applied sciences

MDPI

Article

Evaluation of the Level of Reliability in Hazardous Technological Processes

Darja Gabriska

Department of Applied Informatics, University of SS. Cyril and Methodius, 91701 Trnava, Slovakia; darja.gabriska@ucm.sk

Abstract: In an automated systems environment is very important to predicted failures or unexpected situations to achieve system reliability. Failure of such systems can cause serious property damage, the environment, damage to human health or cause death. The essential task is to determine the tolerable and acceptable risk. The required level of risk for safety-critical systems can be achieved by using international technical standards and applying safety functions. Safety functions are implemented using an electrical/electronic/programmable electronics (E/E/PE) safety-related system. Technical standards offer the aspect of balancing risk tolerability according to the relevant, reliable safety functions. Based on the specific architecture of the whole system, it is possible to determine the maximum failure rate of the probability of failure on demand (PFD_{SYS}) of the selected architecture. Subsequent application of reliability analysis using the event tree analysis (ETA) and fault tree analysis (FTA) methods can optimize the failure rate of the entire system. Application of reliability analysis using event tree analysis (ETA) and fault tree analysis (FTA) methods can only theoretically optimize the failure rate of the entire system with constant initial conditions and constant parameters of the reliability functions. The article proposes a new methodology for dynamic analysis of the state of system reliability as a function of the system operation time, maintenance frequency and system architecture. As a result of the methodology is a library of standard element architectures and simulation models which allows predicting and optimizing the reliability of E/E/PE safety-related systems.

Keywords: failure; safety-critical systems; safety function; event tree analysis; fault tree analysis

Citation: Gabriska, D. Evaluation of the Level of Reliability in Hazardous Technological Processes. *Appl. Sci.* **2021**, *11*, 134. https://dx.doi.org/10.3390/app11010134

Received: 3 November 2020
Accepted: 22 December 2020
Published: 25 December 2020

1. Introduction

Any technical system has no zero faults, no one makes zero-point errors, and in any part of the software design, it is not possible to predict all the operational possibilities of the error. Therefore, the concept of zero risks in a technical system is not achievable nowadays [1]. However, general risk perception, especially as a result of a larger accident, often contributes to perceiving the notion of ideally zero risks. In general, most people understand that this is not possible [2].

Automated safety-critical systems that are used in different industries are characterized by the fact that any unforeseen situation or failure in functionality can cause significant financial losses, loss of life or environmental pollution [3]. In terms of running modern computer safety-critical systems, most unexpected situations or failures are due to abnormal software work [4,5]. Enhanced software functionality, the speed of the spread of alarm [6] and the degree of responsibility for safety-critical systems is reflected in the need for a high-quality design and safety of software safety.

Therefore, the concept of defining and accepting acceptable risk for some specific activities is predominant [7]. The actual risk level that is considered tolerable will vary depending on many factors such as the degree of human control over the circumstances, the voluntary or involuntary nature of the risk, the number of people at risk in an individual case. This partly explains why the household remains at one of the highest positions in

the daily human risk table because we have control over what we have decided to do, and therefore we are willing to tolerate the risks.

Safety technologies have been developed to address the level of target-risk and to assess whether the proposed projects meet these objectives, whether they are technological devices, transport systems, medical equipment or any other application.

The development of hazardous industrial process management systems has been conducted in line with international technical standards (mainly IEC 61508 and IEC 61511). These standards describe the life cycle stages of safety-critical systems and also describe the required level of risk. The safety-related systems contain various elements such as devices, hardware or software. They may comprise a separate device or may be part of other devices that perform safety functions. These safety functions need to be applied to achieve the required level of safety. Any failure of safety function significantly affects the possibility of a threat to humans or the environment. Different safety-related system types require different solutions. The correct response to the input signals and fulfillment of the set requirements ensure the proper functioning of the system. Ensuring functional safety requires the engagement of all specified safety functions. An example of a safety system may be an overheat protection device. That device uses a temperature sensor on the motor coil, which disconnects the engine power before it can overheat. However, the presence of special packaging as high-temperature protection is not associated with functional safety (although it is generally related to safety and can prevent the same dangerous situation).

The following chapters address the design or analysis of control systems that perform a critical function. This function guarantees the required level of safety, which corresponds to technical standards. In the design algorithm, it is an important task to determine the degree of risk. This level can be assigned to a specific safety level according to the requirements of the standards. Fault tree and event tree analysis allow the determination of critical fault paths. The proposed logic control scheme represents the investigated technological process. The required level of safety must be ensured throughout the life cycle of this process. The possible set of goals should be achieved by implementing elements of safety functions. The elements are divided into a high-demand or low-demand mode operation. The reliability of high-demand elements is influenced by choice of the frequency of demand.

2. Definition of Safety-Critical Function

Safety features are features implemented with electrical/electronic/programmable electronics (E/E/PE) by a safety-related system. The safety system is based on technologies or external risk mitigation devices designed to achieve a safety status or to support the safety of the equipment under control (EUC) concerning a particularly hazardous situation.

The development of safety-critical software is based on international standards. However, their use leads to multiple delays in software development time and software, as opposed to the development of software not intended for critical safety systems. The software development of safety-critical systems is primarily reflected in financial costs, lengthening the time needed to develop and implement the end product. In addition to the aforementioned problems associated with developing and deploying safety-critical software, the core issues associated with software development organizations include [8]:

- The need to deploy software within a specified time by customers or competitors on the market considerably increases the risk of software failures. Especially errors associated with the program that were not discovered in the development or testing process;
- The development of safety-critical systems is typically the nature of classified information, and therefore, there is no possibility of reusing scientific and technological potential in similar sectors in practice;
- Insufficient qualification of specialists involved in the development of safety-critical systems.

Ensuring the necessary level of reliability and safety while minimizing financial and time losses of safety-critical systems require a special approach to software development, testing, and operation. The meaning of "safety-critical" generally refers to concepts such as nuclear power plants, oil refineries, aviation, and other safety applications, with emphasis

on a high safety, where the loss of safety can cause death, injury or large financial loss. However, it is possible to use an expression in other types of applications, where failure can cause not only injury or death but also a natural disaster.

The aim is to ensure that the residual risk—the likelihood of a dangerous event that arises even with safety features—is less or equal to the permissible risk. Figure 1 shows that it is effective where the risk associated with the managed equipment is reduced to permissible risk using the "necessary risk mitigation" strategy. A risk reduction can be achieved by combining elements such as dependence only on safety systems and may also include organizational measures. EUC risk is the risk that exists within the control system and defines specific dangerous situations. To determine the level of risk, in this case, no safety functions are taken into account. Tolerable risk is a risk that is tolerable following the definition of current values. Residual risk—the risk that exists within the control system, but the addition of E/E/PE safety systems and other risk reduction measures is also considered.

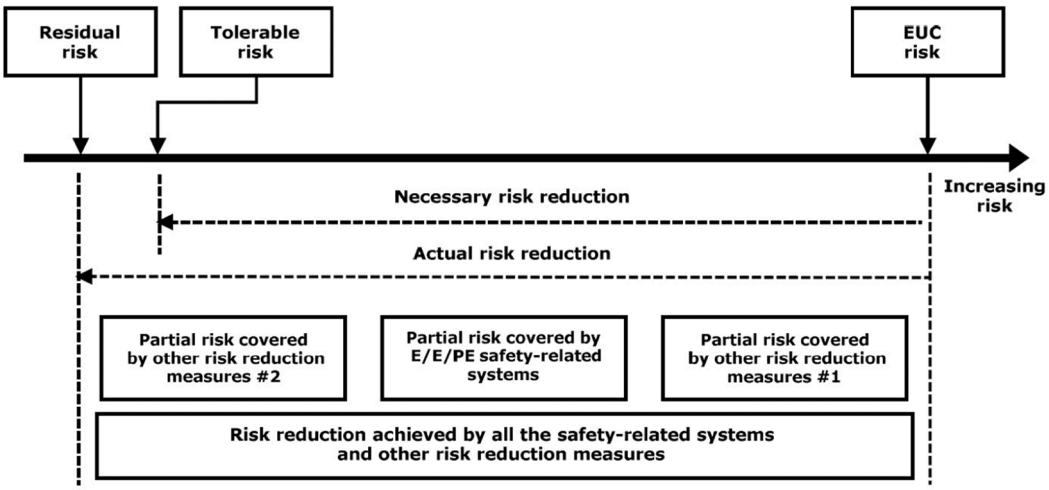

Figure 1. The relationship between the residual risk and the tolerable risk [9].

The method for determining the probability of failure of a safety function for PES (programmable electronic systems) associated with safety operating in high demand or continuous request mode is the same as the calculation method for low demand operation. Except that the average probability of failure on request of the probability of failure on demand (PFD_{SYS} is replaced by the average frequency of the perilous failure per hour of PFH_{SYS}. The general probability of a PFH_{SYS} PES is determined by calculating the severity of the hazardous failures for all subsystems whose set assures the safety function and the resulting sum of the values obtained. Because the probability is small, then the relationship is used [9]:

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE} \quad (1)$$

where PFH_{SYS} is the average frequency of the dangerous failure for the safety function of the safety-related PES, PFH_S is the average value of the dangerous failure for the sensor subsystem, PFH_L is the average value of the dangerous failure for the actuator subsystems and PFH_{FE} is average dangerous failure value for subsystem end elements.

ETA and FTA

The analysis of dangerous situations and risks is one of the phases of the safety life cycle. The assessment of adverse events follows from the concept of the development of the EUC controlled device and its control system. The assessment of risks or adverse events influences the adoption of different measures based on the frequency of the event and the consequent severity of the event. Many analytical methods are used to analyze hazards

and risks. These methods include the techniques fault tree analysis (FTA) and event tree analysis (ETA) [10,11].

FTA is a fault tree analysis. The method is used to identify the probable occurrence of an event that may lead to an adverse event. Events are determined deductively, based on the peak event and looking for the causes that could have caused this event. A tree diagram is used to represent the causes, which shows the structure of the identified events about the fault events. The tree diagram can be used to identify potential causes and failures for qualitative analysis. Quantitative analysis allows you to calculate the probability of occurrence of a peak event based on the partial probabilities of the event [12,13].

ETA is an event tree analysis. The analytical technique used for general reliability assessment. The course of the process and the events that can lead to a possible accident are evaluated. Based on the analysis, equipment failures or errors are specified. The adverse event is the basic starting point. Subsequently, all system responses that may lead to a failure are taken into account. The aim is to evaluate measures, e.g., safety features that are effective in reducing side effects. The method can be used as a complementary FTA method to determine the consequences of an adverse event [13,14].

3. Architectures for High-Demand or Low-Demand Mode

3.1. Architecture 1oo1

This architecture 1oo1 (1 out of 1) consists of a single channel. If any of the individual elements in the circuit fails, then the entire system stops working [15]. The following formulas are used to calculate the intensity of failure:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} \tag{2}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{3}$$

$$\lambda_{DU} = \lambda_D(1 - DC);\ \lambda_{DD} = \lambda_D DC \tag{4}$$

where λ_D is the dangerous failure rate (per hour) of a channel in a subsystem, λ_{DU} is the undetected dangerous failure rate (per hour) of a channel in a subsystem, λ_{DD} is the detected dangerous failure rate (per hour) of a channel in a subsystem, t_{CE} is the channel equivalent mean downtime (hour) for 1oo1 and 1oo2 architectures, MRT is the mean repair time (hour), $MTTR$ is the mean time to restoration (hour), DC is the diagnostic coverage.

If it can be assumed that a safety-related system detects any failure in a safe state, then for the 1oo1 architecture:

$$PFH_G = \lambda_{DU} \tag{5}$$

where PFH_G is the average frequency of dangerous failure for the group of voted channels.

3.2. Architecture 1oo2

Full 1oo2 (1 out of 2) architecture consists of two channels. If one of two in the circuit fails, then the redundant logic solvers can execute the safety function individually. The t_{CE} value is calculated according to Equation (3). If the safety system is assumed to bring the output unit system to a safe state immediately upon detection of a failure in both channels and a conservative approach is used, then the following relationship is used:

$$PFH_G = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})(1 - \beta)\lambda_{DU}\, t_{CE} + \beta\lambda_{DU} \tag{6}$$

where β is the fraction of undetected failures that have a common cause.

Formulas for calculating static reliability are written in the standard 61508-6 for every architecture. In the article, Equations (2)–(6) are given as a result of replacing the constant variable T (time) in the formulas for calculating the intensity of failures for derivation dt/t. Thus, Equations (2)–(6) determine the change in the reliability of the control system during operation.

Table 1 lists the basic formulas for specific system-wide architectures. At the constant value of the proof test interval (T1) parameter, it is possible to determine the maximum failure rate of the PFD_G of the selected architecture. For a variable parameter, it is possible to calculate the instantaneous failure rate at a time when T1 is less than the control interval [16].

Table 1. Basic formulas for specific architectures.

Architecture	Formulas for Specific Architectures of the Whole System
1oo1	$T_1 = var$ **Low demand** $PFD_G(t) = \frac{\lambda_{DU}}{2} \int_0^{T_1} dt_{CE} + \frac{\lambda_{DU}}{2} MRT + \lambda_{DD} MTTR$ **High demand** $PFH_G(t) = const = \lambda_{DU}$
1oo2	$T_1 = var$ $PFD_G(t) =$ $2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 \left(\frac{\lambda_{DU}}{6\lambda_D} \left(\int_0^{T_1} dt_{CE} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right)^2 +$ $+\beta \frac{\lambda_{DU}}{2} \left(\int_0^{T_1} dt_{CE} + MRT \right) + \beta_D \lambda_{DD} MTTR$

There are known methods that are used to analyze the risks and hazards of computer-controlled systems and technological processes. The choice of a particular method depends on the experience of system designers and analysts and the amount of information about the reliability of system components and the quality of this data. At the same time, standard 61508 allows both the use of statistical data, which are the result of testing of components offered by the manufacturer and data which have been obtained during previous use. The actual use of the fault tree and event tree is described in the next chapter.

4. Description of the Technological Process

As an object for analysis, we will use the winding dryer as an element of the technological process of production of clutch lining for the automotive industry. The basic element of the liner is the cord rope, which, when soaked in a flammable solvent, passes through a winding dryer. The drying process produces a combustible gas, which can cause an explosion if the parameters of the technological processes are not met. Controlled parameters are the heating temperature and the concentration of combustible gas. When the temperature exceeds the maximum set temperature, then arises the danger of explosion. The control system receives information on exceeding the set level temperature. The system starts a program to implement the safety function of the technological process. A measuring system, an operator, protection system with architecture 1oo2 for controlling fans and valves for removing hazardous gas are involved in the implementation. The level of risk of an explosion is determined by the reliability of the control system, which is implemented by architecture 1oo2. The article provides, as an example, a model for simulating the change in reliability over time during the operation of a technological process.

The winding dryer (Figure 2) on the right side has a gas warning device that forms an infrared gas transducer and a sampling system. Signal evaluation and eventual alarm reporting are performed in the central switch box. The concentration of solvents in the dryer is measured in an infrared gas transducer before the concentration exceeds the limit value, which is 35% lower explosive limit (LEL) through the throttle valve, the volume of exhaust air is increased, and an alarm is triggered on the gas warning system. At a concentration higher than 25% of the LEL, the heating of the circulating air is switched off, and the drive motor reels and a warning signal is turned on. Individual gas samples are obtained from the utility space and subsequently pumped into the dryer.

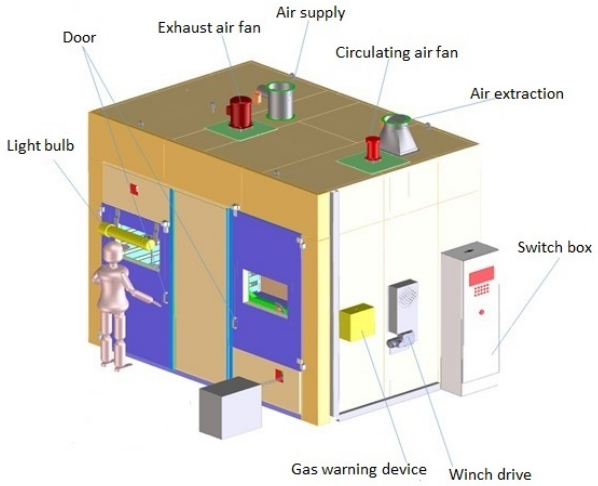

Figure 2. Winding dryer.

Circulating air is cooled in copper conduit to the ambient temperature, where the volume flow is monitored through the flowmeter. If the bulk flow of gas in the analytical instrument is not large enough, then the heating is switched off.

The winding dryer is equipped with one V1 exhaust air fan and one V2 circulating air fan in Figure 3. With the position of the fresh air flaps K1 and the heating air K2, it is possible to regulate the temperature of the circulating air while the exhaust air flap K3 is regulated based on the concentration of solvents in the interior of the furnace. If it is necessary to remove it during the emergency or the flue gas flushing directly from the production hall, the flushing flap K4 is used.

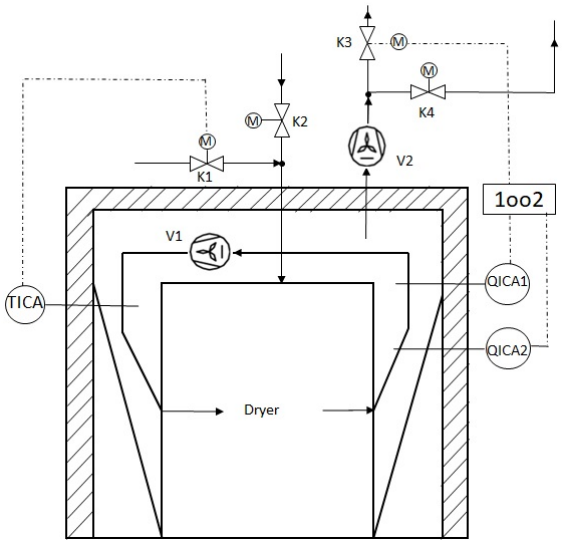

Figure 3. Block diagram of the winding dryer.

Automatic programmable devices from Siemens type S7-300 are used to control automatic operation and to implement safety-critical functions. Communication with the Micromaster frequency inverter, which delivers the technological air to the reel dryer, runs through the Profibus interface. Operation of this control is performed via the touch panel, which communicates with the processor via multipoint interface (MPI). The circulating air temperature in the furnace is measured in the volume flow of the circulating air through a temperature sensor (TICA). If the maximum temperature is exceeded, the safety temperature limiter is activated. The redundancy of the gas concentration in the air is ensured by implementing the reliability architecture 1oo2 connected to the explosive gas concentration measuring systems (QICA1, QICA2) measuring systems.

5. Results

5.1. Applying Reliability Analysis of PES Management Using the ETA Method

Figure 4 shows simple calculations for an example event tree for completely independent branches. Exceeding temperatures can trigger 7 different types of emergency events. The analysis shows that there is an explosion in the case of dangerous events 4 and 7. With the proposed level of safety, the probability of explosion is 1.9×10^{-4}, which corresponds to the safety integrity level of SIL1 [17]. In the case of this technological process, the next layer of protection is the outer enclosure itself, which protects personnel in case of an explosion. Each subsequent protective layer increases the level of safety integrity. Therefore, in the case of a winding dryer, the final level of safety integrity is SIL2, which is sufficient for this technological process. For SIL2, the probability of large economic losses and/or lifetime losses is in the range of 10^{-7} to 10^{-6} per hour.

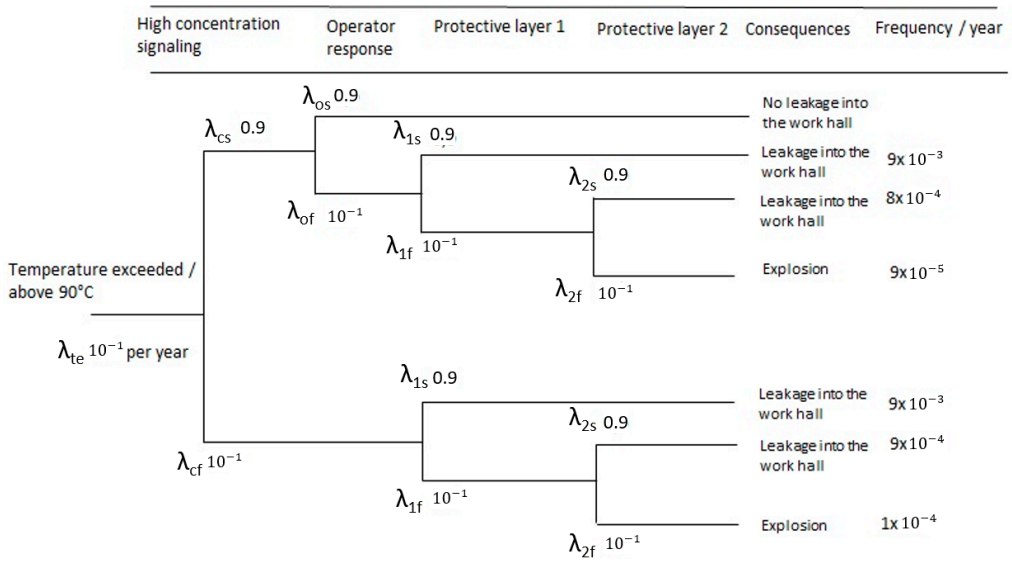

Figure 4. Fault tree. Where λ_{cs} is the control success, λ_{cf} is the control fault, λ_{os} is the operator success, λ_{of} is the operator fault, $\lambda_{1,2s}$ is the protective layer success, $\lambda_{1,2f}$ is the protective layer fault.

The fault tree (Figure 4) of the operation of the technological process control system allows tracing the possible variants of the propagation of errors in the functioning of the control system. Each variant of error propagation ends with a description of the consequences of an accident and numerical value. This value represents the probability of accident occurrence with a specific description. The probability of error is described by the frequency of occurrence of the error in one year. The frequency of accidents per year is determined by the product of the error rates along the path of propagation of events.

For example, the maximum probability of a gas explosion (Figure 4, the lower branch of error propagation) is determined by the frequency:

$$\lambda_{exp} = \lambda_{te} \times \lambda_{cf} \times \lambda_{1f} \times \lambda_{2f} = 10^{-1} \times 10^{-1} \times 10^{-1} \times 10^{-1} = 10^{-4}(1/year) \quad (7)$$

where λ_{exp} is the frequency of probability of explosion in case of failure of safety-critical functions, λ_{te} is the input event that starts a safety-critical function, λ_{cf} is the signaling failure frequency, $\lambda_{1f,2f}$ is the probability of failure of the signaling system.

5.2. Applying Reliability Analysis of PES Management Using the FTA Method

The tree of failure method is a hardware malfunction evaluation method that represents a logical approach to identifying the failure of individual components along with general system failure [18–20]. The fault tree represents the logical structure of the system, but this model does not consider the aspect of system behavior over time. The fault tree

uses a deductive method of analyzing events from the top level to the failure of individual components. Figure 5 shows a troubleshooter of a winding dryer control system that consists of elements operating sequentially and connected by the OR operator or elements operating in parallel and thus connected by the AND operator. The tree diagram of failures shows how the failure of individual elements in a certain sequence can lead to system failure in the case of an exploded technological process. Elements of the tree (Figure 5) V1, V2, . . . , K3, represented by rectangles, simulate the binary logical state (Ok, fault) of the elements of the functional diagram of the control system (Figure 3). The presented diagram allows you to check the logic of the process protection system.

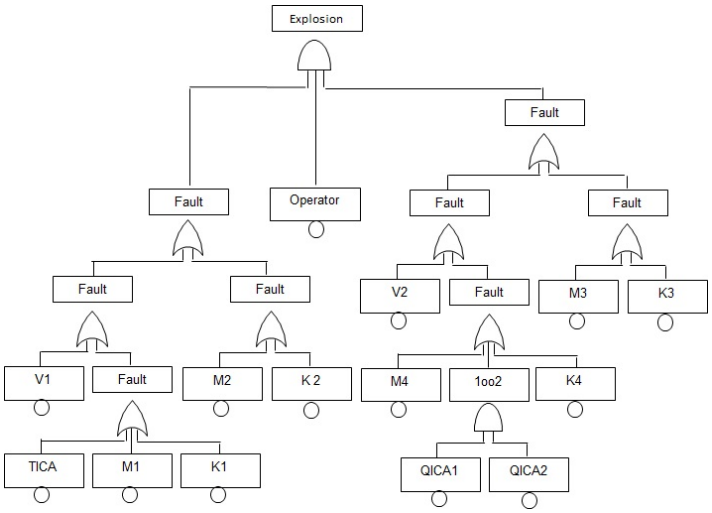

Figure 5. Event tree.

5.3. Design of a Mathematical Model of a Dynamic Tree of Failures

As mentioned above, the fault tree model does not take into account the temporal aspect of system behavior. Computational formulas in the standard are listed for the device check, where T_1 is constant. Therefore, a dynamic mathematical model is proposed in which the failure interval is represented by the function $\int_0^{T_1} dt$. Figure 6 shows the design of the 1oo1 architecture model for the calculation of the instantaneous failure rate in the Simulink environment of the Matlab software. The given architecture assumes the use of one channel, and any dangerous failure leads to a breach of the safety function when a request for its execution arises. Subsequently, according to the calculations, it is possible to take into account the time parameter and its impact on the overall failure of the system.

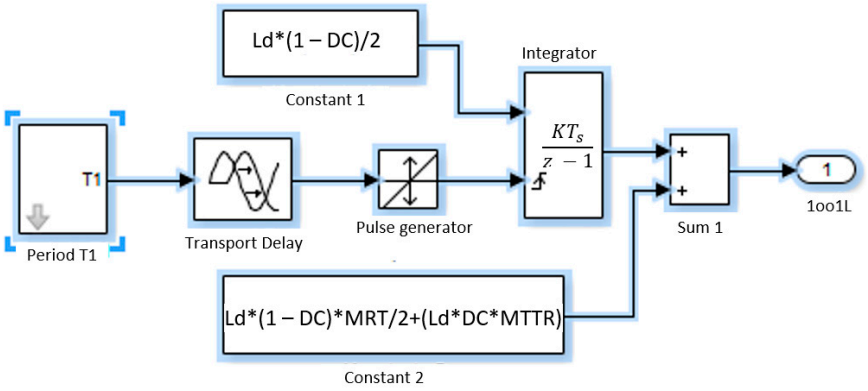

Figure 6. Model of instantaneous failure calculation for 1oo1 architecture in Simulink of Matlab software.

Figure 7 shows the design of a 1oo2 architecture model for the calculation of the instantaneous failure rate in the Simulink environment of the Matlab software. The architecture is

represented by two channels connected in parallel so that any of the channels can perform a safety function. Thus, dangerous failures in both channels must occur due to a breach of the safety function. It is assumed that any diagnostic testing only informs about the faults found and cannot change either the output states of the channels or the result of the voting. In this case, it is also possible to take into account the time parameter and its impact on the overall system failure based on the calculations. Figure 8 shows the logical structure of the control system.

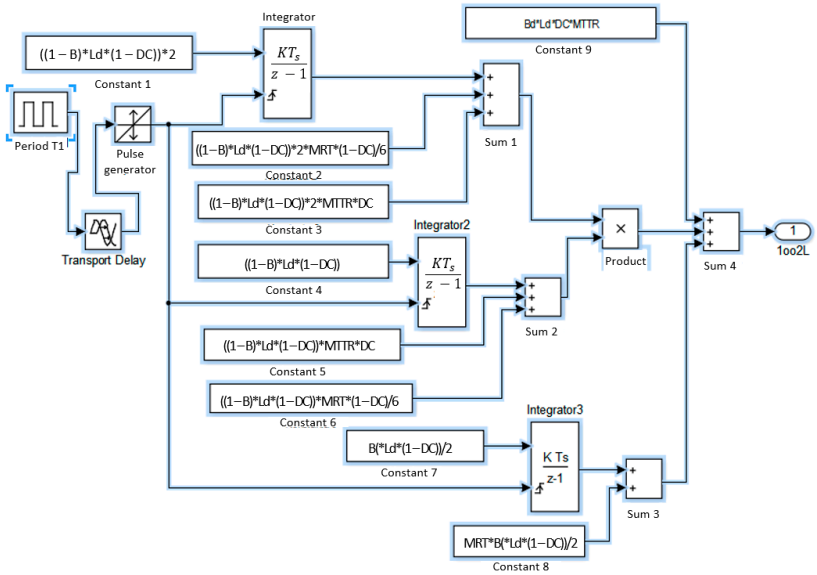

Figure 7. Model of instantaneous failure calculation for 1oo2 architecture in Simulink of Matlab software.

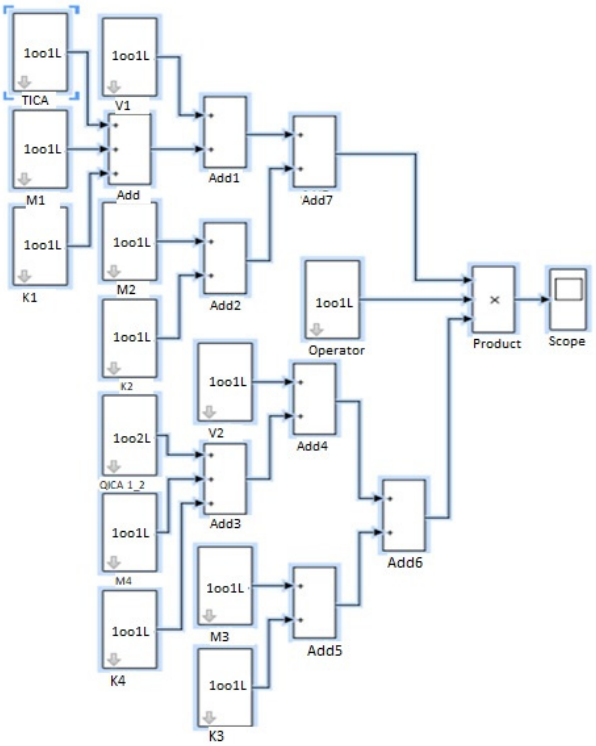

Figure 8. The complete model of winding dryer.

Each model component has its configuration form in which it is necessary to enter the relevant input parameters according to the calculation formulas. The contents of all parameters of each component are given in Table 2.

Table 2. Parameters for component modeling.

Parameter	Architecture	T_1 (h)	Delay T_1	L_d	MRT(h)	MTTR	DC (%)	β (%)	β_d
TICA	1oo1	4380	0	2.5×10^{-6}	8	8	90	-	-
M1	1oo1	8760	0	0.5×10^{-6}	8	8	60	-	-
K1	1oo1	17,520	0	0.5×10^{-5}	8	8	0	-	-
V1	1oo1	8760	0	0.5×10^{-5}	8	8	60	-	-
M2	1oo1	8760	2190	0.5×10^{-6}	8	8	60	-	-
K2	1oo1	17,520	4380	0.5×10^{-6}	8	8	0	-	-
QICA1,2	1oo2	4380	1100	0.5×10^{-6}	8	8	90	10	5
M4	1oo1	8760	4380	0.5×10^{-6}	8	8	60	-	-
K4	1oo1	17,520	8760	0.5×10^{-5}	8	8	0	-	-
V2	1oo1	8760	4380	0.5×10^{-5}	8	8	60	-	-
M3	1oo1	8760	6570	0.5×10^{-6}	8	8	60	-	-
K3	1oo1	17,520	10,950	0.5×10^{-6}	8	8	0	-	-
Operator	-	4380	0	2.5×10^{-6}	8	8	0	-	-

Figure 9 shows the configuration form for the simulation models of the 1oo1 and 1oo2 architectures.

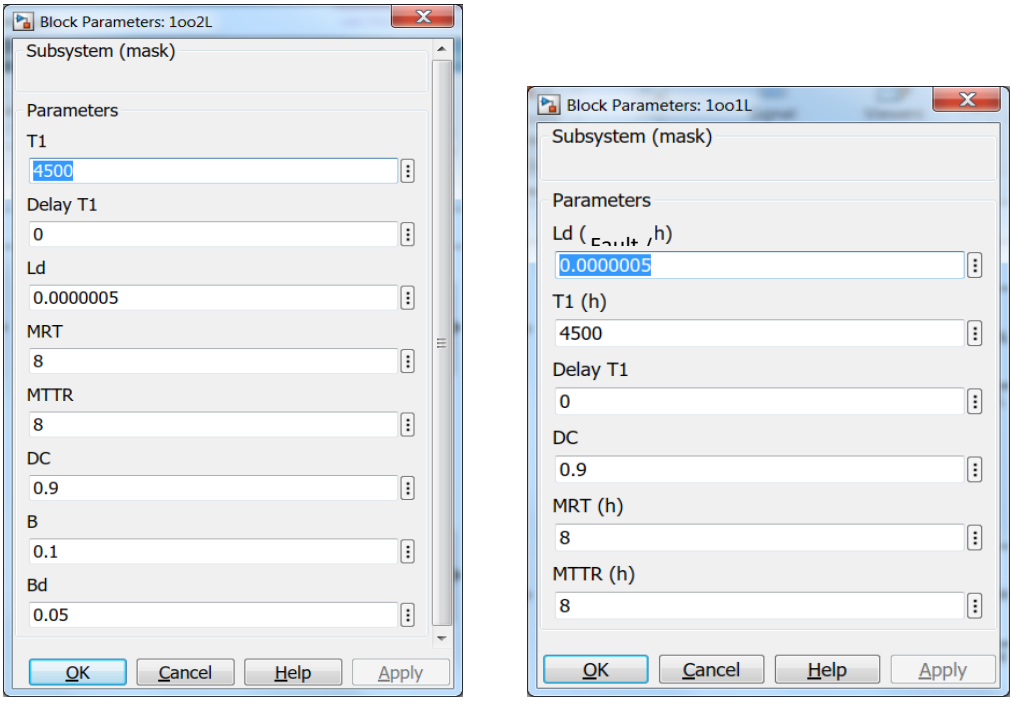

Figure 9. Configuration form for 1oo1 and 1oo2 architecture simulation models.

Table 2 lists numeric parameter values for each component model. The described process with protective layers is represented as an example of the use of the safety of operation. Therefore, the values in the table represent only the test parameters selected based on the estimates from tables given in IEC 61508-6. The value of T_1 represents the time interval between tests (hours). Determination of the shift parameter T_1 (delay T_1) is determined by the time shift that occurs between the commissioning time and the first test time. By changing the shift parameter for individual components, it is possible to optimize

the failure of the entire system, divide the control time so that the moments of maximum failure are not at the same time.

Other parameters in Table 2 represent values such as MRT (hours), which is the mean repair time (hours), MTTR the mean time to restoration (hour), DC is the diagnostic coverage (0%, 60%, 90%, 99%), β is the proportion of undetected faults that have a common cause (expressed as a fraction in equations and elsewhere in percent) 2%, 10%, 20% and β d are disorders that are detected by diagnostic tests and represent fractions that have a common cause (1%, 5%, 10%). Ld represents λ_d. The Simulink environment does not allow writing the letters of the Greek alphabet, so it is listed as Ld. The values of the probability of failures of individual elements of the structure were provided by the technologists of the production process based on a 15-year history of operation.

In modeling, the "fixed step" type with a numerical value of 1 is selected for the modeling step, which corresponds to a real one-hour time. Figure 10 shows an output timing diagram of the variation of the winding dryer failure rate over 5 years. The maximum failure rate reaches 1.58×10^{-4} 1/h, corresponding to SIL1.

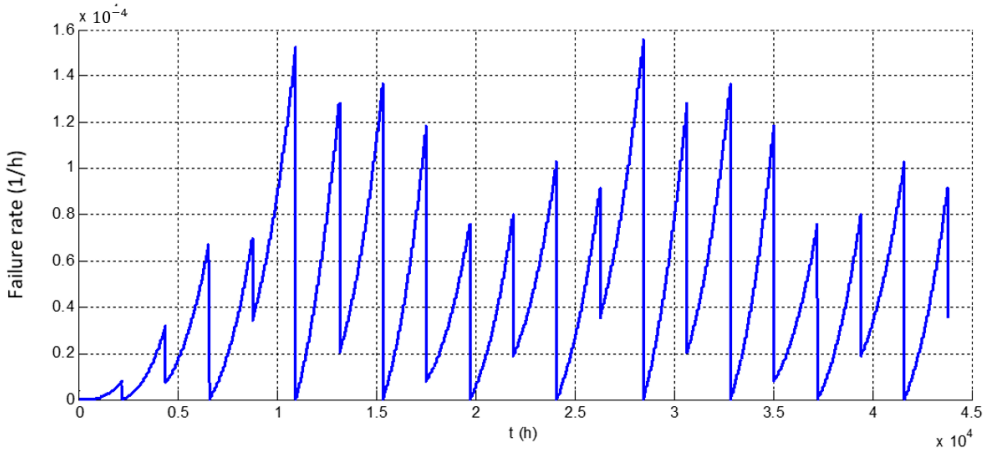

Figure 10. The timing diagram of system failure.

6. Discussion

The use of safety-critical systems in the industry carries the risk of a dangerous event, which may be caused by an unforeseen situation, as well as the failure of the system with possible economic, environmental consequences, or injuries to loss of life. By defining the concept of safety-critical systems, concepts such as failure, dangerous events, etc., come to the fore. These concepts are relevant throughout the life cycle of safety-critical systems, and their essence is determined by probability theory. The technical standards for the implementation of safety-critical systems contain basic calculation procedures for determining the probability of failure, and the basis for the calculations are statistical parameters obtained from theoretical calculations or the analysis of data from the previous operation of similar systems [21–24].

The calculation results then form the basis for the design and implementation of a system, which ensures the safety of a technological process throughout its entire life cycle.

Methods for the analysis and design of software and hardware systems for the implementation of safety functions widely use various principles of theoretical mathematical calculations, mathematical and simulation modeling [25]. These methods describe the principles of ensuring the required level of safety at all stages of the process life cycle. To assist with the selection of methods and means, tables are available for the various methods according to the four safety integrity levels [10].

Possible modeling methods include:

- Analysis of the consequences of the causes of failure [10];
- Fault tree analysis [26];

- Markov models [27,28];
- Block diagrams of reliability [29,30].

Methods designed for the analysis of hardware and software systems for the implementation of safety functions show the possibilities of using the application for specific technological processes. These methods describe the technologies that can be used to ensure the safe operation of the technological process. The event tree method allows you to graphically display possible scenarios of system operation in terms of the time factor. By building an event tree, it is possible to prove the safety of the entire system even in the event of unwanted basic events. The fault tree method allows a graphical representation of unreliable locations and provides an in-depth analysis of system reliability. By applying the use of the event tree and the fault tree to a specific winder dryer process, it is possible to optimize the failure rate of the entire system. The example given also shows the analysis of the evaluation of the failure of safety-critical functions of a part of the technological process of production of automotive clutches using the most used methods.

The above methods allow the development of systems for the implementation of nonchalant-critical functions. However, they do not solve the issue of changing some parameters of reliability during the animal cycle of the technological process. For example, the aging of electrical components. The presented methodology for modeling the dynamics of standard control implementation architectures allows us to optimally decompose their servicing in time.

Figures 4 and 5 present the results of the analysis of the safety of the technological process using the methods recommended by the standards IEC 61508-6. This standard contains the formulas that were the basis for the analysis of the safety level of the technological process. In the structure of elements of control systems, there are elements of continuous demand and operation with low demand. For elements with low demand, there is an assumption that maintenance takes place periodically. After the service, this element becomes more reliable. The level of safety decreases with operating time. This fact seriously affects the overall reliability of the system. There is a chance of random occurrence when several elements at the same time have the lowest reliability. Such a case is the cause of the existence of moments when the overall reliability may fall below the permissible level. It follows that changing the periodicity and sequence of revisions minimizes the likelihood of failure. For optimization, it is necessary to have a time course of the change of reliability for elements with low demand. The time course of the reliability change can be determined by designing a process simulation using the formulas given in Table 1. The modeling scheme in the Simulink environment contains models of elements of standard architectures for the implementation of safety-critical functions. The configuration of the models corresponds to Figure 5. The result of the modeling is shown in Figure 10. The figure shows that there are times when there is a greater probability of failure. The probability arises due to the synchronization of the maximum failures of elements with low demand. The shown effect is the reason for the expansion of research in the field of design methods for minimizing the failure rate of safety-critical systems. Optimization is possible by changing the periodicity and sequence of revisions. Scientific research is important in areas where failures can be critical, such as in aviation, nuclear power plants, etc.

Funding: This research was funded by the Scientific Grant Agency of the Ministry of Education, Science, Research and Sport of the Slovak Republic and the Slovak Academy of Sciences, grant number VEGA 1/0145/18.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Durmuş, M.S.; Eriş, O.; Yildirim, U.; Söylemez, M.T. A New Bitwise Voting Strategy for Safety-critical Systems with Binary Decision. *Turk. J. Elec. Eng. Comp. Sci.* **2015**, *23*, 1507–1521. [CrossRef]
2. IEC. *IEC 61511-3:2016, Functional Safety—Safety Instrumented Systems for the Process Industry Sector—Part 3: Guidance for the Determination of the Required Safety Integrity Levels*; IEC: Geneva, Switzerland, 2016.
3. Smith, D.J.; Simpson, K.G.L. *Safety Critical Systems Handbook*, 1st ed.; Butterworth-Heinemann: Oxford, UK, 2010.
4. Gabriska, D. Risk analysis in control design of safety critical process. In Proceedings of the Applied Natural Sciences 2015: The 5th International Scientific Conference, Jasna, Low Tatras, Slovakia, 30 September–2 October 2015; pp. 102–108.
5. Billinton, R.; Allan, R.N. *Reliability Evaluation of Engineering Systems: Concepts and Techniques*; Springer Science & Business Media: Berlin, Germany, 2013; p. 349. ISBN 978-1-4615-7730-0.
6. Šimon, M.; Huraj, L.; Dirgová Luptáková, I.; Pospíchal, J. Heuristics for Spreading Alarm throughout a Network. *Appl. Sci.* **2019**, *9*, 3269. [CrossRef]
7. Smith, D.J. *Reliability, Maintainability and Risk: Practical Methods for Engineers*; Elsevier Science Technology: Amsterdam, The Netherlands, 2011.
8. Mudrončik, D.; Galik, M. Normy Pre Tvorbu Softvéru Riadiacich Systémov. *At. J.* **2009**, *4*, 22–25. Available online: http://www.odbornecasopisy.cz/res/pdf/38879.pdf (accessed on 26 October 2020).
9. IEC. *IEC 61508-5:2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*; IEC: Geneva, Switzerland, 2010.
10. IEC. *IEC 62502-2011, Methods of Analysis of Reliability. Event Tree Analysis (ETA)*; IEC: Geneva, Switzerland, 2011.
11. IEC. *IEC 61025-2007, Fault Tree Analysis (FTA)*; IEC: Geneva, Switzerland, 2007.
12. Ragheb, M. Event Tree Analysis. 2013. Available online: http://mragheb.com/NPRE%20457%20CSE%20462%20Safety%20Analysis%20of%20Nuclear%20Reactor%20Systems/Event%20Tree%20Analysis.pdf (accessed on 10 October 2020).
13. Hosseini, N.; Givehchi, S.; Maknoon, R. Cost-based fire risk assessment in natural gas industry by means of fuzzy FTA and ETA. *J. Loss Prev. Process Ind.* **2020**, *63*, 104025. [CrossRef]
14. Shafiee, M.; Enjema, E.; Kolios, A. An Integrated FTA-FMEA Model for Risk Analysis of Engineering Systems: A Case Study of Subsea Blowout Preventers. *Appl. Sci.* **2019**, *9*, 1192. [CrossRef]
15. Goble, W.M. *Evaluating Control System Reliability—Techniques and Applications*, 3rd ed.; Instrument Society of America: Research Triangle Park, NC, USA, 2010; p. 458. ISBN 978-1-934394-80-9.
16. Gabriska, D.; Nemeth, M. Modeling based on probability calculations related to the E/E/PE system. In Proceedings of the INES 2016—20th Jubilee IEEE International Conference on Intelligent Engineering Systems, Budapest, Hungary, 30 June–2 July 2016; pp. 113–118.
17. Gulland, W.G. Methods of Determining Safety Integrity Level (SIL). Requirements—Pros and Cons. Practical Elements of Safety. In Proceedings of the Twelfth Safety-Critical Systems Symposium, Birmingham, UK, 17–19 February 2004; pp. 105–122.
18. Clifton, A.E. *Hazard Analysis Techniques for System Safety*; John Wiley & Sons: Hoboken, NJ, USA, 2005.
19. Fuchs, P.; Kamenicky, J.; Saska, T.; Valis, D.; Zajicek, J. Some Risk Assessment Methods and Examples of their Application. Technical University of Liberec. 2012. Available online: https://www.researchgate.net/publication/310493920_Some_Risk_Assessment_Methods_and_Examples_of_their_Application (accessed on 10 October 2020).
20. Moubray, J. *Reliability-Centred Maintenance*; Butterworth-Heinemann: Oxford, UK; Industrial Press Inc.: New York, NY, USA, 1997.
21. Norwegian Oil and Gas. *Norwegian Oil and Gas Association Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry. No.: 070*; Norwegian Oil and Gas: Stavanger, Norway, 2018.
22. Johnson, C. *Failure in Safety-Critical Systems: A Handbook of Incident and Accident Reporting*; Glasgow University Press: Glasgow, UK, 2003.
23. The Motor Industry Research Association. *Development Guidelines for Vehicle Based Software*; The Motor Industry Research Association: Nuneaton, UK, 1994.
24. The Center for Chemical Process Safety (CCPS). *Layer of Protection Analysis—Simplified Process Risk Assessment*; The Center for Chemical Process Safety (CCPS): New York, NY, USA, 2001.
25. Leveson, N. A New Accident Model for Engineering Safer Systems. *Saf. Sci.* **2004**, *42*, 237–270. [CrossRef]
26. Greenberg, H.R.; Cramer, J.J. *Risk Assessment and Risk Management for the Chemical Process Industry*; Wiley and Sons: Hoboken, NJ, USA, 1991.
27. IEC. *IEC 61165-1995. Application of Markov Techniques*; IEC: Geneva, Switzerland, 1995.
28. Cox, R.E.; Miller, H.D. *The Theory of Stochastic Processes*; Methuen and Co. Ltd.: London, UK, 1963.
29. Fussel, J.B.; Arend, J.S. System Reliability Engineering Methodology. *Nucl. Saf.* **1979**, *20*, 97.
30. Vesely, W.E.; Goldberg, F.F.; Roberts, N.H.; Haasl, D.F. *Fault Tree Handbook. NUREG—0942, Division of System Safety Office at Nuclear Reactor Regulation*; U.S. Nuclear Regulatory Commission: Washington, DC, USA, 1981.