

Article

Assessing the Operation System of Fire Alarm Systems for Detection Line and Circuit Devices with Various Damage Intensities

Jacek Paś¹ , Adam Rosiński^{2,*} , Michał Wiśnios¹ and Marek Stawowy² 

¹ Division of Electronic Systems Exploitations, Faculty of Electronics, Institute of Electronic Systems, Military University of Technology, 2 Gen. S. Kaliski St, 00-908 Warsaw, Poland; jacek.pas@wat.edu.pl (J.P.); michal.wisnios@wat.edu.pl (M.W.)

² Division Telecommunications in Transport, Faculty of Transport, Warsaw University of Technology, 75 Koszykowa St, 00-662 Warsaw, Poland; marek.stawowy@pw.edu.pl

* Correspondence: adam.rosinski@pw.edu.pl

Abstract: The paper presents a method for assessing operation processes for Fire Alarm Systems (FAS) applied in civil structures, based on use analysis. Individual FAS devices include components with varying ‘lifetimes’ and damage intensities λ . This is because these elements are operated in different internal and external environments. Probability distributions with various damage λ and recovery μ intensity values must, hence, be taken into account for the FAS operation process and to determine the $R(t)$ reliability. The life cycle of elements comprising a FAS can be divided into three distinguishing time periods. The first is the so-called ‘childhood’. The second, the longest, is characterized by damage intensity $\lambda = \text{const}$, and the third period is where FAS is unfit more frequently. Based on knowledge of actual FAS operation process data, it is possible to determine damage λ and recovery μ intensity parameters. Such data can be employed to determine FAS reliability parameters within the presented service life intervals. The authors of the article first discuss the basic issues associated with FAS, followed by analyzing the current status of the topic. They also present power supply matters and system solution examples, develop an operation process model and determine selected operational indicators for the structures in question. The paper ends with conclusions.

Keywords: fire alarm system; damage intensity; recovery intensity; system model; reliability



Citation: Paś, J.; Rosiński, A.; Wiśnios, M.; Stawowy, M. Assessing the Operation System of Fire Alarm Systems for Detection Line and Circuit Devices with Various Damage Intensities. *Energies* **2022**, *15*, 3066. <https://doi.org/10.3390/en15093066>

Academic Editor: Maria Founti

Received: 18 March 2022

Accepted: 21 April 2022

Published: 22 April 2022

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Fire alarm systems (FAS) are some of the most important electronic security systems (ESS) currently used in civil structures [1,2] that are either:

- stationary, i.e., set permanently on the ground (foundations), such as critical infrastructure buildings (CIB), warehouses, airports and seaports, logistics hubs, train stations, stadiums, shopping centers, etc. [3];
- non-stationary (not permanently bonded with the ground)—e.g., aircraft, ships or other vessels, locomotives, passenger and freight rail carriages, trucks intended for material transport, etc. [4].

FAS are ESSs, the use of which in technical, stationary or non-stationary facilities is governed by specific legal regulations and standards—national and international. Pursuant to the regulation of the European Parliament (EP) and of the Council of the European Union (EU) No. 305—CPR dated 9 March 2011, as FAS modules, devices and components shall be treated and marketed in such countries as building materials, similarly to such items as i.e., joists [5,6]. This is why they should have specific national and international certificates.

FAS implement the most important security functions within these facilities. This is associated with the protection of the life and health of people that use such buildings, the environment where the buildings are operated, as well as movable and fixed property

stored in facilities supervised by FAS—Figure 1. All elements, devices and modules that are FAS operation components are necessary in the context of facility fire safety. Using FAS in given stationary or non-stationary facilities, and their proper operational supervision (e.g., implementation of preventive inspections within set time intervals) results from the relevant legal provisions applicable in individual countries—Figure 1 [1,7].

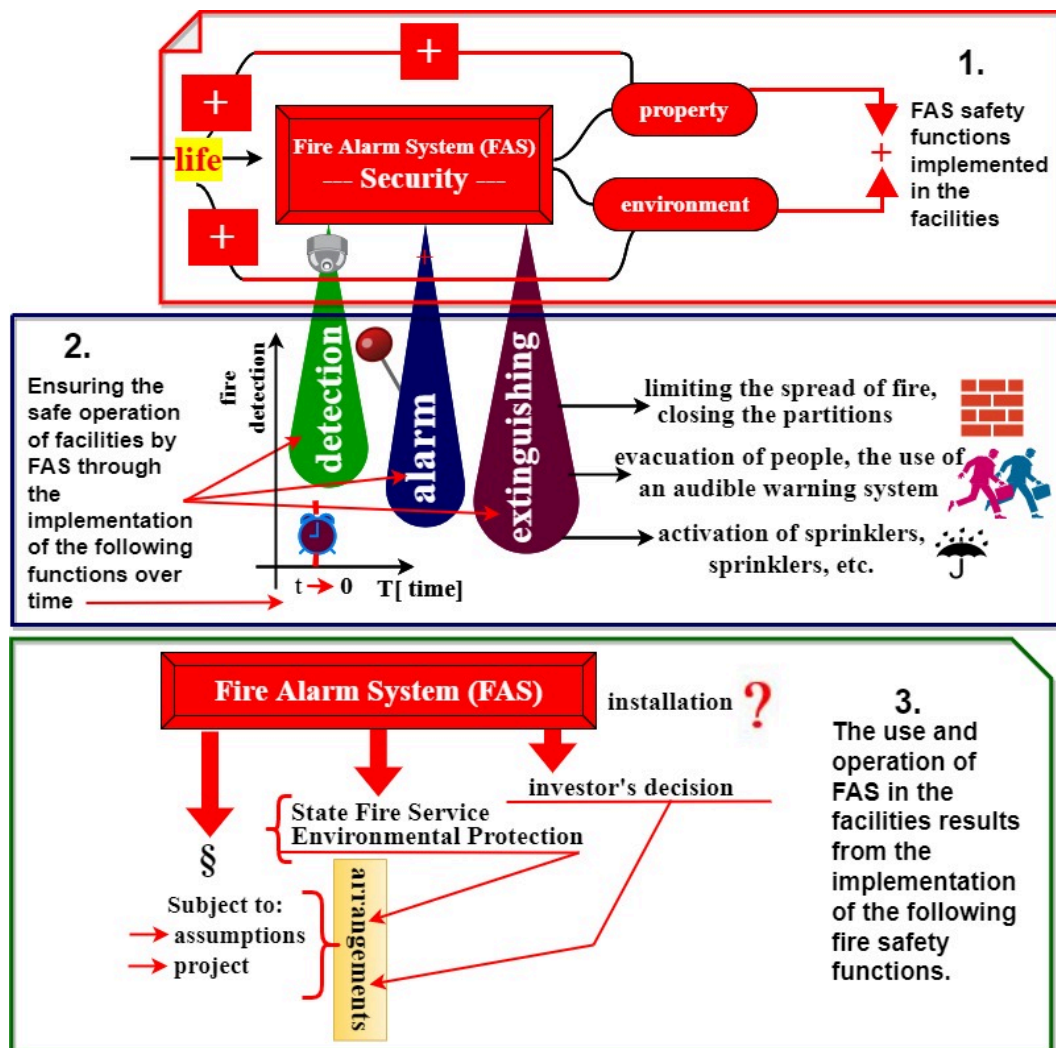


Figure 1. Fire safety and FAS use requirements in various facilities. Design, installation and subsequent operation, including servicing of FAS within specific civil structures and non-stationary technical facilities are governed by relevant legal conditions and recommendations of authorities responsible for fire supervision within a given country (e.g., State Fire Service (PSP—Państwowa Straż Pożarna) in Poland) or the very need to protect the external environment surrounding buildings covered by system supervision—Figure 1. The facility Investor itself can also decide to install FAS within a given facility for security's sake and, e.g., in the light of a discount in terms of insuring such building(s). The essential role of FAS operated within such facilities includes both active and passive protection of life, health and property, as well as the environment, triggering fire suppression through activating fixed fire extinguishers (FEE)—Figure 1. Not all electronic security systems used by humans provide such a wide range of protection measures against undesirable external or internal forced impacts within operated stationary or non-stationary facilities. Please also note the very important economic aspect of using FAS in such facilities. Sounding an alarm in, e.g., a railway or aviation facility means suspending traffic, evacuating people, closing a railway station or platforms, PSP arrival, mobilizing certain employees to take specific actions associated with the threat and the very fire suppression process—activating FFEs or the gas suppression system (GSS).

Activating the suppression process is also associated later with the process of restoring the initial state of a given facility, e.g., removing gas from the server room, transformer station or selected rooms. Even the so-called false alarm event in a FAS entails similar financial consequences [1,8]. Restoring railway traffic, reopening a given transport facility and setting all FAS equipment into detection state after a temporary alarm state requires incurring specific financial outlays and time, which is crucial in the case of transport hubs.

The above is only an example for a single facility type of the so-called state's critical infrastructure, but also company and bank buildings or power switching stations with integrated security or user comfort control systems are exposed to such forced events. After the FAS goes into an alarm state, the aforementioned facilities also generate considerable financial costs associated with temporary decommissioning. This is why, already at the FAS engineering stage, particular attention should be paid to its functional reliability. It will be operated under various external and internal environmental conditions, existing technical and organizational (service) restrictions and the use of certain firefighting elements, modules or devices. This also includes existing interference, such as mechanical—vibrations or electromagnetic [1,9]. Designing and implementing specific FAS technical structures in buildings requires the application of all available principles (solutions) that increase functional reliability—e.g., redundancy, reserves, fail-safe principle or the alarming and control procedure or organization, etc. [10,11]. People have great influence on the aforementioned technical solutions—from FAS development, engineering, through installation to commissioning. However, there are also random factors that are beyond the control of people responsible for operating the system. Changing physical parameters of the environment (temperature, humidity or pressure), architectonic changes within the facility or the very important technical recovery process ensured by service personnel are often random processes. The maintenance team (service) is especially responsible for upkeeping a certain FAS functional reliability level through the implementation of timely preventive maintenance, and replacing unfit components, modules or devices with fit ones. The aforementioned technical facilities used to implement the recovery process are not always obtained directly from the manufacturer. In such a case, these elements have a practically “zero” service life. In the event of FAS unfitness, the most significant factor that restricts restoring its fitness is time. In the case of large, extensive (so-called ‘distributed’) FAS systems, the service team always has a spare part storage within the facility. However, FAS components or constituent devices may be stored under various environmental conditions or exhibit a specific service life (they are not new). In such a case, a given FAS operation process, after determining the reliability of this system, shall take into account the initial damage intensity value λ for this element or device, i.e., reliability $R_{tx}(t)$, where: t_x —time corresponding to a specified initial value of probability, determined upon the commencement of the operation process for a given technical structure within the FAS [12,13].

Currently used FAS exhibit various technical and functional structures that are a complex function of numerous variables, e.g., building geometrical dimensions, the cubature of the civil structure itself expressed in, e.g., $[m^3]$, type of property accumulated within the building (electrical and electronic devices, archives, museum exhibitions, etc.), area of the building(s) expressed in, e.g., m^2 , the very purpose of these buildings—fuel storages, transport and general use facilities—cinemas, theatres or so-called ‘critical infrastructure facilities’. The manner of individual room fit-out and internal architecture, i.e., flat and complex ceilings or the implementation and solutions associated with communication routes also significantly impact the use of specific FAS structures. Based on technical solutions, all currently operated FAS can be divided into three basic structures:

- simple, with a focused structure, where all detection, control and alarm lines and circuits start and end at the fire alarm control unit (FACU). These solutions are preferred in small civil structures, where the fire control matrix implemented by FACU is not too extensive and complex.
- distributed, used in large civil structures or within a vast area with several or even several hundred different buildings. The number of the elements themselves, as well

as the control matrix and fire scenario for such a facility are very advanced. This is why an appropriately organized and connected network of FACUs supervising the entire facility operation process is used. A system with such a structure is scalable, which enables its easy expansion or retrofitting.

- mixed, which is a combination of the two technical solutions above. Used in practice in the case of various civil structures with different, but significant security priorities, e.g., in a part of a protected, vast area with CIBs, fuel storages, explosive storages, hangars with aircraft parking places, switching and transformer stations with fixed gas suppression systems (GSS) and fixed fire extinguishers (FEE)—e.g., sprinklers, spray nozzles [1,6].

Figure 2 shows a functional diagram for a FAS with a focused structure that takes into account selected detection, control and alarm lines, as well as back-up power supply and an alarm and damage signal transmission device (ADSTD).

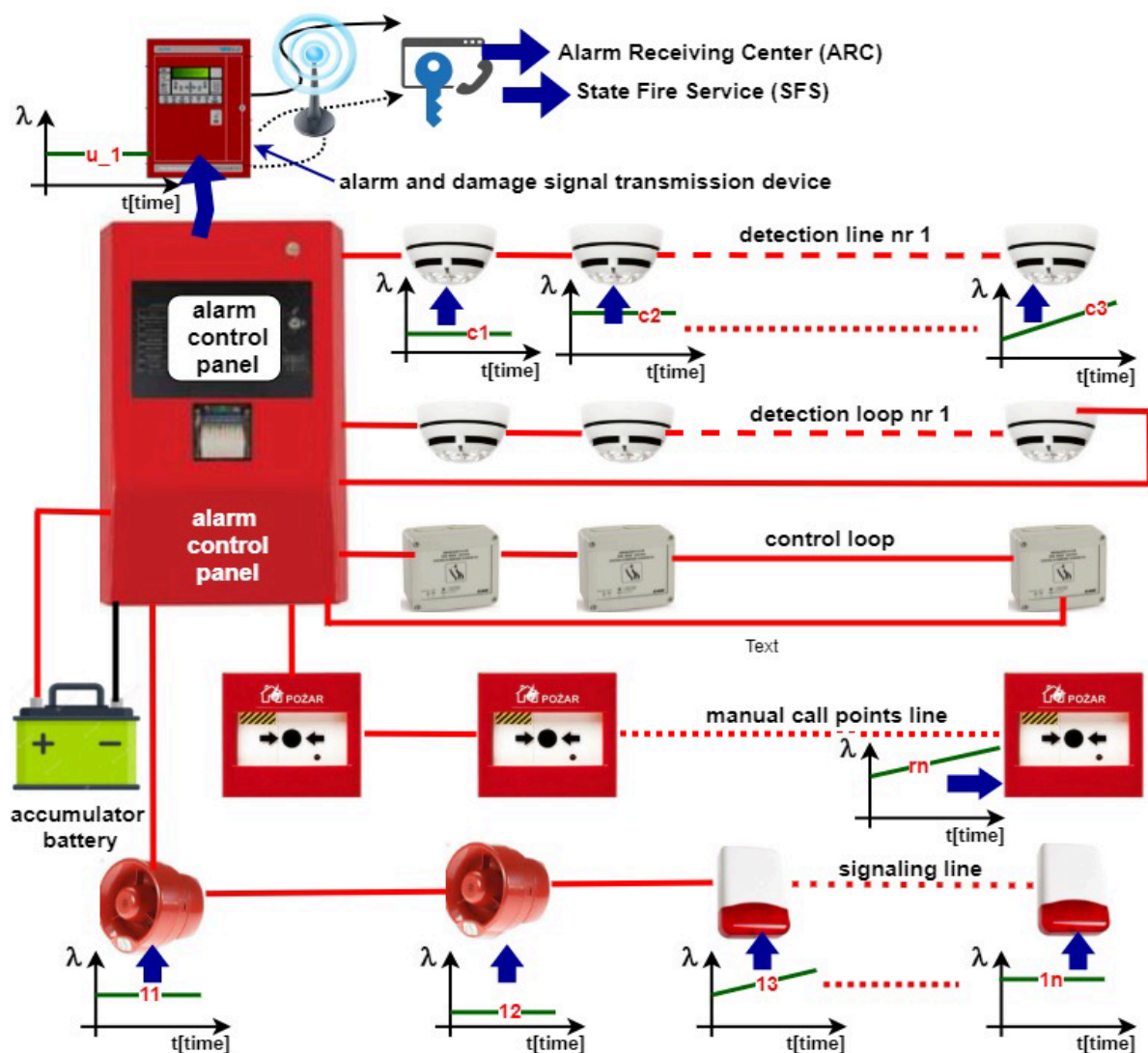


Figure 2. Diagram of a focused FAS, taking into account selected detection circuits and lines with sample damage intensities for individual elements and devices.

The alarm and damage signals within this system are connected to the PSP and an Alarm Receiving Centre (ACR) through an alarm and damage signal transmission device (ADSTD). In addition, the transmission of alarm and damage signals is conducted via two transmission tracks for reliability reasons.

The rest of this article is organized as follows. Section 2 is a critical review of the source literature on the current state of the issue in question. Analysis of the basis matters associated with ESS and FAS power supply constitutes Section 3. Section 4 contains basic information on the damage intensity λ of elements and devices used in FAS. Section 5 presents a reliability and operational analysis of a fire alarm system for detection circuit and line equipment with varying damage intensities. It also includes simulation results. The last, sixth chapter contains conclusions arising from the conducted tests and computer simulations. FAS structure and functionality are directly associated with the control matrix developed based on a fire scenario for a given protected facility. A fire scenario should take into account the fire dynamics within a facility—that is, the construction materials of the building, spreading of flames and combustion products in the facility or fire zone etc. These functions directly and indirectly impact the change in the detection response time and the functioning of the entire FAS, its functional and reliability structure, implemented functionalities, division into detection circuits and lines, etc. The authors of the article included the application of flameproof materials in a given FAS reliability structure, directly resulting from the control matrix developed for a given fire scenario that should take into account the aforementioned building properties.

2. Literature Review

Influence of environmental conditions on FAS. Variability in environmental conditions, including temperature changes, in particular, is one of the important factors encountered in the so-called ‘fire triangle’, which enables detecting a fire, but also leads to a straightforward change in the damage intensity λ . This operating parameter λ directly impacts the reliability of FAS elements, modules and devices. This is why the authors of [14–17] discuss temperature-based reliability analysis covering the key electronic subsystems of devices and systems. The conducted analysis enables optimization and arrangement of electronic elements on a PCB. The temperature simulation related to the issues above is executed using so-called ‘finite’ elements—FEM (Finite Element Modelling) [4,16]. These articles are based on the Ansys computer analysis. However, this relates to a single electronic module used at a certain place within the system.

In the case of distributed FAS [1,18–20], the elements of which are located in different rooms, environmental changes inside and outside of buildings will significantly impact the functional reliability of different system components [21–23]. Temperature is one of the environmental factors that determines damage intensity λ , thus the reliability of the entire FAS [24,25]. The operational tests involving selected FAS conducted by the authors enable assessing the impact of this parameter on reliability through defining e.g., damage intensities λ or the very process of μ recovery [26–29].

For the proper functioning of a FAS, it is also important to determine the global influence of environmental conditions on FAS operation. This is associated with the correct selection of fire detectors, which do not only react to a fire event, but also operational reliability [30–32]. Through their research on fire detectors, the mentioned authors developed a dynamic description of the impact of changes in the fire characteristic values (FCV) on the very detection phenomenon. However, this was not followed up by any reliability studies on, e.g., temperature or humidity characteristics of electronic subassemblies or the entire FAS [33,34]. The authors of the articles [35,36], having FAS damage statistics and a variable recovery process of system elements and devices, were able to determine damage intensities for detectors, modules, devices or elements.

Diagnosing and the impact of disturbances on the functioning of FAS. An important issue related to security systems, and also FAS, is the very process of diagnosing their technical condition [37–40]. These papers, however, only discuss the general assumptions for measuring systems implementing this process in static or dynamic conditions, or for measurements of specific technical conditions using various diagnostic techniques. The aforementioned also did not take into account the impact of various natural or artificial interferences that result from the application of long detection, control, signaling, alarm and

transmission circuits and lines [41–44]. The authors of this article minimized such errors. The execution of actual FAS tests enabled avoiding these mistakes. This was achieved through observing output signals in fire alarm control units (FACU), where the process of conditioning and developing output waveforms takes place. It should be noted that the FACU determines (develops) an output signal with information on the damage [1,15,21].

Important, reliability-impacting issues that should be taken into account within the FAS operating process are electromagnetic interference [27,45], maximum permissible temperature changes in building rooms with installed detectors [46,47], as well as changes to accelerations, vibrations and shocks in electronic elements [48,49]. In the case of the studies discussed above, individual factors disturbing the FAS operation process were always considered separately. The authors of the article conducted actual FAS tests, and the interference was taken into account for all detection lines and circuits hooked up to the FACU. In the course of the tests conducted by the authors, it was also physically possible for a given fire alarm control unit to authenticate the interference or damage signal/alarm in a given room through practical event verification.

Reliability and transmission of utility signals in FAS. The authors of [50–52] conducted quality and reliability studies involving the power supply of FAS, as well as selected electronic security systems. However, the authors only discussed general technical requirements related to power supply, including its quality. No studies regarding FAS power supply were presented [1,14]. In the course of conducting operational tests, the authors of this article also considered transitions of the system to backup power supply. These tests were taken into account when the authors calculated selected operational indicators, i.e., damage λ and μ recovery intensities in FAS.

A very noteworthy issue within the operation process is the transmission of alarm and damage signals [53–55]. The authors of the listed articles focused only on reliability, quality, availability or transmission time to remote PSP or ACR points. The authors of the article analyzed the notification and reaction of service personnel to a damage signal. This parameter was taken into account in the FAS μ recovery intensity, as this is important in terms of restoring FAS to its fit state [1,56].

Performance of the FAS—e.g., false alarms. The authors of [57–60] present several diverse methods for reducing the probability of a false alarm and increasing the functional reliability of detectors for various signals not associated with FCV. Modern techniques are applied within these solutions. They include, e.g., a concept related to fuzzy sets, neural networks, multisensor, optical or laser detectors, etc. The authors took into account the application of these solutions through conducting FAS analysis and operational tests. These parameters are considered in FAS operational graphs and models, as well as numerical values for the indicators of λ damage and μ repair intensities.

FAS implement individual tasks related to the protection of the health and life of people in the facilities, which is why they should be characterized by a reliability level assigned to the hardware domain [61–63]. The decision on the alarm system condition within the protected area should be properly developed based on detector signals [1,64,65]. The second of the aforementioned aspects discussed in the article can be considered as a diagnostic and measurement issue, included within the FAS operation process. Conducting actual FAS studies by the authors of the article was hindered by access to actual critical infrastructure buildings and the systems operated therein.

Available literature sources [66–69] discuss various technical and organizational issues related to the very process of FAS operation. The problem associated with minimizing the probability of a false alarm through the use of appropriate detectors, e.g., a linear smoke detector, should be taken into account at the engineering stage and during the operation process itself [1,15,25]. The authors of the article do not address these issues. However, FAS operational analysis and the presented study results may be useful for the designers and users of such systems—e.g., selecting a given FAS reliability structure or analyzing signals associated with a false alarm. Such analysis has not yet been conducted in this field. This is

a consequence of discussions with companies, FAS users and people supervising the use operation and service processes.

3. Power Supply Analysis for Electronic Security Systems

Ensuring appropriate voltage value and the reliability of its supply to elements and devices within electronic security systems is the basic prerequisite for the correct functioning of all the aforementioned technical facilities [1,6,43]. All electronic security systems are supplied with 12 V DC from an industrial power network through a specific power supply type. This excludes fire alarm systems that require 24 V due to the values of working currents flowing in specific FAS devices—e.g., smoke exhaust dampers, opening/closing drives for doors, fire windows, acoustic and optical signaling devices, etc. [1,9,10]. A power balance for specific (required) detection and alarm times in the case of a primary power (power grid) failure is developed for all electronic security systems.

These times depend on the class of security systems (I–IV), which should operate for a certain period of time in the case of a primary power failure. The determination of the power balance, which takes into account specific values of detection and alarm currents that flow through the lines and circuits of specific ESS is followed by the determination of battery capacity value(s). Such a battery is treated as a backup power supply for these systems. The capacity, expressed in [Ah], is a function of many variables—e.g., load current in two technical states (detection, alarm), length L [m] of lines and circuits with connected detectors, control modules, signaling devices; internal and external (temperature) environment, permissible values of voltage drops on ESS lines and devices for which these objects implement their functionalities, etc. [1,9,35,43].

The issue of ESS power supply is crucial due to the functions of these systems—protection of life, health, property and the environment where humans function. All ESS battery banks are located as close to the alarm control unit as possible and are usually enclosed in a metal cabinet, the contacts of which are monitored by anti-tampering circuits. Battery voltage value is always monitored by the diagnostics system located in the alarm control unit. When this parameter is too low, it is reported as a fault to the alarm receiving center (ACR), service personnel and persons responsible for ongoing technical monitoring of the civil structure [9,35,43]. Besides these two methods for ensuring ESS power supply, the ESS functioning within the so-called ‘state critical infrastructure’ also operates using power supplied from generators and UPS devices. In addition, in the event of a power failure of power line L1, a backup power switch automatically changes over to the L2 power supply line (ensured supply from a different power plant).

Figure 3 shows an ESS power supply diagram for two cases: systems supplied with 12 V, which include an intrusion detection system (IDS-SSWiN), access control system (ACS-SKD), closed-circuit television (CCTV), entry/exit biometry systems (BS-SB); and with a 24 V fire alarm system (FAS-SSP) and an acoustic warning system (AWS-DSO) [1,6,18]. The backup power source in an ESS is always diagnosed in terms of voltage value by the alarm control unit. The value of this parameter can be read from, among others, the system access LCD keyboard panel. This is one of the fundamental ESS diagnostic parameters, visualized in real-time by all systems [1,18,35].

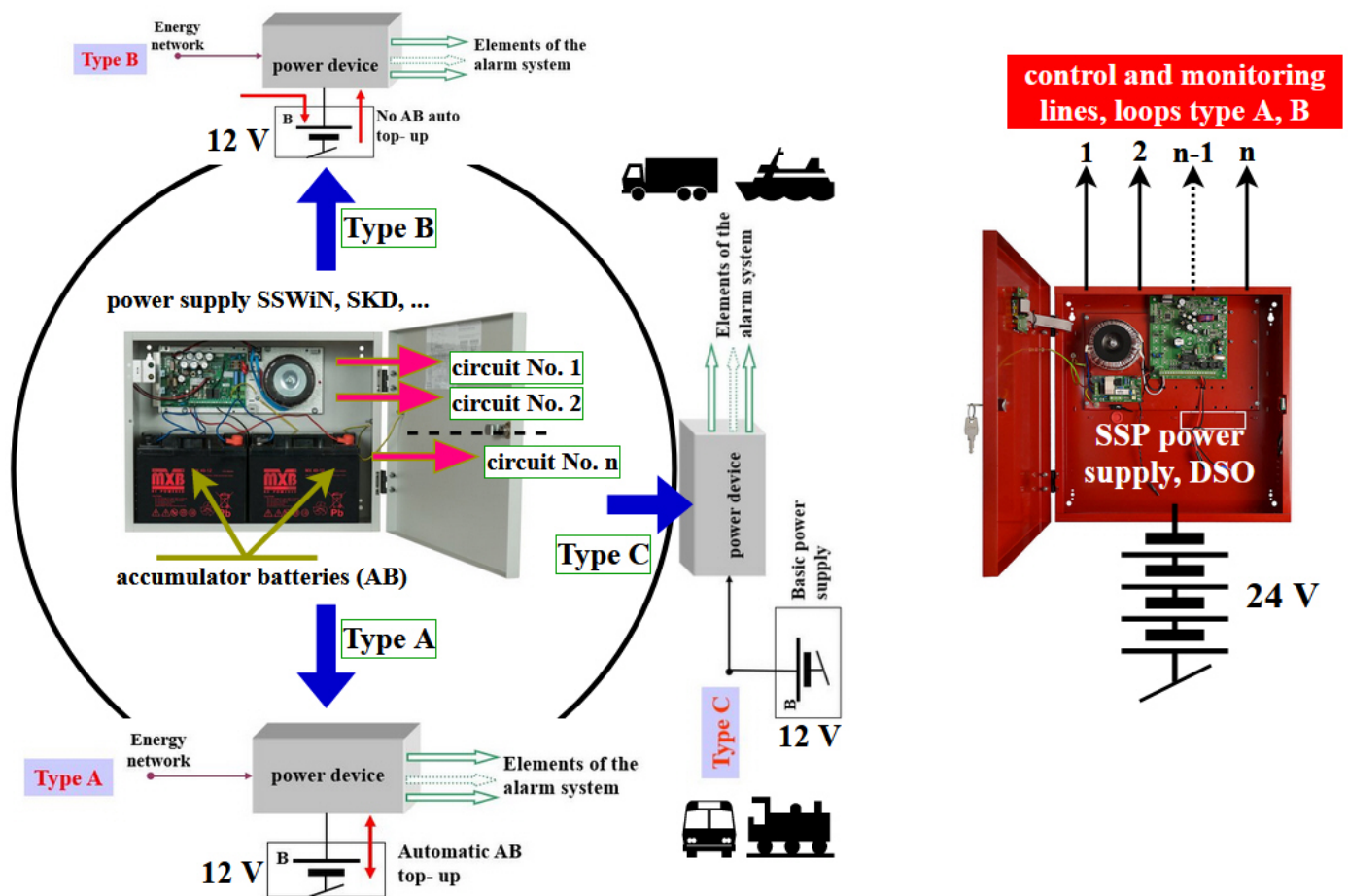


Figure 3. Power supply diagram for electronic security systems.

4. Basic Information on the Damage Intensities λ of Elements, Modules and Devices Used within Fire Alarm Systems

The act of operating FAS devices, modules and elements means undertaking the entire set of specified actions to be organized and conducted, periodically or on an ongoing basis, by persons or an organization responsible for maintaining the operational readiness of this security system. An operated FAS is impacted by a number of external and internal forces, both favorable and unfavorable to its operation. These forces include external and internal changes of environmental parameters (temperature, humidity, pressure, wind, rain, solar and electromagnetic radiation, etc.), as well as changes in the amplitude levels of interference penetrating into individual FAS elements, such as mechanical (e.g., vibrations, shocks, oscillations etc.) and electromagnetic (external and internal sources with a wide frequency spectrum, containing signals in the conducted and radiated interference band). The changes in the electroclimate within the building and individual rooms also influence the functioning of these systems [70,71]. Such interference may be generated intentionally (on purpose—sabotage) or unintentionally—radio, TV, mobile telephony stations, etc. All conducted maintenance, preventive or recovery activities within the operation process are always aimed at maintaining the constant readiness of a FAS for operation or restoring functionality, i.e., ensuring fire protection. The service activities conducted in the course of operation are usually of technical or organizational nature.

Figure 4 shows selected factors that passively or actively impact the FAS operation process (including reliability) [72,73]. Factors that can impact the entire FAS operation process include four fundamental, essential and basic activities associated with:

- FAS operation in accordance with the intended purpose of a given civil structure,
- preventive maintenance in accordance with the FAS operation schedule,

- transporting, e.g., spare parts for the recovery process or supplementing the on-site resources—local warehouse, at the permanent FAS dislocation,
- implementing a proper storage process involving spare parts and devices for current repairs or replacing worn elements—Figure 4.

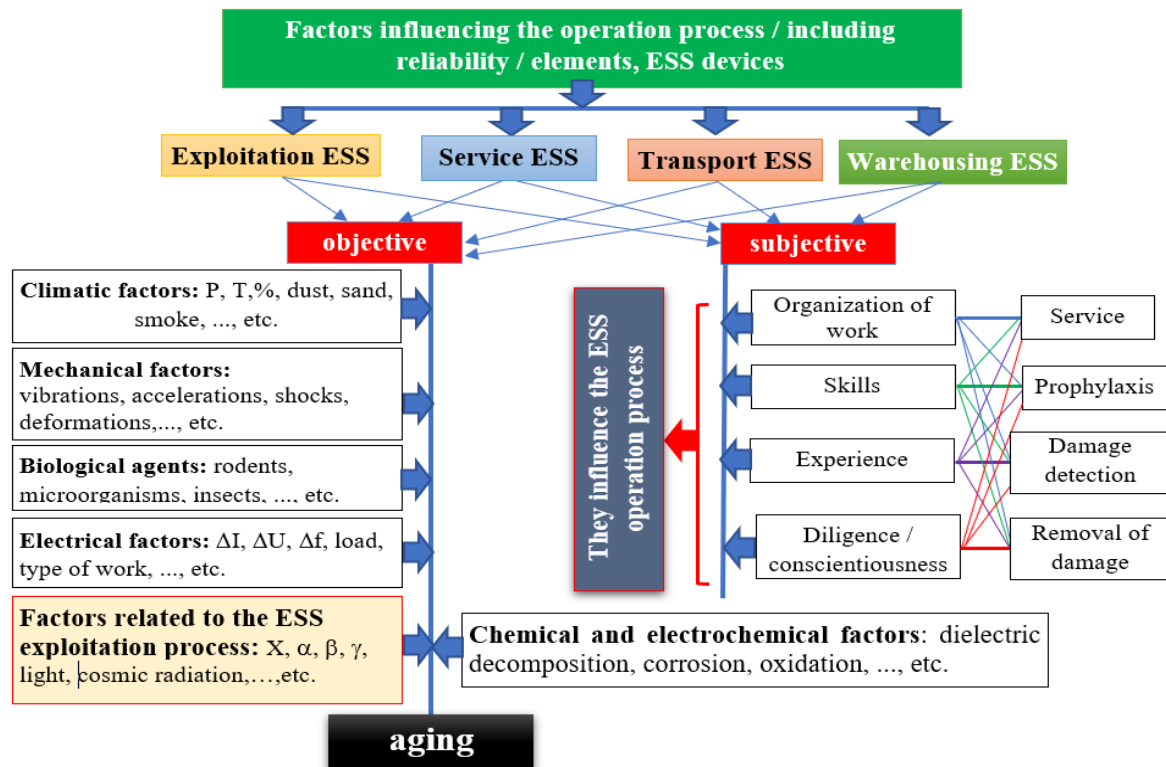


Figure 4. Impact of selected passive and active factors on the FAS operation process [72,73].

All FAS elements and devices operated within a given civil structure are always located within two different environments—external and internal. Figure 5 shows a simplified impact of this adverse environment on the operation process of individual FAS elements, devices or modules, through changing the damage intensity parameter λ for the aforementioned technical components [74].

All of these FAS devices are exposed to constant, favorable or unfavorable, technical parameter changes in individual elements—e.g., change in the resistance of the parametric line R_p or in detection lines (passive elements), change in the current amplification factor β of the transistors, change in the matrix parameters h_{11} , h_{12} , h_{21} or h_{22} (active elements) or change in radiation intensity of signaling elements such as the acoustic and optical signaling devices (AOSD). The changes also involve internal and external connection resistance—Figure 5 [75].

However, environmental changes have the largest impact upon external FAS elements and devices—e.g., alarm and damage signal transmission devices, acoustic and optical signaling devices or external fire detectors located outside of the building, e.g., in the warehouse—Figure 5. In addition, other ESSs with external elements, e.g., on building walls, are particularly exposed to the impact of adverse environmental conditions, including cameras, card readers within an access control system, tripods and entry/exit gates of the protected area [76–78].

Figure 6 shows a sample waveform of p parameter changes during the operation of FAS elements, devices and modules. The following are possible due to the source of these changes:

- a continuous change in selected or all parameters of a given device,

- a step-wise change impacted by external and internal factors, resulting from the factors presented in Figure 4 [73,74].

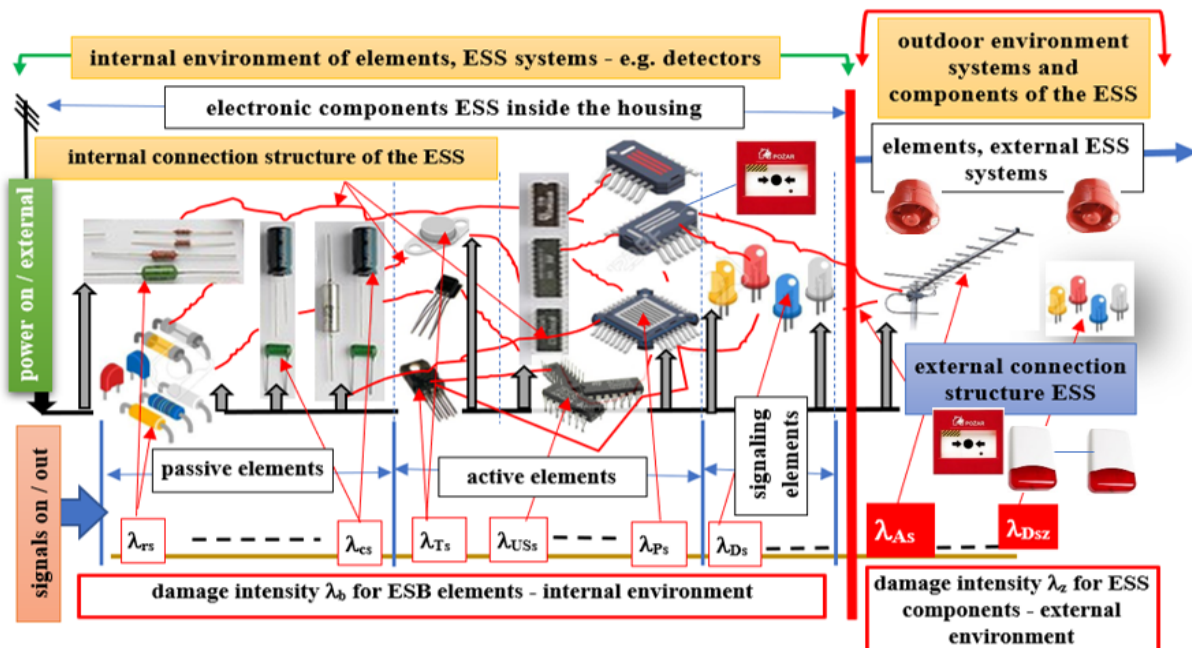


Figure 5. Adverse impact of an external and internal environment on the operation process of individual FAS elements, devices or modules.

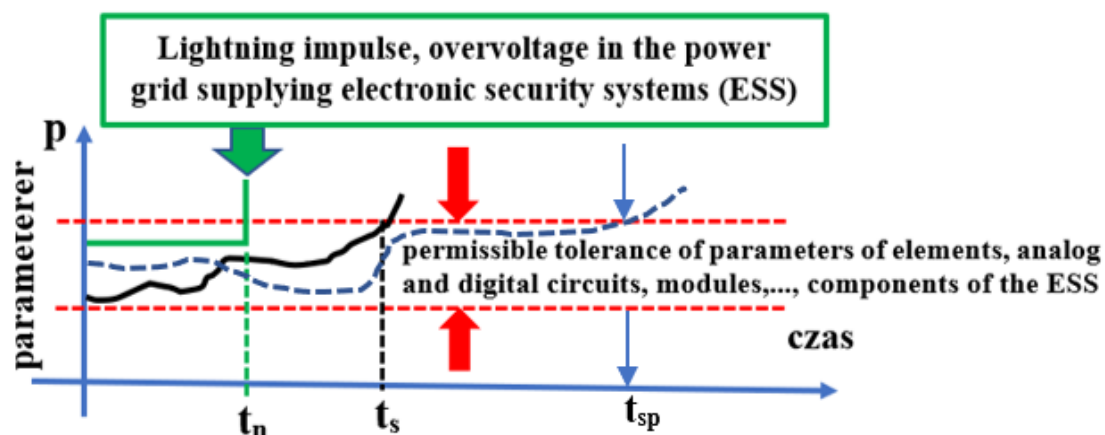


Figure 6. Continuous or step-wise change in the p parameters of FAS elements, systems, modules or devices, impacted by environmental changes, where: t_s —damage time in the case of so-called ageing changes related to operation time, t_n —time to damage upon pulsed actions causing unfitness—e.g., supply grid overvoltage, occurrence of an atmospheric discharge pulse, t_{sp} —time to damage in the event of so-called ‘ageing changes’ related to operation time under favorable external environmental conditions.

The impact of a changing environment on FAS elements and devices leads to changes in the p technical parameters used within the security system of technical facilities. Figure 7 shows a change in the damage intensity coefficient k_λ for elements, devices or individual electronic circuits of FAS operated under various environmental conditions. Therein, the range of changes ΔK in the k_λ coefficient, and the application range for FAS elements that are used in practice within such a security system is illustrated [79–81].

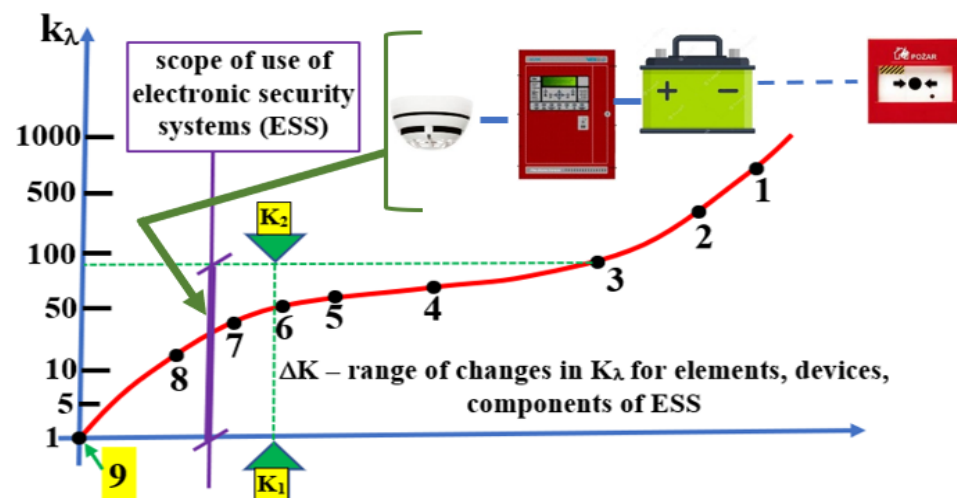


Figure 7. Change of the k_λ damage intensity coefficient for FAS elements, modules and components operated under the following environmental conditions, where: 1—modern rocket types, 2—older rocket types, 3—aircraft, 4—electronic instrumentation, so-called ‘high-mountain’, 5—railway devices (e.g., locomotive, train, carriage, etc.), 6—cars, 7—ships, vessels, 8—ground electronic devices, other security systems operated in civil structures, 9—laboratory conditions, facilities, rooms with environmental parameters stabilized within a specific range.

The impact of operation process conditions, i.e., use, maintenance and the power or information supply of the FAS on damage intensity λ of electronic elements of FAS modules or components in the case of external and internal adverse factors can be determined using the damage intensity coefficient k_λ [82,83].

The value of this coefficient indicates how many times the actual damage intensity λ_{rz} for a given FAS element is correspondingly higher or lower under given conditions than the damage intensity λ under laboratory conditions. This can be expressed using Equation (1).

The 3–9 range is practically used for calculating changes in the damage intensity λ for the entire FAS. Original study, based on [11,12,72,73].

$$k_\lambda = \frac{\lambda_{rz}}{\lambda}, \quad (1)$$

where: k_λ —damage intensity coefficient for FAS component elements, λ_{rz} —actual damage intensity for FAS elements, λ —damage intensity for FAS elements studied under given laboratory conditions [72,84].

After reading the damage intensity coefficient k_λ using the characteristics set out in Figure 6, the actual damage intensity for electronic FAS coefficients can be calculated by applying expression (2).

$$\lambda_{rz} = k_\lambda \cdot \lambda, \quad (2)$$

where: designations in expression (2) are physically interpreted as in relationship (1).

The basic FAS ‘lifetime’ characteristics (lifetime is the time period from commissioning to decommissioning) is always a continuous random variable. This can be, e.g., reliability. Reliability $R(t)$ is the probability that, at a given time, the FAS will be fit to implement all functions assumed within the control matrix, in accordance with a previously adopted fire scenario for a specific civil structure and within a specific time. FAS reliability is also a degree of confidence that a security system conducts all the assumed functions associated with a fire event within a civil structure, i.e., detection, notification, commencing suppression using fixed fire extinguishers (FFE) or a gas suppression system (GSS). A specific value of this probability is always the formal expression of such confidence [73,84]. Therefore, the reliability function also determines the probability for failure-free FAS operation—from

the moment it is installed within a structure, most usually as new, to a certain moment in time, when such a technical object responsible for fire safety is decommissioned. FAS lifetime is a continuous random variable τ that takes values from the $(0, \infty)$ range. At the same time, the implementation of this random variable is always a measure of FAS service within a given civil structure—in this case, the implementation guarantees safety. Various values can be adopted as a service unit of measure in FAS—they are or can be a function of the facility under protection. The aforementioned is an implementation of a service by the system—e.g., detecting a fire, detection time, PSP notification time and time of triggering an audio warning system (AWS), FFE or GSS activation and the fire scenario implementation time, etc. The random variable τ —FAS lifetime is continuously characterized over time by specific functions, e.g., the distribution function $F(t)$, probability distribution density $f(t)$, reliability function $R(t)$ and damage intensity function $\lambda(t)$ [72–74]. All of the above parameters are determined for the time of $t \geq 0$, while the $R(t)$ function is always adjudged for time—interval $(0, t)$. This means the probability that a damage occurs later than at time t , i.e., FAS is fit at time $(0, t)$. $R(t)$ is always a non-increasing function relative to time t and it can be described by Equation (3).

$$R(t) = P(\tau > t) \text{ for } t \geq 0, \quad (3)$$

Accordingly, $R(t) = 0$ means that the probability of FAS unfitness at switching on, activation and commissioning is equal to 0. The $f(t)$ probability distribution density function for variable τ is always a distribution function derivative. This is determined using expression (4), while the damage intensity function $\lambda(t)$ is defined through Equation (5).

$$f(t) = \frac{dF(t)}{dt} \text{ for } t \geq 0, \quad (4)$$

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \text{ for } t \geq 0, \quad (5)$$

where: $F(t)$ —denotes a reliability function—which is the probability of a FAS unfitness prior to the t moment.

FAS damage intensity is also a local characteristic of the durability of a given security system element, if we take into account time. Hence, the statistical interpretation of FAS damage intensities λ at a given time t can be expressed through the ration of the number of objects in a large and technically homogeneous population (e.g., set of detectors, modules, control devices, etc.) that are damaged within the next unit of time, to the total number of objects that had survived until a given time t of FAS operation without a failure [1,74,85]. Due to the simple interpretation of function $\lambda(t)$, this characteristic feature can be deemed fundamental for the FAS service life [1,15,86]. Therefore, the function $\lambda(t)$, which increases over time, corresponds to the wear and tear of FAS—its individual elements, modules and systems—detectors, modules, control devices, sprinklers, etc. The decreasing function $\lambda(t)$ is usually the initial phase of FAS service life. The extreme of the $\lambda(t)$ function is the FAS ‘critical service point’. This means it is a good time to decommission the entire system. The $\lambda(t)$ for the FAS can also be constantly decreasing or increasing throughout the entire FAS ‘lifetime’. For many types of technical objects, the $\lambda(t)$ function can also be monotonic, but also with intervals [73,74]. Taking into account the relationship $R(t) = 1 - F(t)$, the damage intensity function $\lambda(t)$ can be described via expression (6).

$$\lambda(t) = \frac{\sigma F(t)}{\sigma t} \cdot \frac{1}{R(t)}, \quad (6)$$

FAS elements, devices and modules are characterized by high reliability owing to redundancy, backups and fail-safe solutions applied in the designs. Hence, $R(t) \rightarrow 1$, and expression (6) can be written using Equation (7).

$$\lambda(t) = \frac{\sigma F(t)}{\sigma t} = \frac{\sigma F(t)}{\sigma X} \cdot \frac{\sigma X}{\sigma t}, \quad (7)$$

where: X —resistance reserve of a given FAS element, module, detector, resistance to a given external or internal mechanical X_m , electrical X_E or thermal X_c factor.

FAS contains numerous passive and active elements of modules, detectors and devices with different degrees of the exhibited X_m , X_E , X_c resistance reserves that are always changing under the impact of various forcing factors of the external and internal environment—favorable or unfavorable to a given operation process. Therefore, the number of used aforementioned objects can be determined as: $X = \sum_{i=1}^k X_i$.

Subsequently, the equation taking into account the aforementioned resistances can be included in the general notation of Equation (7), and its function $\lambda(t)$ can be determined using Equation (8).

$$\lambda(t) = \frac{\sigma F(t)}{\sigma X_m} \cdot \sum_1^{k_m} \frac{\sigma X_m}{\sigma t} + \frac{\sigma F(t)}{\sigma X_e} \cdot \sum_1^{k_e} \frac{\sigma X_e}{\sigma t} + \frac{\sigma F(t)}{\sigma X_c} \cdot \sum_1^{k_c} \frac{\sigma X_c}{\sigma t}, \quad (8)$$

The relationship (8) has two functions, which determine the following for FAS elements and modules:

- $\frac{\sigma F(t)}{\sigma X}$ —change rate of FAS unreliability—its elements, detectors, sensors, modules, etc. resulting from resistance changes impacted by environmental changes,
- $\frac{\sigma X}{\sigma t}$ resistance change rate for FAS elements, detectors, modules, etc. impacted by degradation processes ongoing therein. This is associated with changes in the environment, interference and, e.g., supply voltage fluctuations (decays, overvoltages, etc.).

Determination of the damage intensity $\lambda(t)$ for a FAS or other electronic security systems requires testing and analyzing the statistics of their damage and recovery process, which is implemented on an ongoing basis within the actual operation processes of the aforementioned technical objects [1,18,87]. In this work, 10 systems with varying technical structures—from focus to distributed—were used to calculate these two indicators of the FAS operation process. FAS structures use elements, devices and modules installed within detection lines or circuits controlling monitored civil structures. FAS elements, modules and devices are located in civil structures and outside of such buildings. In such cases, they are directly exposed to the variable climate of the Earth. In this work, FAS operation process analysis was based on electronic data saved in FACU event logs for all three fundamental technical states of the system, namely, states of fitness, unfitness and partial unfitness or damage to detection line No. x with correct functioning of other lines. Operation process data is saved in the non-volatile memory of the fire alarm control unit. The mentioned systems were operated under similar internal and external environmental conditions.

More than 100,000 operational events in FAS were distinguished for the purposes of testing and calculating selected operational indicators. FAS unfitness states can be divided into two types. The first type is caused by errors of operators supervising the FAS operation system. The second depends on environmental parameters, as well as the external and internal factors independent of the system operator—e.g., interference, decay, dip or surges within power supply lines [88,89].

A significant issue related to FAS operation, discussed in this article, is the varying service life of individual elements installed within detection and control lines or circuits hooked up to the FACU. If we consider a longer FAS operation period, e.g., 10 years, then, in the event of identifying unfitness, the replacement of detectors, modules, signaling devices or other elements with new ones, having a ‘zero’ service life is not always conducted by the monitoring or service personnel. Fit FAS elements, which are most often damaged within the operation process are stored in the so-called ‘on-site’ warehouse or directly procured

from a given manufacturer. They are stored in various environmental conditions. Operational tests also involved interviews with persons directly responsible for the implemented FAS recovery process. In terms of FAS faults, a very important factor that limits the very recovery process is time. In this case, detection circuits or lines are fitted with elements of various ‘lifetimes’—some are new, delivered directly from a warehouse or purchased from a manufacturer, however, time constraints also force the use of technically sound detectors with a different time elapsed from manufacturing. This is why the operation process related to these elements does not include an exponential distribution, which in most cases, is ensured within the manufacturing process in a plant. In contrast, it involves conducting a so-called ‘preliminary ageing’ after manufacturing a finished product, already at the manufacturing plant [1,73,83]. The preliminary ageing time is always specified by the manufacturer of a given FAS element and it is not made available to the public.

Conducting such a process makes FAS elements exhibit a constant damage intensity λ for a specific period of operation. However, the process requires conducting a computer analysis of actual FASs with elements of different damage intensity λ waveform within the operation process and determining reliability and safety parameters. Figure 2 shows a sample FAS with a focused structure, which includes selected detection lines and circuits with elements of various damage intensities λ , marked in this Figure with a sample waveform.

5. Reliability and Operational Analysis of a Fire Alarm System for Detection Circuit and Line Equipment with Varying Damage Intensities

In the course of analyzing the functioning of a fire alarm system, the relationships occurring in such a FAS can be illustrated in terms of reliability and operation, as demonstrated in Figure 8. A FAS in which all detection circuits, lines, control devices, acoustic and optical signaling devices, etc. connected to it are fit is considered to be in a state of full fitness— S_{PZ} . In this case, the FAS will execute all controls in the event of a threat that are programmed in the FACU control matrix for a given fire scenario. In the event of an unfitness exhibited by single elements or devices hooked up to FAS detection lines or circuits, the system switches into a state of safety hazard S_{ZB} . In such a scenario, some FAS functions programmed in a FACU control matrix will not be executed, and the damage signal is immediately sent via two transmission tracks to, e.g., an alarm receiving center (ARC) and PSP. There is a strictly defined time period to attempt repair (recovery) of a FAS operated in critical infrastructure buildings (CIBs).

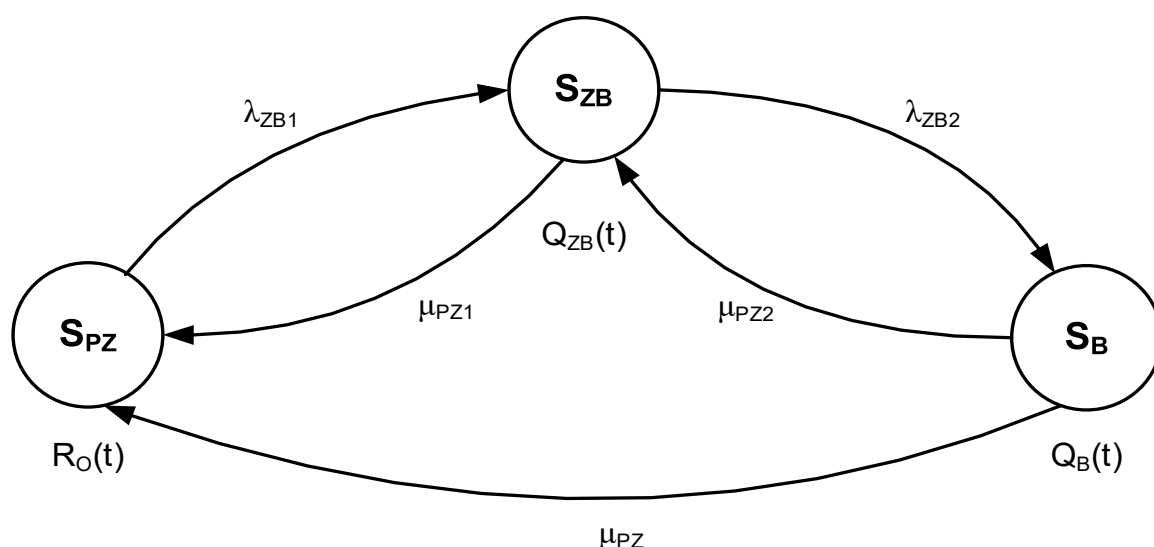


Figure 8. Safety relationships ongoing within a fire alarm system.

Failure to attempt repairing the FAS may lead to further damage, in which case the system will switch from a state of safety hazard S_{ZB} , to a state of safety unreliability S_B . A

FAS for a CIB is designed in a way so that there is no so-called ‘secondary damage’, the source of which is primary unfitness within a detection circuit or line. This is achieved through the system being fitted with, e.g., short-circuit isolators (SCI) within the lines and circuits, as well as redundancy or the fail-safe principle, e.g., in FACU, through a 100% duplication of its most important elements. In a FAS, the probability of total unfitness, which is the transition between the S_{PZ} and S_B states, is practically close to zero. The use of appropriate technical and organizational solutions—e.g., SCI, backup power supply (battery bank), overvoltage protection in supply lines and detection loops, fuses, varistors or other elements and anti-destruction devices (filters, shielding, etc.) makes such a transition almost impossible. A defined duration of a repair conducted in the event of an unfitness by the FAS service or on-site maintenance personnel, an ‘on-site’ spare parts warehouse, and acknowledgement of information on the unfitness are only examples of organizational solutions that increase the probability of the system staying in a state of full fitness S_{PZ} .

Designations in Figure 8:

- $R_0(t)$ —probability function of the fire alarm system staying in a state of full fitness S_{PZ} ,
- $Q_{ZB}(t)$ —probability function of the fire alarm system staying in a state of safety hazard S_{ZB} ,
- $Q_B(t)$ —probability function of the fire alarm system staying in a state of safety unreliability S_B ,
- λ_{ZB1} —intensity of transitions from a state of full fitness S_{PZ} , to a state of safety hazard S_{ZB} ,
- μ_{PZ1} —intensity of transitions from a state of safety hazard S_{ZB} , to a state of full fitness S_{PZ} ,
- λ_{ZB2} —intensity of transitions from a state of safety hazard S_{ZB} , to a state of safety unreliability S_B ,
- μ_{PZ2} —intensity of transitions from a state of safety unreliability S_B , to a state of safety hazard S_{ZB} ,
- μ_{PZ} —intensity of transitions from a state of safety unreliability S_B , to a state of full fitness S_{PZ} .

Full fitness S_{PZ} is a state in which a fire alarm system is functioning correctly and executes all its functions. Safety hazard S_{ZB} is a state in which a fire alarm system is partially fit and executes only certain functions. Safety unreliability S_B is a state in which a fire alarm system is unfit.

If a fire alarm system is in a state of full fitness S_{PZ} and there occurs a non-catastrophic damage, then the FAS switches to a safety hazard state S_{ZB1} with the intensity λ_{ZB1} . If a fire alarm system is in a state of safety hazard S_Z , then in the case of taking action aimed at restoring FAS fitness, the system switches to a state of full fitness S_{PZ} .

When a fire alarm system is in a state of safety hazard S_{ZB} , and there occurs a catastrophic damage, it switches to a state of safety unreliability S_B with the intensity λ_{ZB2} . A transition back to the state of safety hazard S_{ZB} from the state of safety unreliability S_B occurs upon successful repair activity.

A transition from the state of safety unreliability S_B to the state of full fitness S_{PZ} is possible, however, it requires taking corrective actions covering the entire fire alarm system. The system shown in Figure 8 was described by the following Chapman–Kolmogorov equations (expression (9)).

$$\begin{aligned} R'_0(t) &= -\lambda_{ZB1} \cdot R_0(t) + \mu_{PZ1} \cdot Q_{ZB}(t) + \mu_{PZ} \cdot Q_B(t) \\ Q'_{ZB}(t) &= \lambda_{ZB1} \cdot R_0(t) - \mu_{PZ1} \cdot Q_{ZB}(t) - \lambda_{ZB2} \cdot Q_{ZB}(t) + \mu_{PZ2} \cdot Q_B(t) \\ Q'_B(t) &= \lambda_{ZB2} \cdot Q_{ZB}(t) - \mu_{PZ2} \cdot Q_B(t) - \mu_{PZ} \cdot Q_B(t), \end{aligned} \quad (9)$$

If we adopt the following initial conditions described by the expression (10).

$$\begin{aligned} R_0(0) &= 1 \\ Q_{ZB}(0) &= Q_B(0) = 0, \end{aligned} \quad (10)$$

and then apply the Laplace transform, we obtain a set of linear Equation (11).

$$\begin{aligned} s \cdot R_0^*(s) - 1 &= -\lambda_{ZB1} \cdot R_0^*(s) + \mu_{PZ1} \cdot Q_{ZB}^*(s) + \mu_{PZ} \cdot Q_B^*(s) \\ s \cdot Q_{ZB}^*(s) &= \lambda_{ZB1} \cdot R_0^*(s) - \mu_{PZ1} \cdot Q_{ZB}^*(s) - \lambda_{ZB2} \cdot Q_{ZB}^*(s) + \mu_{PZ2} \cdot Q_B^*(s) \\ s \cdot Q_B^*(s) &= \lambda_{ZB2} \cdot Q_{ZB}^*(s) - \mu_{PZ2} \cdot Q_B^*(s) - \mu_{PZ} \cdot Q_B^*(s), \end{aligned} \quad (11)$$

Symbolic (Laplace) probabilities of a fire alarm system staying in distinguished states takes the following form described by the Equation (12).

$$\begin{aligned} R_0^*(s) &= \frac{s^2 + s \cdot \mu_{PZ} + s \cdot \mu_{PZ1} + s \cdot \lambda_{ZB2} + s \cdot \mu_{PZ2} + \mu_{PZ} \cdot \mu_{PZ1} + \mu_{PZ} \cdot \lambda_{ZB2} + \mu_{PZ1} \cdot \mu_{PZ2}}{s^2 \cdot \mu_{PZ} + s^2 \cdot \lambda_{ZB1} + s^2 \cdot \mu_{PZ1} + s^2 \cdot \lambda_{ZB2} + s^2 \cdot \mu_{PZ2} + s^3 + s \cdot \mu_{PZ} \cdot \lambda_{ZB1} + s \cdot \mu_{PZ} \cdot \mu_{PZ1} + s \cdot \mu_{PZ} \cdot \lambda_{ZB2} + s \cdot \lambda_{ZB1} \cdot \lambda_{ZB2} + s \cdot \lambda_{ZB1} \cdot \mu_{PZ2} + s \cdot \mu_{PZ1} \cdot \mu_{PZ2}} \\ Q_{ZB1}^*(s) &= \frac{s \cdot \lambda_{ZB1} + \mu_{PZ} \cdot \lambda_{ZB1} + \lambda_{ZB1} \cdot \mu_{PZ2}}{s^2 \cdot \mu_{PZ} + s^2 \cdot \lambda_{ZB1} + s^2 \cdot \mu_{PZ1} + s^2 \cdot \lambda_{ZB2} + s^2 \cdot \mu_{PZ2} + s^3 + s \cdot \mu_{PZ} \cdot \lambda_{ZB1} + s \cdot \mu_{PZ} \cdot \mu_{PZ1} + s \cdot \mu_{PZ} \cdot \lambda_{ZB2} + s \cdot \lambda_{ZB1} \cdot \lambda_{ZB2} + s \cdot \lambda_{ZB1} \cdot \mu_{PZ2} + s \cdot \mu_{PZ1} \cdot \mu_{PZ2}} \\ Q_B^*(s) &= \frac{\lambda_{ZB1} \cdot \lambda_{ZB2}}{s^2 \cdot \mu_{PZ} + s^2 \cdot \lambda_{ZB1} + s^2 \cdot \mu_{PZ1} + s^2 \cdot \lambda_{ZB2} + s^2 \cdot \mu_{PZ2} + s^3 + s \cdot \mu_{PZ} \cdot \lambda_{ZB1} + s \cdot \mu_{PZ} \cdot \mu_{PZ1} + s \cdot \mu_{PZ} \cdot \lambda_{ZB2} + s \cdot \lambda_{ZB1} \cdot \lambda_{ZB2} + s \cdot \lambda_{ZB1} \cdot \mu_{PZ2} + s \cdot \mu_{PZ1} \cdot \mu_{PZ2}} \end{aligned} \quad (12)$$

The solution to a set of Equation (12) within the time domain can be the next analysis step, but will not be discussed in this article.

In the course of calculations using the relationships (12), the authors determined probabilities of a fire alarm system staying in the states of full fitness R_0 , safety hazard S_{ZB} and safety unreliability S_B .

Let us adopt the following values describing the analyzed fire alarm system:

- study duration—1 year:

$$t = 8760[h]$$

- FAS reliability (no critical damage):

$$R_{ZB1}(t) = 0.999$$

- FAS reliability (critical damage):

$$R_{ZB2}(t) = 0.9999$$

- intensity of transitions from a state of safety hazard to a state of full fitness:

$$\mu_{PZ1} = 0.1 \left[\frac{1}{h} \right]$$

- intensity of transitions from a state of safety unreliability to a state of safety hazard:

$$\mu_{PZ2} = 0.1 \left[\frac{1}{h} \right]$$

- intensity of transitions from a state of safety unreliability to a state of full fitness:

$$\mu_{PZ} = 0.05 \left[\frac{1}{h} \right]$$

If one knows the values of reliability $R_{ZB1}(t)$, it is possible to estimate intensities of FAS transitions from the state of full fitness to the state of safety hazard. Assuming the simplest, exponential fitness duration distribution model, it is possible to use the following relationship:

$$R_{ZB1}(t) = e^{-\lambda_{ZB1}t} \text{ for } t \geq 0$$

so

$$\lambda_{ZB1} = -\frac{\ln R_{ZB1}(t)}{t}$$

For $t = 8760[h]$ and $R_{ZB1}(t) = 0.999$ we obtain:

$$\lambda_{ZB1} = -\frac{\ln R_{ZB1}(t)}{t} = -\frac{\ln 0.999}{8760} = 1.142124 \times 10^{-7} \left[\frac{1}{h} \right]$$

If one knows the values of reliability $R_{ZB2}(t)$, it is possible to estimate intensities of FAS transitions from the state of safety hazard to the state of safety unreliability. For an exponential distribution, we derive the following relationship:

$$R_{ZB2}(t) = e^{-\lambda_{ZB2}t} \text{ for } t \geq 0$$

so

$$\lambda_{ZB2} = -\frac{\ln R_{ZB2}(t)}{t}$$

For $t = 8760[h]$ and $R_{ZB2}(t) = 0.9999$ we get:

$$\lambda_{ZB2} = -\frac{\ln R_{ZB2}(t)}{t} = -\frac{\ln 0.9999}{8760} = 1.141609 \cdot 10^{-8} \left[\frac{1}{h} \right]$$

For the above input values using the Equation (4) and inverse Laplace transforms, we obtain:

$$\begin{aligned} R_0 &= 0.99999885 \\ Q_{ZB} &= 0.00000114 \\ Q_B &= 8.6923 \cdot 10^{-14} \end{aligned}$$

Assuming that FAS reliability (without critical damage) is $R_{ZB1}(t) = 0.9995$ and FAS reliability (critical damage) is $R_{ZB2}(t) = 0.99995$ we get:

$$\begin{aligned} R_0 &= 0.99999942 \\ Q_{ZB} &= 5.71 \cdot 10^{-7} \\ Q_B &= 2.17 \cdot 10^{-14} \end{aligned}$$

Assuming that FAS reliability (without critical damage) is $R_{ZB1}(t) = 0.9999$ and FAS reliability (critical damage) is $R_{ZB2}(t) = 0.99999$ we get:

$$\begin{aligned} R_0 &= 0.99999989 \\ Q_{ZB} &= 1.1 \cdot 10^{-7} \\ Q_B &= 8.69 \cdot 10^{-16} \end{aligned}$$

The practical application of the aforementioned calculations enables comparing various types of fire alarm systems and matching a specific FAS configuration for building protection. It is particularly important in the case of protecting critical infrastructure buildings.

If we assume that intensity λ_{ZB1} of the transition from a state of full fitness S_{PZ} to a state of safety hazard S_{ZB} takes values in the range of $\lambda_{ZB1} \in \langle 1.147 \cdot 10^{-6}; 1.142 \cdot 10^{-8} \rangle \left[\frac{1}{h} \right]$ (corresponding to reliability values of $R_{ZB1}(t) \in \langle 0.99; 0.9999 \rangle$), then the probability of the analyzed fire alarm system staying in a state of full fitness is as illustrated by the graph in Figure 9.

The practical application of the aforementioned calculations enables comparing various types of fire alarm systems and matching a specific FAS configuration for building protection. This is particularly important in the case of protecting critical infrastructure.

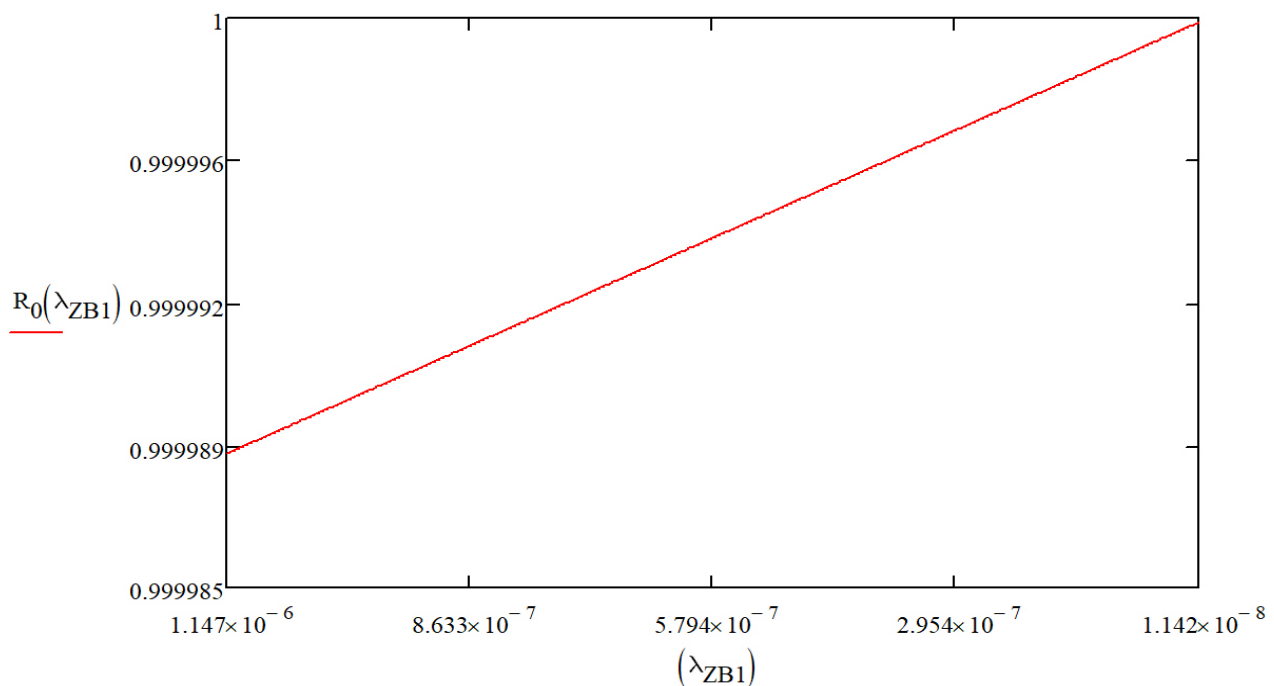


Figure 9. Relationship for the probability of a fire alarm system staying in a state of full fitness R_0 as a function of intensity λ_{ZB1} of the transition from a state of full fitness to a state of safety hazard.

6. Conclusions

The task of electronic security systems is to protect the property, health and life in stationary (e.g., CIB) and non-stationary (e.g., aircraft, cars, ships or railway vehicles—trains, carriages, etc.) structures. FAS are the most important security systems operated in the aforementioned technical and civil structures. Their use is governed by specific acts, standards and legal regulations applicable in individual states (locally), as well as e.g., by Regulation of the European Parliament and the Council of the European Union (EU) No. 305/2011 dated 9 March 2011 (CPR). Such legal solutions result in all elements, modules or devices employed within FAS being treated as all building products built within a given facility. The presented article discusses the most important aspects associated with operating selected FAS in their surrounding environment—favorable and unfavorable—for this process. The FAS operation process, as well as changes to its parameters and functionalities, have been taken into account in the actual values of damage intensity λ and recovery intensity μ that have been determined based on studying a representative group of systems. Based on the developed FAS reliability model, it was possible to determine the basic reliability and operational indicators—e.g., reliability or, e.g., the sole distinguishment of the basic safety state of the systems in question. They are extremely important for security reasons (fire hazards in this case) that occur within the facility and the surroundings. There are different technical and organizational solutions applied within a FAS. Their task is to increase the functional reliability of this system, $R_0(t)$, within a set operating period T_{op} . Within this set time $T_{op} = [0, t_{op1}]$; this means all FAS controls resulting from the control matrix based on the fire scenario for a given CIB. The article discusses the results of a study involving the operation of a selected FAS that is located within a critical infrastructure building. Elements, modules and devices within the FAS in question work under various environments conditions—that are favorable or adverse in terms of a given operation process of this system. Operational process safety indicators were determined assuming certain FAS reliability probability values (without critical damage or with unfitness that may occur within this system). The obtained reliability for a FAS with a distributed structure reaches very high values, in the order of $R_0 = 0.99999943$, which means that such a system is virtually reliable, reaching an approximated value of $R_0(t) \cong 1$. This is why the remaining

probability functions within the FAS in question reach very low values, e.g., the safety hazard function $Q_{ZB}(t) = 5.71 \times 10^{-7}$ and safety unreliability function $Q_B = 2.17 \times 10^{-14}$. This means that a FAS with the structure in question and security relations occurring within the system ‘spends’ most of the time in its basic state, i.e., the state of full fitness S_{PZ} . In such a case, all functionalities planned within the control matrix for a FAS structure in question are implemented. This also includes that which is not associated with direct fire detection within the facility (e.g., FACU diagnostic system, LCD info panel connected to an executive microprocessor that monitors the functioning of this technical structure, and a local printer for operation-related events). These aforementioned FAS elements do not directly take part in the implementation of the main FAS task, namely, detecting a fire and triggering the suppression process; however, they constitute necessary help for the users and service personnel during the diagnostics process—remote or on-site.

Author Contributions: Conceptualization, J.P., A.R. and M.S.; methodology, A.R., J.P. and M.W.; validation, J.P., A.R. and M.S.; formal analysis, J.P., A.R.; investigation, J.P., A.R. and M.S.; resources, J.P., A.R.; data curation, A.R., J.P., M.W. and M.S.; writing: original draft preparation, J.P., A.R. and M.S.; writing: review and editing, J.P., A.R., M.W. and M.S.; visualization, J.P. and A.R.; supervision, J.P. and A.R.; project administration, J.P. and A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This work was co-financed by Military University of Technology under research project UGB 737. This paper was co-financed under the research grant of the Warsaw University of Technology supporting the scientific activity in the discipline of Civil Engineering and Transport.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

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

Abbreviations

Abbr.	Full Name for Abbreviation
FAS	Fire Alarm Systems
λ	Damage intensities
μ	Repair intensities
$Q_{ZB}(t)$	Safety hazard states
$R_0(t)$	Full fitness state
$Q_B(t)$	Safety unreliability state
ADSTD	Alarm and Damage Signal Transmission Device
ARC	Alarm Receiving Centre
GSS	Gas Suppression System
CCTV	Closed-Circuit TV
CIB	Critical Infrastructure Buildings
AWS	Audio Warning Systems
ARC	Alarm Receiving Centre
k_λ	Damage intensity coefficient
$R(t)$	Reliability function
$f(t)$	Variable probability distribution density function τ
X	Durability resource of a given FAS sensor, module, element
S_{PZ}	Probability of a FAS staying in a state of full fitness
S_B	Safety unreliability state
S_{PZ}	Full fitness state
$\sigma X/\sigma t$	Element strength change rate
$\sigma F(t)/\sigma X$	FAS unreliability change rate

References

1. Klimczak, T.; Paś, J. *Basics of Exploitation of Fire Alarm Systems in Transport Facilities*; Military University of Technology: Warsaw, Poland, 2020.
2. Ding, L.; Ji, J.; Khan, F.; Li, X.; Wan, S. Quantitative fire risk assessment of cotton storage and a criticality analysis of risk 616 control strategies. *Fire Mater.* **2020**, *44*, 165–179. [CrossRef]
3. Mahdipour, E.; Dadkhah, C. Automatic fire detection based on soft computing techniques: Review from 2000 to 2010. *Artif. Intell. Rev.* **2014**, *42*, 895–934. [CrossRef]
4. Joglar, F. Reliability, Availability, and Maintainability. In *SFPE Handbook of Fire Protection Engineering*; Hurley, M., Ed.; Springer: New York, NY, USA, 2016; pp. 2875–2940. [CrossRef]
5. Hulida, E.; Pasnak, I.; Koval, O.; Tryhuba, A. Determination of the critical time of fire in the building and ensure successful 668 evacuation of people. *Period. Polytech. Civ. Eng.* **2019**, *63*, 308–316.
6. Jakubowski, K.; Paś, J.; Duer, S.; Bugaj, J. Operational Analysis of Fire Alarm Systems with a Focused, Dispersed and Mixed Structure in Critical Infrastructure Buildings. *Energies* **2021**, *14*, 7893. [CrossRef]
7. Regulation of Ministry of the Interior and Administration of Poland (MSWiA) of 7 June 2010 (Journal of Laws of the Republic of Poland No. 109, Item 719) Concerning Fire Protection of Buildings and Other Facilities and Grounds; Ministry of the Interior and Administration of Poland: Warsaw, Poland, 2021. Available online: <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/ochrona-przeciwpozarowa-budynkow-innych-objektow-budowlanych-i-terenow-17626053> (accessed on 17 November 2021).
8. Idris, A.M.; Rusli, R.; Burok, N.A.; Mohd Nabil, N.H.; Ab Hadi, N.S.; Abdul Karim, A.H.M.; Ramli, A.F.; Mydin, I. Human factors influencing the reliability of fire and gas detection system. *Process Saf. Prog.* **2020**, *39*, e12116. [CrossRef]
9. Jakubowski, K.; Paś, J.; Rosiński, A. The Issue of Operating Security Systems in Terms of the Impact of Electromagnetic Interference Generated Unintentionally. *Energies* **2021**, *14*, 8591. [CrossRef]
10. Rosiński, A. *Modelling the Maintenance Process of Transport Telematics Systems*; Publishing House Warsaw University of Technology: Warsaw, Poland, 2015.
11. Gertsbakh, I. *Reliability Theory with Applications to Preventive Maintenance*; Springer: Berlin/Heidelberg, Germany, 2020.
12. Selech, J.; Andrzejczak, K. An aggregate criterion for selecting a distribution for times to failure of components of rail vehicles. *Eksploat. I Niezawodn. Maint. Reliab.* **2020**, *22*, 102–111. [CrossRef]
13. Kołowrocki, K.; Soszyńska-Budny, J.; Torbicki, M. Critical Infrastructure Impacted by Operation and Climate Change Safety and Resilience Indicators. In Proceedings of the 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 16–19 December 2018; pp. 991–995. [CrossRef]
14. Wang, C. *Structural Reliability and Time-Dependent Reliability*; Springer: Berlin/Heidelberg, Germany, 2021.
15. Da Penha, O.S.; Nakamura, E.F. Fusing light and temperature data for fire detection. In Proceedings of the IEEE Symposium on Computers and Communications (ISCC), Riccione, Italy, 22–25 June 2010; pp. 107–112.
16. Xu, S.; Li, X. Analysis on thermal reliability of key electronic components on PCB board. In Proceedings of the 2011 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering, Xi'an, China, 17–19 June 2011; Huang, H.-Z., Zuo, M.J., Jia, X., Liu, Y., Eds.; IEEE: Xi'an, China, 2011; pp. 52–54.
17. Qiang, G.; Ya, Z.; Jinhua, Z. Dynamic Reliability Testing about Temperature Characteristic of Components. In Proceedings of the 2009 International Conference on Wireless Networks and Information Systems, Shanghai, China, 28–29 December 2009; Luo, Q., Tan, H., Eds.; IEEE: Los Alamitos, CA, USA, 2009; pp. 257–258.
18. Łukasiak, J.; Rosiński, A.; Wiśnios, M. The Impact of Temperature of the Tripping Thresholds of Intrusion Detection System Detection Circuits. *Energies* **2021**, *14*, 6851. [CrossRef]
19. Østrem, L.; Sommer, M. Inherent fire safety engineering in complex road tunnels—Learning between industries in safety management. *Saf. Sci.* **2021**, *134*, 105062. [CrossRef]
20. Lee, C.; Jo, S.; Kwon, D.; Pecht, M.G. Capacity-Fading Behavior Analysis for Early Detection of Unhealthy Li-Ion Batteries. *IEEE Trans. Ind. Electron.* **2021**, *68*, 2659–2666. [CrossRef]
21. Kofanov, Y.N.; Sotnikova, S.Y.; Subbotin, S.A. Method of increasing the reliability of on-board electronic equipment with an analysis of reserves for the electrical, thermal and mechanical loads. In Proceedings of the 2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS), Nalchik, Russia, 4–11 October 2016; Shaposhnikov, S., Ed.; IEEE Russia North West Section: St. Petersburg, Russia, 2016; pp. 94–98.
22. Seehase, D.; Novikov, A.; Nowotnick, M. Resistance development on embedded heating layers during climatic test. In Proceedings of the 2017 21st European Microelectronics and Packaging Conference (EMPC) & Exhibition, Warsaw, Poland, 10–13 September 2017; Dziedzic, A., Jasiński, P., Eds.; IEEE: Neumarkt-St. Veit, Germany, 2017; pp. 1–5.
23. Wang, X.; Liu, X.; Ding, Y.; Hang, C.; Wu, G.; Liu, W.; Li, J. Study on the Low Temperature Reliability of Leaded Solder. In Proceedings of the 2020, 21st International Conference on Electronic Packaging Technology (ICEPT), Guangzhou, China, 12–15 August 2020; IEEE: Piscataway Township, NJ, USA, 2020; pp. 1–5.
24. Vasile, D.-C.; Svasta, P.; Pantazica, M. Preventing the Temperature Side Channel Attacks on Security Circuits. In Proceedings of the 2019 IEEE 25th International Symposium for Design and Technology in Electronic Packaging (SIITME), Cluj-Napoca, Romania, 23–26 October 2019; IEEE: Piscataway Township, NJ, USA, 2019; pp. 244–247.
25. Łukasiak, J.; Rosiński, A. Analysis of exploitation process in the aspect of readiness of electronic protection systems. *Diagnostyka* **2017**, *18*, 37–42.

26. Polak, R.; Laskowski, D.; Matyszek, R.; Łubkowski, P.; Konieczny, Ł.; Burdzik, R. Optimizing the Data Flow in a Network Communication between Railway Nodes. In *Research Methods and Solutions to Current Transport Problems, Proceedings of the International Scientific Conference Transport of the 21st Century, Advances in Intelligent Systems and Computing, Ryn, Poland, 9–12 June 2019*; Siergiejczyk, M., Krzykowska, K., Eds.; Springer: Cham, Switzerland, 2020; Volume 1032, pp. 351–362.
27. Pas, J.; Rosinski, A.; Chrzan, M.; Bialek, K. Reliability-operational analysis of the LED lighting module including electro-magnetic interference. *IEEE Trans. Electromagn. Compat.* **2020**, *62*, 2747–2758. [\[CrossRef\]](#)
28. Grabski, F. *Semi-Markov Processes: Applications in System Reliability and Maintenance*; Elsevier: Amsterdam, The Netherlands, 2015; p. 560.
29. Bogalecka, M.; Kołowrocki, K. Minimization of critical infrastructure accident losses of chemical releases impacted by climate-weather change. In Proceedings of the International Conference on Industrial Engineering and Engineering Management-IEEM, Bangkok, Thailand, 16–19 December 2018. [\[CrossRef\]](#)
30. Serio, M.A.; Bonamno, A.S.; Knight, K.S.; Newman, J.S. Fourier Transform Infrared Diagnostics for Improved Fire Detection Systems. In Proceedings of the NIST Annual Conference on Fire Research, Gaithersburg, MD, USA, 28–31 October 1996.
31. Morgan, A. Left Luggage, Automatic Fire Detection and the New Century. *Fire Eng. J.* **2000**, *60*, 37–39.
32. Menon, S.; Chen, D.Y.; Osterman, M.; Pecht, M. Copper trace fatigue life modeling for rigid electronic assemblies. *IEEE Trans. Device Mater. Reliab.* **2021**, *21*, 79–86. [\[CrossRef\]](#)
33. Epstein, B.; Weissman, I. *Mathematical Models for Systems Reliability*; CRC Press/Taylor & Francis Group: Boca Raton, FL, USA, 2008.
34. Zhao, H.; Schwabe, A.F.; Schläfli, F.; Thrash, T.; Aguilar, L.; Dubey, R.K.; Karjalainen, J.; Hölscher, C.C.; Helbing, D.; Schinazi, V.R. Fire evacuation supported by centralized and decentralized visual guidance systems. *Saf. Sci.* **2022**, *145*, 105451. [\[CrossRef\]](#)
35. Kubica, P.; Boroń, S.; Czarnecki, L.; Węgrzyński, W. Maximizing the retention time of inert gases used in fixed gaseous extinguishing systems. *Fire Saf. J.* **2016**, *80*, 1–8. [\[CrossRef\]](#)
36. Urbanik, M.; Tchórzewska-Cieślak, B.; Pietrucha-Urbanik, K. Analysis of the Safety of Functioning Gas Pipelines in Terms of the Occurrence of Failures. *Energies* **2019**, *12*, 3228. [\[CrossRef\]](#)
37. Zajkowski, K. The method of solution of equations with coefficients that contain measurement errors, using artificial neural network. *Neural Comput. Appl.* **2014**, *24*, 431–439. [\[CrossRef\]](#)
38. Duer, S.; Duer, R.; Mazuru, S. Determination of the expert knowledge base on the basis of a functional and diagnostic analysis of a technical object. *Nonconv. Technol. Rev.* **2016**, *20*, 23–29. Available online: <http://revtn.ro/index.php/revtn/article/view/115/76> (accessed on 10 January 2022).
39. Żyluk, A.; Kuźma, K.; Grzesik, N.; Zieja, M.; Tomaszewska, J. Fuzzy Logic in Aircraft Onboard Systems Reliability Evaluation—A New Approach. *Sensors* **2021**, *21*, 7913. [\[CrossRef\]](#)
40. Majewski, M.; Kacalak, W. Innovative Intelligent Interaction Systems of Loader Cranes and Their Human Operators. Advances in Intelligent Systems and Computing. In *Artificial Intelligence Trends in Intelligent Systems*; Springer: Cham, Switzerland, 2017; Volume 573, pp. 474–485. [\[CrossRef\]](#)
41. Duer, S.; Zajkowski, K.; Harničárová, M.; Charun, H.; Bernatowicz, D. Examination of Multivalent Diagnoses Developed by a Diagnostic Program with an Artificial Neural Network for Devices in the Electric Hybrid Power Supply System “House on Water”. *Energies* **2021**, *14*, 2153. [\[CrossRef\]](#)
42. Kierzkowski, A.; Kisiel, T. Simulation model of security control system functioning: A case study of the Wrocław Airport terminal. *J. Air Transp. Manag.* **2017**, *64*, 173–185. [\[CrossRef\]](#)
43. Burdzik, R.; Konieczny, Ł.; Figlus, T. Concept of on-board comfort vibration monitoring system for vehicles. In *Communications in Computer and Information Science, Activities of Transport Telematics, Proceedings of the 13th International Conference on Transport Systems Telematics, TST 2013, Katowice-Ustroń, Poland, 23–26 October 2013*; Mikulski, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2013; Volume 395, pp. 418–425.
44. Stawowy, M.; Rosiński, A.; Siergiejczyk, M.; Perlicki, K. Quality and Reliability-Exploitation Modeling of Power Supply Systems. *Energies* **2021**, *14*, 2727. [\[CrossRef\]](#)
45. Drzazga, M.; Kołowrocki, K.; Soszyńska-Budny, J. Methodology for oil pipeline critical infrastructures safety and resilience to climate change analysis. *J. Pol. Saf. Reliab. Assoc. Summer Safety Reliab. Semin.* **2016**, *7*, 173–178.
46. Dziula, P.; Paś, J. Low Frequency Electromagnetic Interferences Impact on Transport Security Systems Used in Wide Transport Areas. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2018**, *12*, 251–258. [\[CrossRef\]](#)
47. Siergiejczyk, M.; Paś, J.; Dudek, E. Reliability analysis of aerodrome’s electronic security systems taking into account electromagnetic interferences. In *Safety and Reliability-Theory and Applications, Proceedings of the 27th European Safety and Reliability Conference (Esrel 2017), Portorož, Slovenia, 18–22 June 2017*; Cepin, M., Briš, R., Eds.; CRC Press/Balkema: Schiphol, The Netherlands, 2017; pp. 2285–2292.
48. Zieja, M.; Szelmanowski, A.; Pazur, A.; Kowalczyk, G. Computer Life-Cycle Management System for Avionics Software as a Tool for Supporting the Sustainable Development of Air Transport. *Sustainability* **2021**, *13*, 1547. [\[CrossRef\]](#)
49. Shilo, G.; Ogrenich, E.; Kulyaba-Kharitonova, T.; Buhaiev, O. Thermal design of the Electronic Equipment Enclosures with Natural Air Cooling. In Proceedings of the 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 5–7 June 2019; pp. 153–156.
50. Boryczko, K.; Piegoń, I.; Szpak, D.; Żywiec, J. Risk Assessment of Lack of Water Supply Using the Hydraulic Model of the Water Supply. *Resources* **2021**, *10*, 43. [\[CrossRef\]](#)

51. Suproniuk, M.; Paś, J. Analysis of electrical energy consumption in a public utility buildings. *Prz. Elektrotechniczny* **2019**, *95*, 97–100. [\[CrossRef\]](#)
52. Duer, S. Assessment of the Operation Process of Wind Power Plant's Equipment with the Use of an Artificial Neural Network. *Energies* **2020**, *13*, 2437. [\[CrossRef\]](#)
53. Krzykowski, M.; Paś, J.; Rosiński, A. Assessment of the level of reliability of power supplies of the objects of critical infrastructure. *IOP Conf. Ser. Earth Environ. Sci.* **2019**, *214*, 012018. [\[CrossRef\]](#)
54. Kossakowski, D.; Krzykowska, K. Application of V2X Technology in Communication between Vehicles and Infrastructure in Chosen Area. In *Research Methods and Solutions to Current Transport Problems, Proceedings of the International Scientific Conference Transport of the 21st Century, Advances in Intelligent Systems and Computing, Ryn, Poland, 9–12 June 2019*; Siergiejczyk, M., Krzykowska, K., Eds.; Springer: Cham, Switzerland, 2020; Volume 1032, pp. 247–256.
55. Stypułkowski, K.; Gołda, P.; Lewczuk, K.; Tomaszewska, J. Monitoring System for Railway Infrastructure Elements Based on Thermal Imaging Analysis. *Sensors* **2021**, *21*, 3819. [\[CrossRef\]](#) [\[PubMed\]](#)
56. Stawowy, M.; Olchowik, W.; Rosiński, A.; Dąbrowski, T. The Analysis and Modelling of the Quality of Information Acquired from Weather Station Sensors. *Remote Sens.* **2021**, *13*, 693. [\[CrossRef\]](#)
57. Andrzejczak, K.; Bukowski, L. A method for estimating the probability distribution of the lifetime for new technical equipment based on expert judgement. *Eksplot. i Niezawodn. Maint. Reliab.* **2021**, *23*, 757–769. [\[CrossRef\]](#)
58. Sharma, A.; Singh, P.K.; Kumar, Y. An integrated fire detection system using IoT and image processing technique for smart cities. *Sustain. Cities Soc.* **2020**, *61*, 102332. [\[CrossRef\]](#)
59. Wu, H.; Wu, D.; Zhao, J. An intelligent fire detection approach through cameras based on computer vision methods. *Process Saf. Environ. Prot.* **2019**, *127*, 245–256. [\[CrossRef\]](#)
60. Wieczorek, A.N.; Konieczny, Ł.; Burdzik, R.; Wojnar, G.; Filipowicz, K.; Kuczaj, M. A Complex Vibration Analysis of a Drive System Equipped with an Innovative Prototype of a Flexible Torsion Clutch as an Element of Pre-Implementation Testing. *Sensors* **2022**, *22*, 2183. [\[CrossRef\]](#)
61. Jafari, M.J.; Pouyakian, M.; Khanteymoori, A.; Hanifi, S.M. Reliability evaluation of fire alarm systems using dynamic Bayesian 555 networks and fuzzy fault tree analysis. *J. Loss Prev. Process Ind.* **2020**, *67*, 104229. [\[CrossRef\]](#)
62. Keding, L. An Optimization of Intelligent Fire Alarm System for High-Rise Building Based on ANASYS. In *Intelligence Computation and Evolutionary Computation*; Du, Z., Ed.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 415–421. [\[CrossRef\]](#)
63. Pati, V.B.; Joshi, S.P.; Sowmianarayana, R.; Vedavathi, M.; Rana, R.K. Simulation of Intelligent Fire Detection and Alarm System for a Warship. *Def. Sci. J.* **1989**, *39*, 79–94. [\[CrossRef\]](#)
64. Cha, J.H.; Finkelstein, M. *Point Processes for Reliability Analysis Shocks and Repairable Systems*; Springer: Berlin/Heidelberg, Germany, 2018.
65. Świdorski, A.; Borucka, A.; Grzelak, M.; Gil, L. Evaluation of Machinery Readiness Using Semi-Markov Processes. *Appl. Sci.* **2020**, *10*, 1541. [\[CrossRef\]](#)
66. Liu, Z.; Kim, A.K. Review of Recent Developments in Fire Detection Technologies. *J. Fire Prot. Eng.* **2003**, *13*, 129–151. [\[CrossRef\]](#)
67. Zajkowski, K. Two-stage reactive compensation in a three-phase four-wire systems at nonsinusoidal periodic waveforms. *Electr. Power Syst. Res.* **2020**, *184*, 106296. [\[CrossRef\]](#)
68. Kukulski, J.; Jacyna, M.; Gołębiowski, P. Finite Element Method in Assessing Strength Properties of a Railway Surface and Its Elements. *Symmetry* **2019**, *11*, 1014. [\[CrossRef\]](#)
69. Chiodo, E.; De Falco, P.; Di Noia, L.P. Challenges and new trends in power electronic devices reliability. *Electronics* **2021**, *10*, 925. [\[CrossRef\]](#)
70. Duer, S. Examination of the reliability of a technical object after its regeneration in a maintenance system with an artificial neural network. *Neural Comput. Appl.* **2012**, *21*, 523–534. [\[CrossRef\]](#)
71. Hwang, H.R.; Kim, B.S.; Cho, T.H.; Lee, I.S. Implementation of a Fault Diagnosis System Using Neural Networks for Solar Panel. *Int. J. Control Autom. Syst.* **2019**, *17*, 1050–1058. [\[CrossRef\]](#)
72. Ziółkowski, J.; Żurek, J.; Małachowski, J.; Oszczypała, M.; Szkutnik-Rogoż, J. Method for Calculating the Required Number of Transport Vehicles Supplying Aviation Fuel to Aircraft during Combat Tasks. *Sustainability* **2022**, *14*, 1619. [\[CrossRef\]](#)
73. Żółtowski, B.; Niziński, S. *Modeling of Machine Exploitation Processes*; Markar: Bydgoszcz: Sulejówek, Poland, 2002.
74. Migdalski, J. *Reliability Engineering—A Handbook*; ATR: Bydgoszcz, Poland, 1992.
75. Gupta, S.; Kanwar, S.; Kashyap, M. Performance characteristics and assessment of fire alarm system. *Part 19 Mater. Today Proc.* **2021**, *47*. [\[CrossRef\]](#)
76. Paś, J.; Klimczak, T.; Rosiński, A.; Stawowy, M. The Analysis of the Operational Process of a Complex Fire Alarm System Used in Transport Facilities. *Build. Simul.* **2022**, *15*, 615–629. [\[CrossRef\]](#)
77. Kollek, W.; Kudźma, Z.; Stosiak, M.; Mackiewicz, J. Possibilities of diagnosing cavitation in hydraulic systems. *Arch. Civ. Mech. Eng.* **2007**, *7*, 61–73. [\[CrossRef\]](#)
78. Soszyńska-Budny, J. General Approach to Critical Infrastructure Safety Modelling. In *Safety Analysis of Critical Infrastructure. Lecture Notes in Intelligent Transportation and Infrastructure*; Springer: Cham, Switzerland, 2021. [\[CrossRef\]](#)
79. Kołowrocki, K.; Soszyńska-Budny, J. Critical Infrastructure Safety Indicators. In *Proceedings of the 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 16–19 December 2018*; pp. 1761–1764. [\[CrossRef\]](#)

-
80. Blokus, A.; Dziula, P. Relations of Imperfect Repairs to Critical Infrastructure Maintenance Costs. *Sustainability* **2021**, *13*, 4917. [[CrossRef](#)]
 81. Dziula, P.; Kołowrocki, K.; Soszyńska-Budny, J. Maritime Transportation System Safety-Modeling and Identification. *TransNav Int. J. Mar. Navig. Saf. Transp.* **2013**, *7*, 169–175. [[CrossRef](#)]
 82. Barone, G.; Frangopol, D.M. Life-cycle maintenance of deteriorating structures by multi-objective optimization involving reliability, risk, availability, hazard and cost. *Struct. Saf.* **2014**, *48*, 40–50. [[CrossRef](#)]
 83. Młynarski, S.; Pilch, R.; Smolnik, M.; Szybka, J.; Wiązania, G. A model of an adaptive strategy of preventive maintenance of complex technical objects. *Eksploat. I Niezawodn. Maint. Reliab.* **2020**, *22*, 35–41. [[CrossRef](#)]
 84. Frangopol, D.M.; Liu, M. Maintenance and management of civil infrastructure based on condition, safety, optimization, and lifecycle cost. *Struct. Infrastruct. Eng.* **2007**, *3*, 29–41. [[CrossRef](#)]
 85. Paprocka, I.; Kempa, W.M.; Ćwikła, G. Predictive Maintenance Scheduling with Failure Rate Described by Truncated Normal Distribution. *Sensors* **2020**, *20*, 6787. [[CrossRef](#)]
 86. Slowak, P.; Kaniewski, P. Stratified Particle Filter Monocular SLAM. *Remote Sens.* **2021**, *13*, 3233. [[CrossRef](#)]
 87. Petrillo, A.; Picariello, A.; Santini, S.; Scarciello, B.; Sperlí, G. Model-based vehicular prognostics framework using Big Data architecture. *Comput. Ind.* **2020**, *115*, 103177. [[CrossRef](#)]
 88. Wang, L.; Chen, W.; Chen, K.; He, R.; Zhou, W. The Research on the Signal Generation Method and Digital Pre-Processing Based on Time-Interleaved Digital-to-Analog Converter for Analog-to-Digital Converter Testing. *Appl. Sci.* **2022**, *12*, 1704. [[CrossRef](#)]
 89. Duer, S.; Scaticailov, S.; Paś, J.; Duer, R.; Bernatowicz, D. Taking decisions in the diagnostic intelligent systems on the basis information from an artificial neural network. *MATEC Web Conf.* **2018**, *178*, 07003. [[CrossRef](#)]