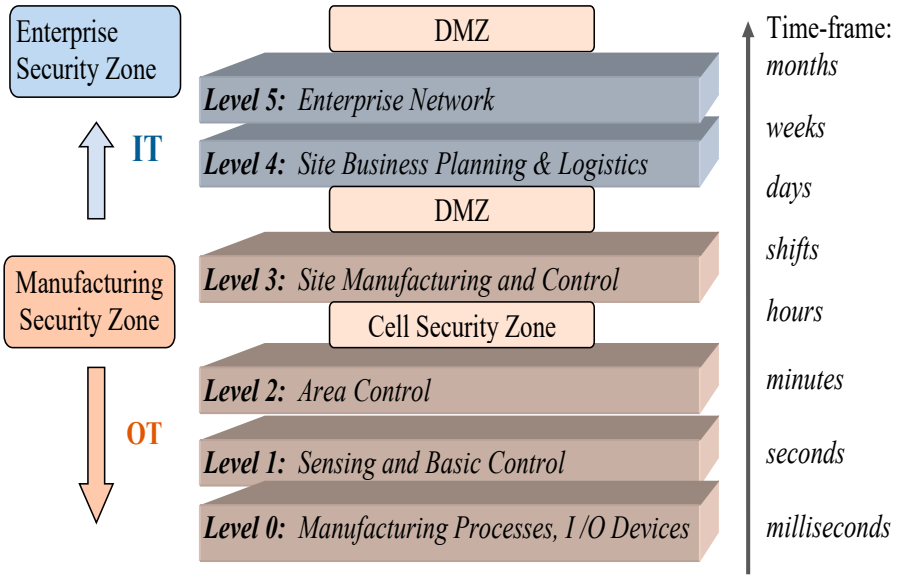


**Figure 1.** Traditional reference model of an industrial system based on the ANSI/ISA95 standard.

In an open manufacturing system, assigning safety and security-related requirements requires the special attention of designers and operators [3,30,31].

From an information security point of view, an important requirement and solution is to prioritize segmentation of the complex industrial computer system and network, distinguishing cell security zones and designing a Demilitarized Zone (DMZ), as illustrated in Figure 1.

The DMZ is sometimes referred to as a perimeter network or screened subnet, and is a physical or logical subnetwork for controlling and securing internal data and services from an organization's external services using an untrusted (usually larger) network such as a corporate-wide area network (WAN), the Internet, or a cloud technology (CT).

Thus, the purpose of a DMZ is to add a layer of security to an organization's local area network (LAN); an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled [1,30].

An actual list of internal and external influences, hazards, and threats should be considered during the design and operation of the OT and IT systems and networks. Basic features of these systems are presented in Figure 2.

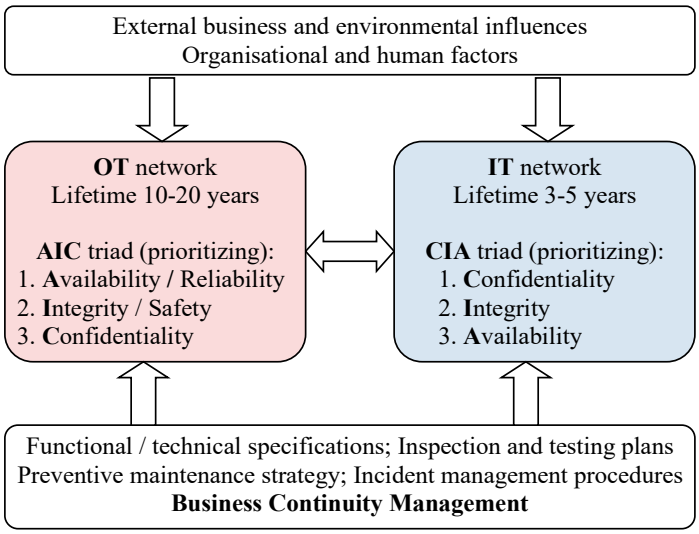


**Figure 2.** Basic features characterizing OT and IT systems and networks [23].

While the expected lifetime of OT systems is typically evaluated in the range of 10–20 years, this drops to only 3–5 years in the case of IT systems [23]. In characterizing the OT system, the AIC triad (Availability, Integrity, and Confidentiality) is often used to prioritize basic requirements, while the CIA triad (Confidentiality, Integrity, and Availability) is used to characterize the IT network.

The safety and security of both OT and IT systems and networks are dependent on various external and internal influences, including organizational and human factors [32]. Traditionally, a general MTE (Man-Technology-Environment) approach has been proposed for systemic analyses and management in the life cycle of industrial installations. An interesting framework for dealing with complex technical systems is offered by systems engineering (SE) [13]. The industrial automation and control system (IACS) [26,33] can be considered as a cyber-physical system [17,34,35].

### *2.2. Functional Safety of OT Systems*

For high dependability and safety of the OT system, an operational strategy within BCM should be elaborated that includes inspections and periodical testing of safety-related control systems, for instance, electrical/electronic/programmable electronic (E/E/PE) systems [27] and safety instrumented systems (SIS) [36], including their sensors and the equipment under control (EUC).

The operational equipment of manufacturing lines (machinery, drives, operational control systems, etc.) requires an advanced preventive maintenance strategy to be implemented in order to achieve the required high OT availability and reduce the risk of outages and related production losses. Incident management procedures must be developed to reduce the risk of potentially hazardous events leading to major losses.

A set of safety functions are implemented in the safety-related ICS of required safety integrity levels (SILr), determined in the risk assessment process in relation to the criteria defined [12], to be assigned, for instance, to the E/E/PE or SIS systems (see the OT block in Figure 3).

Two different requirements must be specified to ensure an appropriate level of functional safety [37]:

- The requirements imposed on the performance of safety functions designed for hazard identification;
- The safety integrity requirements, i.e., the probability that a safety function will be performed in a satisfactory way when a potentially hazardous situation occurs.

Safety integrity is defined as the probability that a safety-related system, such as the E/E/PE system or SIS, will satisfactorily perform a defined safety function under all stated conditions within a given time. For safety-related ICS in which a defined safety function is implemented two probabilistic criteria must be defined, as presented in Table 1 for four categories of the SIL [27], namely:

- The probability of failure on demand average ($PFD_{avg}$) of the safety-related ICS in which the considered safety function is implemented, operating in a low-demand mode (LDM); or
- The probability of dangerous failure per hour (PFH) of the safety-related ICS operating in a high- or continuous-demand mode (HCM).

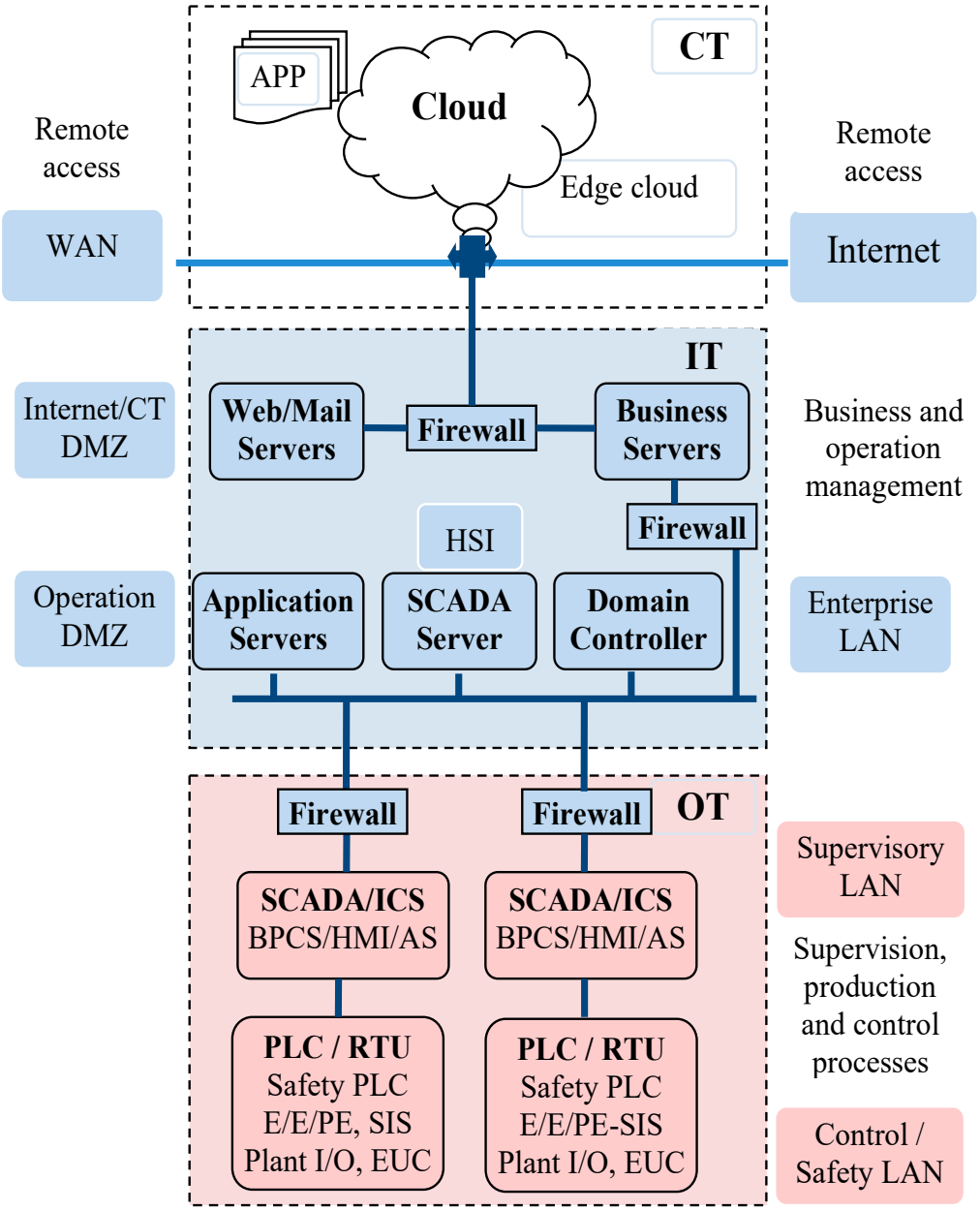


**Figure 3.** Typical ICT and ICS architecture including OT, IT, and CT.

**Table 1.** Categories of SIL and probabilistic criteria to be assigned to safety-related ICS operating in LDM or HCM.

| SIL | $PFD_{avg}$ | $PFH$ [$h^{-1}$] |
|---|---|---|
| 4 | $[10^{-5}, 10^{-4})$ | $[10^{-9}, 10^{-8})$ |
| 3 | $[10^{-4}, 10^{-3})$ | $[10^{-8}, 10^{-7})$ |
| 2 | $[10^{-3}, 10^{-2})$ | $[10^{-7}, 10^{-6})$ |
| 1 | $[10^{-2}, 10^{-1})$ | $[10^{-6}, 10^{-5})$ |

The SIL requirements assigned for the safety-related ICS to be designed for implementing a specified safety function stem from the results of the risk analysis and evaluation meant to reduce the risk of losses by sufficiently considering specified risk criteria, namely, for individual risk and/or group or societal risk [27].

If societal risk is of interest, analyses can generally be oriented on three distinguished categories of loss, namely [27,36,38], health ($H$), environment ($E$), and material ($M$) damage; then, the SIL required ($SIL_r$) for a particular safety function is determined as follows:

$$SIL_r = \max\left(SIL_r^H,\ SIL_r^E,\ SIL_r^M\right) \quad (1)$$

As mentioned above, SIL verification can generally be carried out for either of two operation modes, namely, LDM or HCM. The former is characteristic of the process industry [36], while the latter is typical for machinery [39], railway transportation systems, and the monitoring and real-time control of any installation using an ICS/SCADA system.

Management of the OT system and IACS, including safety-related lifecycle ICS, can be challenging; in industrial practice, it is difficult to achieve the above-specified requirements concerning the AIC triad (see Figure 3) for various reasons. Nevertheless, these systems contribute significantly to the realization of required quality and quantity of products in time, and influence overall equipment effectiveness (OEE). No less important are the functional safety and cybersecurity issues regarding the requirements and criteria discussed above.

The following items should be specified for implementation in industrial practice:

- A plan for operating and maintaining E/E/PE safety-related systems or SIS;
- Operation, maintenance, and repair procedures for these systems over their whole life cycle;

Implementation of these items must include initiation of the following actions:

- Implementing procedures;
- Following maintenance schedules;
- Maintaining relevant documentation;
- Periodically carrying out functional safety audits;
- Documenting any modifications to the hardware and software in E/E/PE systems.

Thus, all modifications that have an impact on the functional safety of any E/E/PE safety-related system must initiate a return to an appropriate phase of the overall E/E/PE system or software safety lifecycles. All subsequent phases must then be carried out in accordance with the procedures specified for the specific phases regarding the requirements in the above-mentioned standards.

For each phase of the overall functional safety lifecycles, a plan for verification and validation should be established concurrently with the development of consecutive phases. The verification plan must document or refer to the criteria, techniques, and tools to be used in verification activities.

Chronological documentation of operation, repair, and maintenance of safety-related systems should be maintained and must include the following information:

- The results of functional safety audits and tests;
- Documentation on the time and cause of demands on E/E/PE safety-related systems in actual operation the performance of the E/E/PE safety-related systems when subject to those demands, and any faults found during routine testing and maintenance;
- Documentation of any modifications made to safety-related ICS, including equipment under control (EUC).

The requirements concerning chronological documentation should be sufficiently detailed for the specific context of safety-related ICS operations [27,36,39].

### *2.3. Cybersecurity of IT Systems*

From a cybersecurity perspective, the systems and networks used within the business environment (level 4 of the ISA95 model in Figure 1) should be considered as potentially insecure, as they contain complex interdependent hardware and software (see simplified architecture in Figure 3), remote access paths, and external communications. Therefore, IT and OT systems with the access to the Internet and/or a wide area network (WAN), or when the cloud technology (CT) is used, should be secured at the required security

assurance level (SAL) for assignment to respective zones [26]. It has been postulated that the SAL assigned to the relevant domain should be included when verifying the safety integrity level (SIL) of safety-related ICS in which a specified safety function is to be implemented [12,40].

Security-related risks can be mitigated through the combined efforts of component suppliers, the machinery manufacturer, the system integrator, and the machinery final end user (with the company owner responsible) [26,33]. Generally, the response to a security risks should be as follows [41]:

(a) Eliminate the security risk by design (avoiding vulnerabilities);
(b) Mitigate the security risk by risk reduction measures (limiting vulnerabilities);
(c) Provide information about residual security risks and measures to be adopted by the user.

The IEC 62443 standard [26] proposes an approach to dealing systematically with security-related issues in IACS. Four security levels (SLs) have been defined, understood as a confidence measure for ensuring that the IACS is free from vulnerabilities and will function in the intended manner. These SLs are suggested in the standard IEC 63074 [41] for dealing with the security of safety-related ICS designed for the operation of manufacturing plants.

These levels (numbered from 1 to 4, see Table 2) represent a piece of qualitative information addressing the relevant protection scope of the domain or zone considered in the evaluation against potential violations during safety-related ICS operation in a zone.

**Table 2.** Security levels and protection description of the IACS domain [26,41].

| Security Levels | Description |
|---|---|
| SL 1 | Protection against casual or coincidental violation |
| SL 2 | Protection against intentional violation using simple means with low resources, generic skills, and low motivation |
| SL 3 | Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation |
| SL 4 | Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation |

The relevant SL number from 1 to 4 should be assigned to seven consecutive foundational requirements (FRs) relevant within the domain considered [26]:

FR 1—Identification and authentication control (IAC);
FR 2—Use control (UC);
FR 3—System integrity (SI);
FR 4—Data confidentiality (DC);
FR 5—Restricted data flow (RDF);
FR 6—Timely response to events (TRE);
FR 7—Resource availability (RA).

Thus, it is suggested that dependability and security-related evaluations apply a defined vector of relevant FRs from those specified above. Such a vector might be defined for the security-related requirements for a zone, conduit, component, or system. It contains the general integer numbers characterizing the SL from 1 to 4 (or 0 if not relevant) to be assigned to consecutive FR.

A general format of the security assurance level (SAL) to be evaluated for a given domain is defined as a function of [FRs] [26]:

$$\text{SAL} \times (\text{[FRs] domain}) = f\ \text{[IAC UC SI DC RDF TRE RA]} \quad (2)$$

### 2.4. Integrated Functional Safety and Cybersecurity Evaluation

Assigning the SAL to the domain or zone as an integer number from 1 to 4 [37,42] can present problems. To overcome this difficulty, the security indicator $SI^{Do}$ for a domain (*Do*) can be defined [40] to determine security levels $SL_i$ for a set (Re) of relevant fundamental requirements ($FR_i$) with relevant weights $w_i$ evaluated based on the opinions of ICT and ICS experts. This indicator is a real number from the interval (1.0, 4.0) calculated using the following formula:

$$SI^{Do} = \sum_{i \in \mathrm{Re}} w_i SL_i, \sum_i w_i = 1 \quad (3)$$

Four intervals of the domain security index $SI^{Do}$ (from $SI^{Do1}$ to $SI^{Do4}$) are proposed in the first column of Table 3 for assigning an SAL category integer number from 1 to 4. This approach corresponds with that used in earlier publications for attributing an SAL to the domain based on the dominant $SL_i$ for the relevant fundamental requirements, $FR_i$.

**Table 3.** Proposed correlation between $SI^{Do}$/SAL for the evaluated domain and final SIL to be attributed to the safety-related ICS of a critical installation.

| Security Indicator $SI^{Do}$/SAL | SIL Verified According to IEC 61508 * | | | |
|---|---|---|---|---|
| | **1** | **2** | **3** | **4** |
| $SI^{Do1}$∈**[1.0, 1.5)/SAL 1** | SIL 1 | SIL 1 | SIL 1 | SIL 1 |
| $SI^{Do2}$∈**[1.5, 2.5)/SAL 2** | SIL 1 | SIL 2 | SIL 2 | SIL 2 |
| $SI^{Do3}$∈**[2.5, 3.5)/SAL 3** | SIL 1 | SIL 2 | SIL 3 | SIL 3 |
| $SI^{Do4}$∈**[3.5, 4.0]/SAL 4** | SIL 1 | SIL 2 | SIL 3 | SIL 4 |

* verification includes the architectural constraints regarding $S_{FF}$ and HFT of subsystems.

Three types of vectors describing $SL_i$ for consecutive $FR_i$ of a domain can be distinguished [24]:

- SL-T (target SAL)—Desired level of security;
- SL-C (capability SAL)—Security level that the device can provide when properly configured;
- SL-A (achieved SAL)—Actual level of security of a particular device.

Proposed correlations between the security index to be assigned to the domain $SI^{Do}$/SAL and the final SIL attributed to the safety-related ICS in a hazardous installation are presented in Table 3. It was assumed that SILs were verified according to IEC 61508 requirements based on the results of probabilistic modelling [12,43], regarding potential common cause failures (CCFs) and the influence of the human and organizational factors regarding architectural constraints for the evaluated $S_{FF}$ and HFT of the E/E/PE subsystems (see explanations above). Thus, SIL verification requires probabilistic modelling of the safety-related ICS of the proposed architecture regarding the $S_{FF}$ and HFT of the subsystems.

### 2.5. Scope of BCM

Business continuity management (BCM) is usually understood as the capability and specified activity of an organization to continue delivery of products and/or services of required quality within acceptable time frames at a predefined capacity relating to the scale of potential disruptions [4].

A disruption is defined as an incident, whether anticipated or unanticipated, that causes an unplanned negative deviation from the expected delivery of products and services according to an organization's objectives. An objective is the result to be achieved. The objective can be strategic, tactical, or operational.

The objective can be expressed in other ways, e.g., as an intended outcome, a purpose, an operational criterion, or using other words with similar meaning (e.g., aim, goal, or target). Objectives can relate to different disciplines (such as financial, health and safety, and

environmental objectives) and can apply at different levels (such as strategic, organization-wide, project, product, and process).

The BCM can be considered an integral part of a holistic risk management that safeguards the interests of the organization's key stakeholders, reputation, brand, and value by creating activities through [10]:

- Identifying potential threats that might cause adverse impacts on an organization's business operations, and associated risks;
- Providing a framework for building resilience for business operations;
- Providing capabilities, facilities, processes, and elaborated action task lists, etc., for effective responses to disasters and failures.

An event can be an occurrence or change in a particular set of circumstances that could have several causes and several consequences. An abnormal event due to a hazard or threat is considered a risk source. An emergency is a result of a sudden, urgent, usually unexpected occurrence or event requiring immediate action. It is a disruption or condition that can be anticipated or prepared for, although seldom exactly foreseen [44–46].

The organization must implement and maintain a systematic risk assessment process. Such a process could be carried out, for instance, in accordance with the ISO 31000 standard. As shown in Figure 4, an organization should:

(a) Identify risks of disruption to the organization's prioritized activities and their supporting resources;
(b) Systematically analyze and assess risks of disruption;
(c) Evaluate risks of disruptions that require adequate treatment.

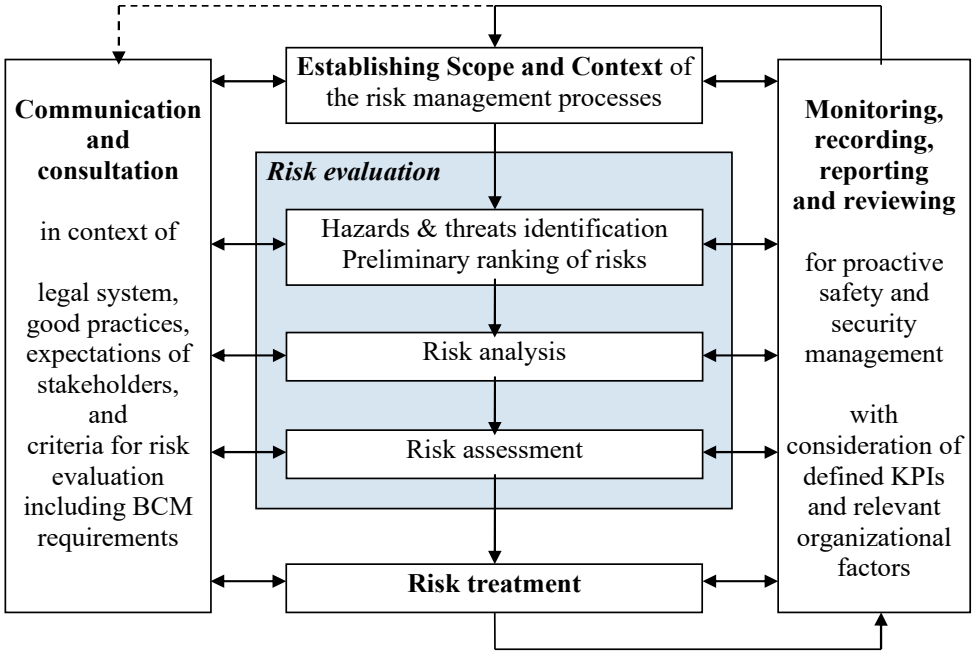


**Figure 4.** Risk management process (based on [47]).

Risk evaluation is considered an overall process of hazard/threat identification, risk analysis, and risk assessment [28,47]. Risk management is a process of coordinating activities in order to direct and control an organization regarding risk.

The general purpose is to reduce an industrial system's vulnerability as required in order to increase its resilience as justified considering current legal and/or regulatory requirements regarding the results of cost–benefit analyses. Relevant protection measures should be proposed that adequately safeguard and enable an organization to prevent or reduce the impact and consequences of potential disruptions.

After a major disruption, the recovery process is to be undertaken in order to restore system operation in a timely manner and improve activities, operations, facilities, and other key determinants of the affected organization where appropriate in order to increase its business resilience for the future.

### *2.6. BCM in Energy Companies*

There have been various approaches proposed to apply the BCM concept in industrial practice. The standard BS 25999-1 [29] provided a proposal based on the concept of good practice. It was intended for use by anyone with responsibility for business operations or the provision of services, from top management through all levels of the organization. It was in principle foreseen for a single-site BCM or, with a more global presence, ranging from a sole trader through a small-to-medium enterprise (SME) to a large company employing thousands of people. However, this standard was withdrawn and replaced in industrial practice in favor of the ISO/DIS 22301 [4], which describes the basic requirements to be assigned in developing modern BCM systems.

As previously mentioned, BCM includes the recovery, management, and continuation of business activities in situations of business disruption as well as integrated management of the overall program through training, exercises, audits, and reviews to ensure that the business continuity plan stays current and up to date [48–50].

When analyzing energy and industrial companies, including their control systems [15,51,52], it is suggested that the following categories of potential disruptions be considered:

- Failures in logistics chains, delays in delivery of raw materials or semi-finished products by business partners, and/or delays in providing services, spare parts etc.
- Failures in electric energy distributed systems
- Power transformer station failures fires, cyberattacks, etc.
- Physical or cyberattack
- Failures and outages of ICT and CT (cloud technology) systems and networks designed using wired and/or wireless technology
- Failures and outages of OT systems and networks, including production lines and storage, and/or malfunctions of industrial automation and control systems (IACS)
- Extreme environmental phenomena, lightning storms, heavy rain, local flooding, flood, hurricane, or tornado, extremely high or low temperature, and heavy snowfall or icing
- Disturbances in critical infrastructure objects and systems needed to deliver water, electricity, gas etc.
- Fire or explosion
- Extreme emission of pollutants and/or dangerous substances
- Destruction due to potentially critical events in physical surroundings or infrastructure installations
- Earthquake and/or tsunami (at sites close to the shore)
- Sabotage, terrorism, or cyberterrorism against critical infrastructure objects/systems inspired by an external principal or agent
- Legislative changes

Only selected categories of potential disruptions will be discussed in the presented approach.

The consequences of an incident may vary significantly and can be far-reaching, including major accidents with both internal and external losses. These consequences might involve loss of life, environmental losses, and loss of assets or income due to the inability to deliver products and services on which the organization's strategy, reputation, or even economic survival might depend.

The importance of shaping the organizational culture and related safety and security culture is essential. It is a fundamental prerequisite both of successful activities and of avoiding failures in any organization, including a modern industrial company present within a competitive market.

Expected outcomes of an effective BCM program implemented in an energy or industrial company are as follows [4,49]:

- Key products and services are identified and protected, ensuring their continuity;
- Incident management capability is enabled to provide an effective response;
- The company understands its relationships with cooperating companies/organizations, relevant regulators and authorities, and emergency services;
- Staff are trained to respond effectively to an incident or disruption through appropriate exercises;
- Stakeholders' requirements are understood and able to be delivered;
- Staff receive adequate support and communications in the event of a disruption;
- The company's supply chain is better secured;
- The organization's reputation is protected and remains compliant with its legal and regulatory obligations.

In the energy sector, it is crucial to have maintain the operation of infrastructure equipment. This is supported by the correct application of BCM. As previously mentioned, there are many factors affecting the operation of any plant, including a power sector plant. These various factors are multidisciplinary and can be applied to different industry sectors.

Several indicators are used for decision-making in BCM, for instance [48], RTO (recovery time objective), the recovery time of a process or the required resources, and MTPD (maximum tolerable period of disruption), the maximal tolerable downtime which, when exceeded, seriously threatens the medium-term or long-term survival of the process or the organization. The maximum time for recovery (RTO) must be smaller than the maximum tolerable period of disruption (MTPD).

A formal set of procedures should be established to deal with information security incidents and identified weaknesses, which may have a physical component. This should encompass [44,49,50]:

- Detection of all information security incidents (and weaknesses) and related escalation procedures and channels;
- Reporting and logging of all information security incidents and weaknesses;
- Logging all responses and preventive and corrective actions taken;
- Periodic evaluation of all information security incidents and weaknesses;
- Learning from reviews of information security incidents(and weaknesses and making improvements to security and to the information security incident and weakness management scheme.

Service providers should ensure that all ICT systems essential for disaster recovery are tested regularly to ensure their continuing capability to support DR plans. Tests should be conducted whenever there are any significant changes in organizational requirements and/or changes in service provider capacity and capability that affect services to organizations. Examples of such changes include relocation of DR sites, major upgrades of ICT systems, and commissioning of new ICT systems.

There is an IT infrastructure in the energy sector, and problems with its proper operation contribute to power outages; information transmission deficiencies can cause blackouts in certain cases.

Several sets of various characteristics influencing performance and key performance indicators (KPIs) are listed [11] for use in evaluations and audits within the BCM of the industrial plant to support relevant decisions. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are two of the most important parameters of a disaster recovery or data protection plan. The RPO and RTO, along with a business impact analysis, provide the basis for identifying and analyzing viable strategies for inclusion in the business continuity plan of the BCM in relation to the previously discussed standards [4,48,50].

An objective of the recovery target time can be set, for instance, in the following cases:

- Resumption of product or service delivery after an incident, or resumption of a performance activity after an incident;
- Recovery of the ICT (information and communication technology) system or computer application after an incident, such as a hacker attack, or IT-OT system failure or

functional abnormality, such as abnormal performance of the industrial automation and control system (IACS).

The BCM approach outlined above is based on esteemed reports and international standards, including current legal and regulatory requirements.

The energy sector is critical to the operation of everything from households to critical infrastructure. In the current consideration of BCM, there are no specific explicit requirements for a particular sector, including the energy sector.

## 3. Proposed Integrated Functional Safety and Cybersecurity Evaluation in the Framework of BCM

In the approach presented below, current research issues are considered from the general perspective of BCM regarding the dependability, safety, and security of the ICT and ICS, including the SCADA (supervisory control and data acquisition) system. Their required functionality and architectures are discussed, distinguishing between information technology (IT) and operational technology (OT) in relevant systems and networks [40]. These systems require effective convergence for advanced manufacturing functionality and improved effectiveness in the realization of advanced manufacturing and business-related processes. In this article, an approach is proposed for integrated functional safety and cybersecurity analysis and management over the whole life cycle based on determining and verifying the safety integrity level (SIL) of the safety-related ICS system regarding the security assurance level (SAL) assigned to the relevant security domain.

The main objective is to outline a conceptual framework for including the above-mentioned technologies and systems within business continuity management activity. The proposed holistic management process identifies potential hazards and threats to an organization and their impact on manufacturing and business processes that, if realized, might cause disruptions and related losses. The purpose of the system is to provide a framework for building organizational resilience and preparing effective response, as such safeguards are important for company owners, key stakeholders, regulators, and local authorities [29,48–50] as well as crucial for brand, reputation, and value-creating activities.

The proposed BCM framework emphasizes the significance of a business continuity plan (BCP) for industrial companies (Figure 5).

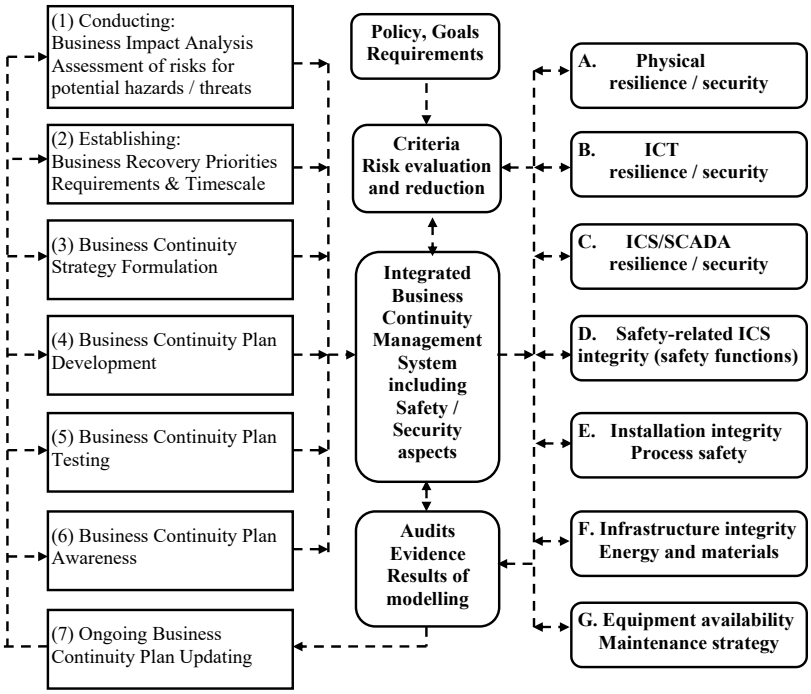


**Figure 5.** Proposed BCM framework for business continuity planning in industrial companies.

The left side of Figure 5 consists of seven specified discrete stages adapted from the standards in [44,50]; these are aimed at developing a comprehensive business continuity plan that will meet a company's business requirements, including the service providers. This is useful in developing recovery procedures (RP) for abnormal situations, failure events, or disaster recovery plans (DRP) [44] for cases of major disruptions and potential disasters.

In the middle part of this figure, basic elements of the approach to integrated BCM are specified, including the dependability, safety, and security aspects. The management activities are based on domain knowledge, current information, evidence, and results of modelling in the following areas:

- Formulating policies, goals, and domain, including legal and regulatory requirements and relevant standards and publications of good practice;
- Criteria for risk evaluation and reduction concerning dependability, safety, and security aspects, including domain key performance indicators (KPIs);
- Updated evidence, results of audits in design and plant operation, and results of modelling to support relevant decisions.

Audits can be (1) a first-party audit using internal resources, (2) a second-party audit initiated by a supplier, customer, contractor, and/or insurer, or (3) a third-party audit performed by an independent body against a recognized standard, i.e., ISO 9001.

On the right side of Figure 5, seven areas are specified and proposed by the authors for inclusion in the process of business continuity planning for a modern plant that requires relevant technical and organizational solutions in the following areas:

A. Physical resilience and security of company resources and assets;
B. Information and communication technology (ICT) resilience and security management over the whole life cycle;
C. Adequate resilience and security of the industrial automation and control system (IACS) and supervisory control and data acquisition (SCADA) system in a specific industrial network/domain and required security assurance level (SAL) [26];
D. Safety-related control systems designed and operated according to the functional safety concept with the required safety integrity level (SIL) [27];
E. Industrial installations and processes with the required physical and functional protection measures;
F. Infrastructure integrity for delivery of raw materials and energy (electricity, gas, oil) needed for production processes;
G. Equipment reliability/availability adequately maintained according to the strategy developed to achieve, for instance, a satisfactory level of overall equipment effectiveness (OEE).

These systems and networks require special attention during the design and operation of Industry 4.0 manufacturing systems due to their complexity, advanced functionality, and external communications. Their architectural complexity and openness make them susceptible to malfunctions and failures as well as vulnerable to external cyberattacks. According to published data, the probability of such attacks on various industrial systems and networks in most European countries is relatively high.

Due to the scope of the problems outlined above, only selected issues will be discussed. In the following sections fundamental aspects related to the Industry 4.0 concept are presented, namely, ICT systems and networks (B in Figure 5), ICS/SCADA resilience and security (C), and safety-related ICS (D) designed for implementing the defined safety functions [27,42,53,54] of the required safety integrity level (SIL) of a safety function in order to reduce relevant risks. The determined SIL is then verified using a probabilistic model of the safety-related ICS of the architecture, including communication conduits.

To better illustrate the authors' new approach, Figure 6 shows five framework elements that directly extend the BCM process.

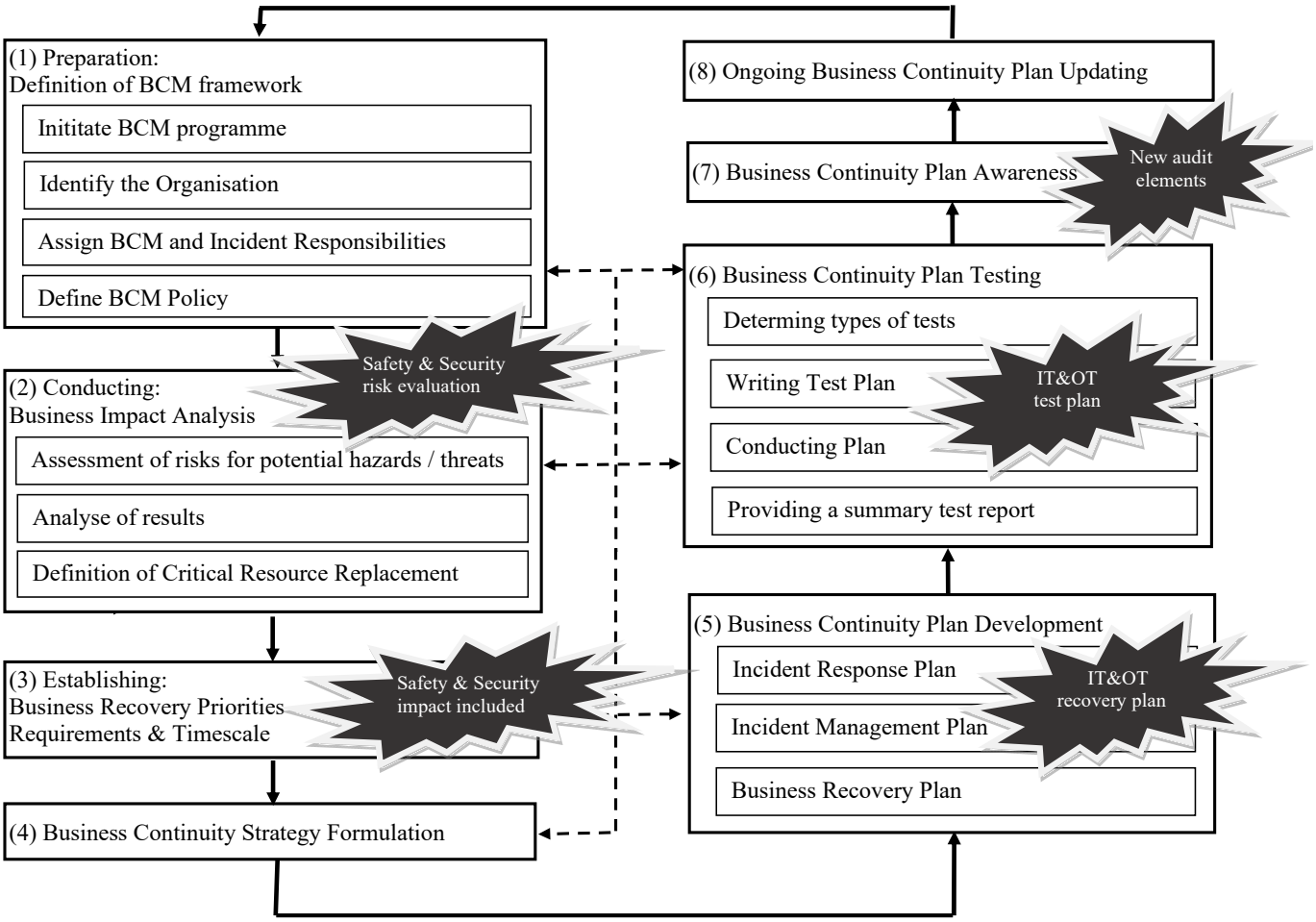


**Figure 6.** Impact of the proposed framework on the BCM process.

The first element of the new approach is to first incorporate the safety and security aspects discussed above into the risk analysis and then throughout the Business Impact Analysis process. The aim of information security management (ISM) is to fulfill specified requirements concerning the CIA triad (Figure 4) of the ICT systems regarding information storage, transfer, and related services. When an organization implements an ISMS (information security management system), the risks of interruptions to business activities for any reason should be identified and evaluated [20,55].

In the third step of the BCM process (Establishing), the conclusions of Step 2 should be considered, including new safety and cybersecurity aspects.

During development of the Business Continuity Plan, the dependencies of IT on OT and their impact on functional safety must first be considered; second, the impact of these events on the recovery plan must be assessed. Planning for business continuity, fallback arrangements for information processing, and communication facilities become beneficial during periods of minor outages and are essential for ensuring information and service availability during a major failure or disaster that requires complete and effective recovery of activities over a period of time.

The fourth important link in the proposed framework is the inclusion of aspects of the risk analysis and the prepared recovery plan in the process of periodic testing and verification.

The last new element appears in the final two steps of the BCM cycle. As previously mentioned, audits are of key importance in any management system, especially in a hazardous industrial plant. Previous authors have examined audit documentation prepared and used by an industrial company as part of a third-party audit in a refinery concerning

the design and operation of safety-related ICS in relation to defined generic and plant criteria [56]. The audit results and conclusions were then discussed with the staff responsible for functional safety to further mitigate risks by implementing the indicated technical and organizational solutions. An important objective in implementing a BCM in a hazardous plant is to satisfy the expectations of stakeholders and insurance companies [10,11] in order to assure a satisfactory level of business continuity, safety, and security. This can be achieved thanks to the implementation in industrial practice of advanced, consistent and effective BCM systems.

Thus, the BCM is useful in taking a systemic and proactive approach to dealing with dependability, safety, and security issues. It specifies various interrelated process-based activities and procedures for the identification of hazards and threats in order to evaluate relevant risks, supporting safety and security-related decision-making in changing conditions and over the whole plant life cycle.

## 4. Case Study

### *4.1. Safety Aspects*

The risk analysis phase of a plant's BCM takes into account the continuity of the media supply, which is directly linked to the plant's gas boiler room. As part of the functional safety and cybersecurity risk analysis, analyses were performed as a basis for this risk analysis. In this example, only one of the safety functions is presented. A safety function of high-pressure monitoring operating in the low demand mode in a process installation is presented. The high pressure of the steam in the process loop provokes the safety function to drop power to a pair of solenoid valves, which leads to venting to a pneumatic actuator, placing a pair of valves into their failsafe position. From the risk evaluation, the safety integrity level of this function was determined to be SIL 3. The safety function to be implemented in the safety-related ICS architecture is shown in Figures 7 and 8. The related at BCM framework, including the safety and security aspects, is shown in Figure 9.

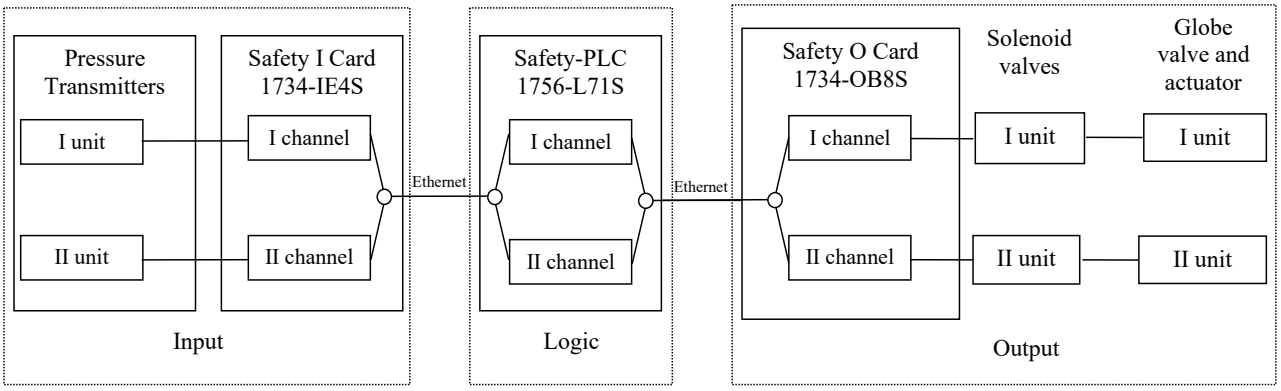


**Figure 7.** The architecture of the ICS system with implemented safety function.

In the analysed example, the 4–20 mA two-wire pressure transmitters are directly wired into analog input modules. The safety controller and the input and output cards are connected on an EtherNet/IP network. The final control elements of this safety function are the combination of solenoids, actuators, and globe valves. The controller and safety I/O modules have a built-in HFT = 1 (two field signals are used). The sensors and final elements require redundant hardware in the 1oo2 configuration to meet the required HFT = 1. The data for evaluating the probability of failure on demand average $PFD_{avg}$ of subsystems was calculated by the authors based on data provided by manufacturers of the components (Table 4).

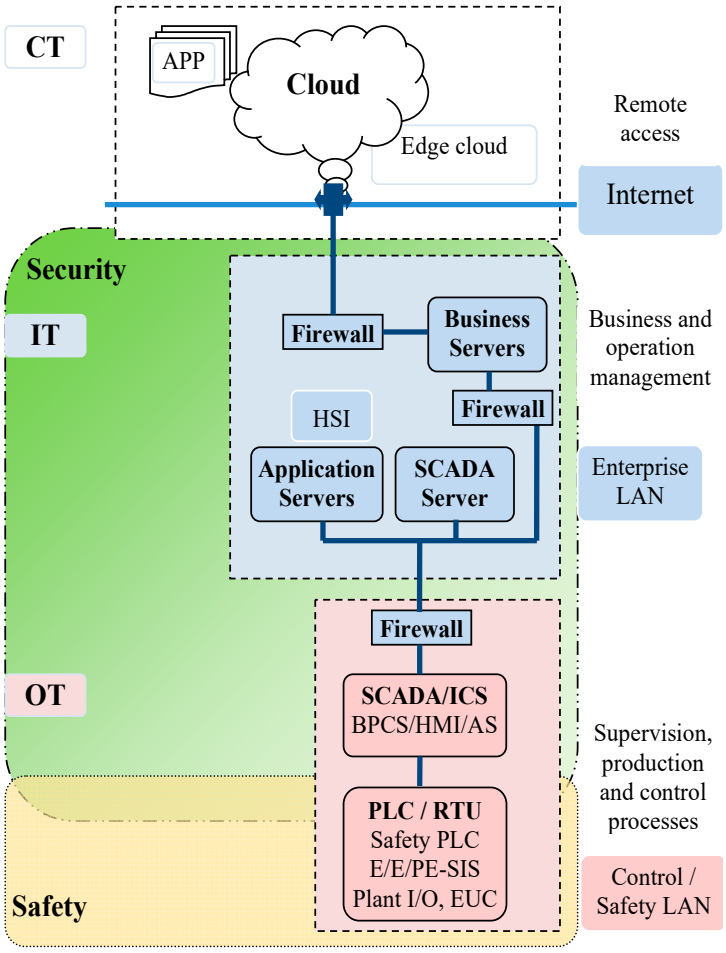


**Figure 8.** Analysed object architecture.

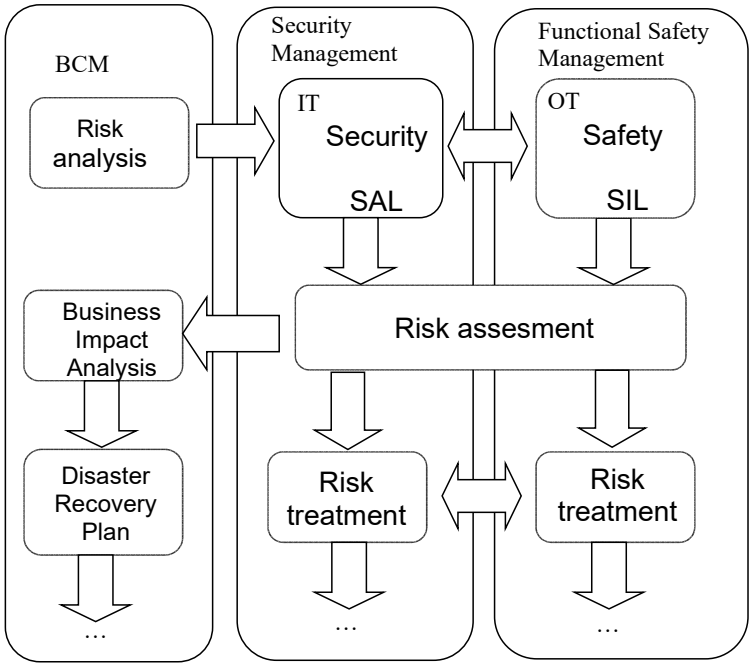


**Figure 9.** Diagram of relations of BCM framework, including safety and security aspects.

**Table 4.** Reliability data for safety-related ICS components for implementing the safety function.

| Subsystem | SIL | $PFD_{avg}$ |
|---|---|---|
| **A**. Input subsystem<br>Pressure transmitter<br>Analog Input Card | SIL 4 | $3.1 \times 10^{-5}$ |
| **B**. Logic subsystem<br>Safety PLC | SIL 4 | $3.5 \times 10^{-5}$ |
| **C**. Output subsystem<br>Digital Output Card<br>Solenoid valve<br>Globe valve &<br>Pneumatic Actuator | SIL 4 | $4.6 \times 10^{-5}$ |

The value of $PFD_{avg}$ for the considered safety-related ICS is calculated from the formula [39]:

$$PFD_{avg} \cong PFD_{avg}^{A} + PFD_{avg}^{B} + PFD_{avg}^{C} \quad (4)$$

Thus, in this case study, $PFD_{avg} \cong 11.2 \times 10^{-5}$; the safety integrity level of SIL 3 was obtained via the results of probabilistic modelling, with the interval criteria presented in the second column of Table 1 and the architecture constraints presented in the IEC 61508 series standard.

### *4.2. Safety-Related ICS Aspects*

Considering the domain of the safety-related ICS in which the safety function was implemented, including the communication conduits, the SL-A vector was evaluated as follows: (3 4 3 3 3 3 4). Assuming that weights of all $SL_i$ are equal ($w_i$ = 1/7), using Equation (3) the obtained result is $SI^{Do}$ = 3.28 and the assigned security assurance level is SAL 3. From column 4 of Table 3, the final safety integrity level validated regarding the security aspects in the domain of interest is SIL 3, the same as required. Therefore, in this case there is no need to propose improvements to the safety-related system [40]. If the SAL obtained for another less secure domain was lower, e.g., SAL 2, then the assigned safety integrity level should be lower, i.e., SIL 2 (see Table 3).

### *4.3. Risk Treatment*

From a risk management point of view, it would be justified to consider changing the configuration of the sensor subsystem shown in Figure 7 from 1oo2 to 2oo3 in order to reduce the probability of spurious operation of this safety-related ICS. It is known that while the 2oo3 configuration has a slightly higher $PFD_{avg}$, it has a much lower probability of spurious operation than configuration 1oo2. Probabilistic modeling of the safety-related ICS consisting of the 2oo3 configuration, including the influence of CCFs and the architectural constrains on subsystems regarding their HFT and $S_{FF}$, is described in detail in [25,43].

### *4.4. Business Continuity Management Impact*

Based on the information previously mentioned in the example above, the team can assess the impact of system architecture and functional and cybersafety safeguards on the criticality of the gas boiler, which translates into the BCM of the entire plant. This in turn allows the enterprise to engage in Business Continuity Planning-wide planning, e.g., creating the capacity to produce a range of products in several factories.

The next stage of BCM is to create a business recovery plan that includes both IT and OT infrastructure. As IT practices are well known, we omit the related description. As far as OT is concerned, especially in terms of functional safety, it is necessary to highlight the creation of backup programs of drivers and safety drivers, knowledge of firmware versions of devices of control systems, protection of spare parts of control elements which

can be destroyed or infected, description of procedures verifying damage, and procedures allowing for the restarting of production after replacement of damaged or infected elements.

The final stage of the BCM process, enriched with new analysis elements, is the test plan. At this stage, it is necessary to equip maintenance personnel with appropriate procedures and instructions to test the disaster event and production recovery in a safe way for the continuity of production in the scope resulting from the risk analysis enriched with functional safety elements for OT and IT.

The frequency of performing a backup depends directly on the Recovery Point Objective (RPO) indicator assumed during the analysis. However, the size of the stock of key spare parts depends on the adopted Recovery Time Objective (RTO)

### *4.5. Summary*

This example demonstrates that in a modern industrial plant equipped with both safety functions and IT networks, these two functionalities intermingle and create interactions that have a direct impact on BCM analyses. Their consideration is essential for a comprehensive analysis of all risks and the creation of an appropriate action plan.

## 5. Conclusions

In this article, an integrated functional safety and cybersecurity evaluation approach is proposed in a framework for business continuity management (BCM) to deal systematically with vulnerabilities that could influence an industrial plant's dependability, safety, and security. Industrial energy companies, including those using Industry 4.0 business and technical solutions, have to pay attention to shaping their resilience regarding existing and emerging hazards and threats, including cyberattacks. This issue concerns the energy sector, power plants, and distributed renewable energy stations.

In such energy plants, information and communication technologies (ICT) and industrial automation and control systems (IACS) play important roles. Using advanced technologies in modern energy manufacturing systems and processing plants can result in management impediments due to their openness to external systems and networks through various communication channels. This makes company assets and resources potentially vulnerable to risk, e.g., due to cyberattacks. In the BCM-oriented approach proposed here, both preventive and recovery activities are considered in light of engineering best practices and following suggested selected international standards, reports, and domain publications.

Potential impediments in energy industrial practice have been identified related to OT security when this technology consists of devices (hardware and software) from several different producers/suppliers. This can cause substantial difficulties in pathing software within relevant computer systems and networks. Thus, this issue requires special attention during the design, implementation, and maintenance of business continuity management systems.

The dependability and security of safety-related ICS in which defined safety functions are implemented can be influenced by both technical and organizational factors. These are related to the quality and reliability of hardware and software. These aspects require further research, especially in the context of the design and operation of highly complex hazardous industrial installations and their ICS, as these must be designed with regard to the defense in depth concept when justified in the context of the risk evaluation results obtained.

Traditionally, manufacturing installations include both information technology (IT) and operational technology (OT). More recently, cloud technology (CT) is often considered to improve data transfer and storage in the context of business management in distributed Industry 4.0 companies.

Advanced automation and control systems are currently in development, based, for instance, on the open platform communication unified architecture (OPC UA) protocol for improved network scalability and implementing new AutomationML concepts [49]. These technologies enable advanced production flexibility and effectiveness. The IT, OT, and

IACS, including safety-related ICS, can be considered more generally as a cyber-physical system (CPS). Additional research should be undertaken in order to deal systematically with distributed co-operating manufacturing systems, including their dependability, safety, and security aspects, regarding an advanced BCM system for improving effectiveness and resilience over the whole plant life cycle. Our future research work will further develop BCM topics in the energy sector related to hydrogen storage and renewable energy technologies. With respect to these topics it is extremely important to include an integrated approach to functional safety and cybersecurity analysis.

**Author Contributions:** Conceptualization, K.T.K.; methodology, K.T.K. and M.Ś.; validation, J.P. and E.P.; formal analysis, E.P., J.P. and M.Ś.; investigation, K.T.K., M.Ś., J.P. and E.P.; resources, E.P. and M.Ś.; writing—original draft preparation, K.T.K.; writing—review and editing, E.P., J.P. and M.Ś.; visualization, K.T.K.; supervision, M.Ś., J.P. and E.P. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was supported by Gdańsk University of Technology.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. SIEMENS Industrial Security. Available online: https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html (accessed on 10 June 2021).
2. Abdo, H.; Kaouk, M.; Flaus, J.M.; Masse, F. Safety and Security Risk Analysis Approach to Industrial Control Systems. *Comput. Secur.* **2018**, *72*, 175–195. [CrossRef]
3. Li, S.W. Architecture Alignment and Interoperability, an Industrial Internet Consortium and Platform Industry 4.0. Available online: https://www.iiconsortium.org/pdf/JTG2_Whitepaper_final_20171205.pdf (accessed on 10 June 2021).
4. *ISO/DIS 22301*; Security and Resilience—Business Continuity Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2019.
5. Xing, J.; Zio, E. *An Integrated Framework for Business Continuity Management of Critical Infrastructures*; CRC Press: Boca Raton, FL, USA, 2016; pp. 563–570.
6. Lundteigen, M.A.; Rausand, M.; Utne, I.B. Integrating RAMS engineering and management with the safety life cycle of IEC 61508. *Reliab. Eng. Syst. Saf.* **2009**, *94*, 1894–1903. [CrossRef]
7. Saraswat, S.; Yadava, G.S. An overview on reliability, availability, maintainability and supportability (RAMS) engineering. *Int. J. Qual. Reliab. Manag.* **2008**, *25*, 330–344. [CrossRef]
8. Misra, K.B. (Ed.) *Handbook of Advanced Performability Engineering*; Springer Nature: Cham, Switzerland, 2021.
9. Niemimaa, M. Interdisciplinary Review of Business Continuity from an Information Systems Perspective: Toward an Integrative Framework. *Commun. Assoc. Inf. Syst.* **2015**, *37*, 4. [CrossRef]
10. Gołębiewski, D.; Kosmowski, K. Towards Process-Based Management System for Oil Port Infrastructure in Context of Insurance. *J. Pol. Saf. Reliab. Assoc.* **2017**, *8*, 23–37.
11. Kosmowski, K.T.; Gołębiewski, D. Functional Safety and Cyber Security Analysis for Life Cycle Management of Industrial Control Systems in Hazardous Plants and Oil Port Critical Infrastructure Including Insurance. *J. Pol. Saf. Reliab. Assoc.* **2019**, *10*, 99–126.
12. Kosmowski, K.T. Systems engineering approach to functional safety and cyber security of industrial critical installations. In *Safety and Reliability of Systems and Processes*; Kołowrocki, K., Bogalecka, M., Dąbrowska, E., Torbicki, M., Eds.; Gdynia Maritime University: Gdynia, Poland, 2020; pp. 135–151.
13. *Systems Engineering Fundamentals*; Defense Acquisition University Press: Fort Belvoir, VA, USA, 2001.
14. Białas, A. *Semiformal Common Criteria Compliant IT Security Development Framework*; Studia Informatica; Silesian University of Technology Press: Gliwice, Poland, 2008.
15. Kriaa, S.; Pietre-Cambacedes, L.; Bouissou, M.; Halgand, Y. Approaches Combining Safety and Security for Industrial Control Systems. *Reliab. Eng. Syst. Saf.* **2015**, *139*, 156–178. [CrossRef]
16. CISA Assessments: Cyber Resilience Review. Available online: https://www.cisa.gov/uscert/resources/assessments (accessed on 10 February 2020).
17. Leitão, P.; Colombo, A.W.; Karnouskos, S. Industrial Automation Based on Cyber-Physical Systems Technologies: Prototype Implementations and Challenges. *Comput. Ind.* **2016**, *81*, 11–25. [CrossRef]

18. MERGE. Safety & Security, Recommendations for Security and Safety Co-Engineering, Multi-Concerns Interactions System Engineering. ITEA2 Project No. 11011. Available online: https://itea4.org/project/workpackage/document/download/2837/D3.4.4.%20MERgE%20-%20Recommendations%20for%20Security%20and%20Safety%20Co-engineering%20v3%20partA.pdf (accessed on 1 June 2021).
19. Integrated Design and Evaluation Methodology. Security and Safety Modelling; Artemis JU Grant Agr., No. 2295354. Available online: http://sesamo-project.eu/sites/default/files/downloads/publications/integrated-design-and-evaluation-communication-material.pdf (accessed on 5 June 2018).
20. Boehmer, W.J. Survivability and business continuity management system according to BS 25999. In Proceedings of the IEEE 3rd International Conference on Emerging Security Information, Systems and Technologies, Athens, Greece, 18–23 June 2009; Volume 1, pp. 142–147.
21. Zawiła-Niedźwiecki, J. *Operational Risk Management in Assuring Organization Operational Continuity*; Edu-Libri.: Kraków, Poland, 2013. (In Polish)
22. Cyber Security for Industrial Automation and Control Systems, Health and Safety Executive (HSE) Interpretation of Current Standards on Industrial Communication Network and System Security, and Functional Safety 2015. Available online: https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf (accessed on 5 May 2021).
23. Kosmowski, K.T. Functional safety and cybersecurity analysis and management in smart manufacturing systems. In *Handbook of Advanced Performability Engineering*; Krishna, B.M., Ed.; Springer Nature: Cham, Switzerland, 2021.
24. Kościelny, J.M.; Syfert, M.; Fajdek, B. Modern Measures of Risk Reduction in Industrial Processes. *J. Autom. Mob. Robot. Intell. Syst.* **2019**, *1*, 20–29. [CrossRef]
25. Kosmowski, K.T. *Functional Safety and Reliability Analysis Methodology for Hazardous Industrial Plants*; Gdansk University of Technology Publishers: Gdańsk, Poland, 2013.
26. *IEC 62443*; Security for Industrial Automation and Control Systems. Parts 1–14 (Some Parts in Preparation). The International Electrotechnical Commission: Geneva, Switzerland, 2018.
27. *IEC 61508*; Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems, Parts 1–7. The International Electrotechnical Commission: Geneva, Switzerland, 2016.
28. Gabriel, A.; Ozansoy, C.; Shi, J. Developments in SIL Determination and Calculation. *Reliab. Eng. Syst. Saf.* **2018**, *177*, 148–161. [CrossRef]
29. *BS 25999-1*; Business Continuity Management—Part 1: Code of Practice. British Standard Institution: London, UK, 2006.
30. *SP 800-82r2*; Guide to Industrial Control Systems (ICS) Security. NIST: Gaithersburg, MD, USA, 2015.
31. *ETSI TS 102 165-1*; CYBER Methods and Protocols. Part 1: Method and pro Forma for Threat, Vulnerability, Risk Analysis (TVRA). Technical Specs; ETSI: Sophia Anthipolis, France, 2017.
32. Kosmowski, K.T.; Śliwiński, M. Organizational culture as prerequisite of proactive safety and security management in critical infrastructure systems including hazardous plants and ports. *J. Pol. Saf. Reliab. Assoc.* **2016**, *7*, 133–146.
33. ISA. *Security of Industrial Automation and Control Systems, Quick Start Guide: An Overview of ISA/IEC 62443 Standards*; ISA—International Society of Automation: Alexander, NC, USA, 2020.
34. Saleh, J.H.; Cummings, A.M. Safety in the Mining Industry and the Unfinished Legacy of Mining Accidents. *Saf. Sci.* **2011**, *49*, 764–777. [CrossRef]
35. Subramanian, N.; Zalewski, J. Quantitative Assessment of Safety and Security of System Architectures for Cyberphysical Systems Using NFR Approach. *IEEE Syst. J.* **2016**, *2*, 397–409. [CrossRef]
36. *IEC 61511*; Safety Instrumented Systems for the Process Industry Sector. Parts 1–3. The International Electrotechnical Commission: Geneva, Switzerland, 2016.
37. Holstein, D.K.; Singer, B. *Quantitative Security Measures for Cyber & Safety Security Assurance*; ISA: Alexander, NC, USA, 2010.
38. Śliwiński, M.; Piesik, E.; Piesik, J. Integrated Functional Safety and Cybersecurity Analysis. *IFAC Pap. OnLine* **2018**, *51*, 1263–1270. [CrossRef]
39. *IEC 62061*; Safety of Machinery—Functional Safety of Safety-Related Electrical, Electronic, and Programmable Electronic Control Systems. The International Electrotechnical Commission: Geneva, Switzerland, 2018.
40. Kosmowski, K.T.; Śliwiński, M.; Piesik, J. Integrated Functional Safety and Cybersecurity Analysis Method for Smart Manufacturing Systems. *TASK Q.* **2019**, *23*, 1–31.
41. *IEC 63074*; Security Aspects Related to Functional Safety of Safety-Related Control Systems. The International Electrotechnical Commission: Geneva, Switzerland, 2017.
42. Braband, J. What's security level got to do with safety integrity level? In Proceedings of the 8th European Congress on Embedded Real Time Software and Systems, Toulouse, France, 27–29 January 2016.
43. Kosmowski, K.T. Safety integrity verification issues of the control systems for industrial power plants. In Proceedings of the International Conference on Diagnostics of Processes and Systems, Sandomierz, Poland, 11–13 September 2017; pp. 420–433.
44. *ISO/IEC 24762*; Information Technology—Security Techniques—Guidelines for Information and Communications Technology Disaster Recovery Services. International Organization for Standardization: Geneva, Switzerland, 2008.
45. *ISO/DTR 22100*; Safety of Machinery—Guidance to Machinery Manufacturers for Consideration of Related IT Security (Cyber Security) Aspects. International Organization for Standardization: Geneva, Switzerland, 2018.

46. *IEC TR 63074*; Safety of Machinery—Security Aspects to Functional Safety of Safety-Related Control Systems. The International Electrotechnical Commission: Geneva, Switzerland, 2019.
47. *ISO/IEC 27005*; Information Technology—Security Techniques—Information Security Risk Management. International Organization for Standardization: Geneva, Switzerland, 2018.
48. *BSI-Standard 100-4*; Business Continuity Management. Federal Office for Information Security (BSI): Berlin, Germany, 2009.
49. *ISO/PAS 22399*; Societal Security—Guideline for Incident Preparedness and Operational Continuity Management. International Organization for Standardization: Geneva, Switzerland, 2007.
50. *ISO/IEC 27031*; Information Technology—Security Techniques—Guidelines for Information and Communication Technology Readiness for Business Continuity. International Organization for Standardization: Geneva, Switzerland, 2011.
51. Kanamaru, H. Bridging functional safety and cyber security of SIS/SCS. In Proceedings of the IEEE 56th Annual Conference of the Society of Instrument and Control Engineers of Japan, Kanazawa, Japan, 19–22 September 2017.
52. Smith, D.J. *Reliability, Maintainability and Risk. Practical Methods for Engineers*, 9th ed.; Butterworth-Heinemann: Oxford, UK, 2017.
53. Piesik, E.; Śliwiński, M.; Barnert, T. Determining the Safety Integrity Level of Systems with Security Aspects. *Reliab. Eng. Syst. Saf.* **2016**, *152*, 259–272. [CrossRef]
54. Kosmowski, K.T.; Śliwiński, M. *Knowledge-Based Functional Safety and Security Management in Hazardous Industrial Plants with Emphasis on Human Factors*; Advanced Control and Diagnostic Systems; PWNT: Gdańsk, Poland, 2015.
55. Felser, M.; Rentschler, M.; Kleinberg, O. Coexistence standardisation of operational technology and information technology. *Proc. IEEE* **2019**, *104*, 962–976. [CrossRef]
56. Rogala, I.; Kosmowski, K.T. *Audit Document Concerning Organizational and Technical Aspects of the Safety-Related Control System Design and Operation at a Refinery (Access Restricted)*; Automatic Systems Engineering, Gdańsk and Gdańsk University of Technology: Gdańsk, Poland, 2012.