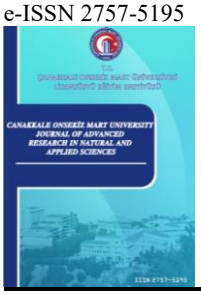
e-ISSN 2757-5195



Çanakkale Onsekiz Mart University

Journal of Advanced Research in Natural and Applied Sciences

Open Access

doi.org/10.28979/jarnas.1121842 2023, Vol. 9, Issue 1, Pages: 65-77 dergipark.org.tr/tr/pub/jarnas

Safety Assessment of Speed Governing Systems in Hydroelectric Power Plants: A Functional Safety Perspective

Özgür Turay Kaymakçı[1,*], Nezihe Merve Balcı[2]

[1]Department of Electrics & Electronics Engineering, Faculty of Engineering, Çanakkale Onsekiz Mart University, Çanakkale, Türkiye
[2]BRK Energy Investment Comp., Istanbul, Türkiye

Article History

Received: 26.05.2022

Accepted: 12.09.2022

Published: 05.03.2023

Research Article

Abstract − In line with the advancing technology, reliability has become one of the critical factors to be taken into consideration by the operators in the energy sector to minimize losses regarding cost and time. This issue is directly related to the reliability of the elements, namely the subsystems that make up the system. This study examines the control architecture of speed governing system within the turbine control system of hydroelectric power plants, which has to be regarded as a critical system and provides an indispensable source of guidance and knowledge to researchers and also implementation engineers as well. For this perspective, a reliability analysis has been performed for the speed governing system and the risks with the control system have been revealed. Taking IEC 61508 and IEC 61511 standards as reference within this scope, the safety concepts and the related parameters have been explained and the corresponding methods for risk analysis have been mentioned. As a result, a new safety-related control system configuration overcoming the unacceptable risks with the speed governing system has also been proposed. It has been proved that safety integrity level of the proposed safety-related control system is at the desired level that can make the related safety related functions verify the identified safety level.

Keywords *– Functional Safety, hydraulic power plants, reliability, safety critical systems, speed governing systems*

1. Introduction

Need for energy in the world has been rising as a result of numerous socioeconomic factors which are increasing population, social and economic growth, as well as other factors, such as urbanization and technological development. Energy projection of EIA (US Energy Information Administration) forecasts that demand for energy will grow nearly %50 between 2021 and 2050 especially driven by non OECD Asia countries. 25% of this energy demand is foreseen to be generated from renewable resources. So hydroelectric power plants must have high-level safety systems to fulfil this high level of energy demand in due time and an uninterrupted manner. This would also enhance the useful life of the plant while keeping production, efficiency, reliability, and availability at the highest level possible (Nalley & LaRose, 2021). The 1950s mark the start of studies on reliability regarding electricity distribution. In the 1960s, the development of new methods for system reliability analyses became the focus of studies. The implication of failures occurring in components on the system and environment was also examined by time. New methods were developed during that period and firstly adapted to nuclear power plants, the most critical process of today's world. The possible consequences of a series of failure scenarios developed were also studied (Brennan, 2001).

As the application of reliability analyses in industrial systems become more widespread; IEC 61508 identifying the references of safety applications for electrical, electronic and programmable electronic systems were formed (IEC, 2010). In time, more detailed standards were developed for different sectors, using IEC 61508

[1] okaymakci@comu.edu.tr
[2] merve.balci@yahoo.com
[*]Corresponding Author

as reference. IEC 61513 is one of those which provides requirements and recommendations for the instrumentation and control of nuclear power plants (IEC, 2011).

Numerous studies, in which reliability analyses of plants are available in literature, such as different electrical energy generation resources (i.e. nuclear, thermal and wind) were examined according to the dynamic characteristics of the power systems. By identifying dynamics through methods such as Monte Carlo simulation, reliability analyses were realized by using Markov model and fault tree method in these studies (Billinton & Wang, 1999; Brown, Gupta, Christie, Venkata, & Fletcher, 1996; Chowdhury, Bertling, Glover, & Haringa, 2006; Gubbala & Singh, 1995; Tripathi, Singh, Singh, & Singh, 2021; Zio, 2013). The authors used the reliability index approach in all the parts of the power plants (Khosravi, Azli, & Babaei, 2010; Perman, Senegacnik, & Tuma, 1997; Yu, Tong, Zhao, & Zhang, 2009). Besides, different stochastic characteristics regarding the integration of the wind energy power plant into the grid were studied. Particularly, the reliability effects of the energy power plants' interconnected system connection on the grid have also recently been addressed (Kilic & Basa Arsoy, 2013; Zhang, Chowdhury, & Koval, 2010). Besides, there exist certain studies in the literature that deal with the frequency control in hydro power plants by the help of governing systems. In these studies, working characteristics and frequency control modes of governing systems were analysed (C. Wang, Wang, & Zhang, 2021). Since the critical position of the speed governing system in energy production is well known by the sector representatives, even a standard has been revealed in this context (IEEE, 2007, 2011). Also, simulation of the speed controller and valve correlation were realized (Zhu et al., 2021).

There are also articles in which improvement of frequency control is aimed at, assessing factors that identify the limits of stability and reliable working (Naghizadeh, Jazebi, & Vahidi, 2012). Also Wang et. al. have worked over speed protection of speed governing systems related to nuclear power plants (L. Wang, Sun, Zhao, & Liu, 2019). Pan et. al. worked on transient performance improvement of speed governing systems by regulating the control strategy in order to improve the safety (Pan, Zhu, Liu, Liu, & Tian, 2021). The studies in the literature conducted mainly dwelled on the frequency control function of the speed governing system, placing emphasis on modelling of the systems and stability thereof.

The risks of the governing system were not analysed from a functional safety perspective. Neither has a theoretical nor a practical work been carried out, concerning the necessity of using the governing system along with a safety related system that is capable of realizing safety functions that will eliminate unacceptable risks. The disaster that occurred in the Sayano Shushenskaya dam in Russia, on August 17, 2009, proved the accuracy of this idea. The disaster occurred as a result of an incorrect start-up process of the turbine and the governing system malfunctioning of the Sayano Shushenskaya dam unit. This failure was not detected by the control system. As a result of this, the system could not respond to the change required by the grid, which led to the over-speeding of the unit having de-loaded. 75 people died as a result of the incident and the entire power plant with 6400 MW was almost totally destroyed (Kuznetsov, Yuldashev, & Yuldashev, 2021; Leonov, Kuznetsov, & Solovyeva, 2015; Naymushin, 2009). This recent incident reveals the necessity of considering governing systems in hydroelectric plants as a safety critical system. It also shows that the reliability analysis of the interaction of speed governing system with the turbine generator system has critical importance and this analysis has to be included in the system design phase (Bulut & Özcan, 2021; Danciu, Popescu, & Rasvan, 2020). It is also a good example that shows the importance of doing reliability analysis by taking the interaction of speed governing system with the turbine generator system into account.

In a power system with high quality, frequency is required to be within an acceptable range. That is why speed control is conducted. Speed governing is a system where both the speed of the turbine generator system and that of electrical energy to be generated is controlled. As one can see from the Sayano Shushenskaya incident, any critical failure occurring in the speed governing system bears many crucial risks such as failure system being unable to stop the system in a safe way, over-speeding of the unit or not being able to synchronize with the grid. At least some part of the speed governing system, which plays a critical role in operating the hydroelectric power plants, should be evaluated from the perspective of safety related system. It should also be ensured that the relevant safety integrity level is at an acceptable level. This approach is of great importance for the sustainability of the system (Glavitsch, Reichert, Peneder, & Singh, 2003). Within this scope, this study was carried out the reliability analyses based on IEC 61362 and IEC 60308 standards so as to ensure the maintenance of operating hydroelectric power plants safely and efficiently by taking the digital speed regulator providing the speed, power and frequency control of the turbine generator system (IEC, 2005a, 2012). For this purpose, medium scale river type Midilli hydroelectric power plant (HEPP) has been examined such that

the Midilli HEPP has 32.548 MWe install capacity provided by 3 big units and 1 small unit. Here the big units have 10.485 MWe and the small one has 1.093 MWe install capacity. The Midilli HEPP has Francis type turbines and its annual power generation is 124 GWh.

The failure records of similar hydroelectric power plants have systematically been reviewed in order to analyse all possible failures and define the risk scores correctly. Besides, the failures that are likely to occur in the system, their possible causes, such as material losses in the event of failure occurrences, damage on the environment and personnel health have been also studied.

At this point, long meetings were held with the experts in the energy sector. The possible effects and frequencies of these determined failures were revealed and the safety functions that can eliminate these relevant risks have been proposed. Also, a safety related system that can realize the identified safety functions has been offered. Finally, the safety integrity level of the overall system has been calculated according to IEC 61511.

2. Materials And Methods Methodology

2.1. Safety Related Systems And Functional Safety

IEC 61508 expresses a safety related system as a "designated system used to implement the required safety related functions necessary to achieve or maintain a safe state for the equipment under control". According to this expression, safety related system is planned to accomplish the required safety functions which are dedicated to take the process to a safe state when outlined conditions are contravened. The safety related systems are composed of special design sensors, logic solver, and final elements. Here reducing risk to the tolerable level is the common aim of implemented safety related functions. On the other hand, to maintain a certain quality in the relevant sectors, independent organizations developed some standards. IEC 61508 is the international and leading standard that defines the functional safety for electrical, electronic and programmable electronic devices. It is also an umbrella document including various industries such that specific standards like IEC 62061 and IEC 61511 were introduced from this perspective (IEC, 2003, 2005b).

IEC 61508 put forth some safety parameters for the sake of reliability. The safety related systems were classified and compared over these defined parameters.

Failure rate: It is the frequency with which the system fails and denoted with λ. It is the rate of the failure density function (f(t)) that denotes the probability of the system's failure to the reliability function (R(t)) which means that the system can perform the identified functions. The failure rate is denoted by λ and modelled as provided in 2.1. It is usually expressed as failures per million hour (FPMH). Failure rate consists of two different types of failure such that these are safe failure and dangerous failure respectively. The ratio of the safe failure is defined with safety ratio (S). These can be seen in Equation 2.1 and 2.2. (IEC, 2010).

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{2.1}$$

$$\lambda = \lambda_S + \lambda_D \tag{2.1}$$

$$\lambda_S = S\ x\ \lambda \tag{2.2}$$

As provided in- Equation 2.3, a dangerous failure consists of two, which are dangerous detected failure (DD) and dangerous undetected failure (DU). In safety-related studies, it is accepted that the failure rate is constant within the use period of the system (Rausand, 2014).

$$\lambda_D = \lambda_{DD} + \lambda_{DD} \tag{2.3}$$

Safe failure fraction (SFF): Safe failure fraction is the percentage of the safe failures such that IEC 61508 expresses the calculation of it in IEC 61508-6 Annex C as Equation 2.4

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \quad (2.4)$$

Diagnostic coverage: Diagnostic coverage (DC) is a measurement as to what extent dangerous failures might occur in failure related systems. DC is defined as given in Equation 2.5 according to IEC 61508-4 section 3.8.6.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} \quad (2.5)$$

The values of this parameter differ a great deal in safety related systems such that while DC is 99% for fail-safe programmable logic controllers, the percentage varies for sensors and actuators. The DC level of the unit can be identified taking IEC 61508-6 Annex C table C.2 as the reference.

Probability of failure on demand: IEC 61608 expresses the system's likelihood of a failure during a time when safety related system is supposed to be working with probability of failure on demand (PFD). It is obvious that, the lower this value is, the safer the system is considered. Then average probability of failure on demand is defined as Equation 2.6

$$PFD_{avg} = \frac{1}{T}\int_0^T P(t)dt \quad (2.6)$$

Mean time to failure (MTTF): This is one of the common parameters used by the industry which is the statistical mean length of time a system or any other product last in operation till the first failure incidence. Products in safety related systems sector are generally compared based on their MTTF values given in Equation 2.7. For example, if a component's failure rate is equal to λ then its MTTF value is equal to 1/λ. The greater the MTBF value of a component, the less likely that component will fail per unit time.

$$MTTF = \int_0^T R(t)dt \quad (2.7)$$

Mean time to repair (MTTR): Another commonly used parameter in the industry is MTTR. This parameter expresses the required average time to repair a failed component or subsystem. If it is not mentioned by the vendor, the IEC 61508 recommends to take 8 hours as MTTR value.

Proof test interval (TI): It is the time that passes in between the main repairs to check whether the system or equipment accurately fulfil all its functionality or not (Rausand, 2014).

Common cause failures: This kind of failures are the interconnected failures of multiple subsystems that arise as a result of single specific event or cause. Although multiple methods are introduced in the literature, the β factor method, which was proposed by Fleming, is still commonly used (Fleming, 1975). It proposes a quantitative method to determine the corresponding values of β and β_D. Here β and β_D parameters define the overall common cause failure factor for undetected failures and the overall common cause failure factor for detected failures respectively.

Hardware fault tolerance (HFT): Hardware fault tolerance is the maximum number of failures that the subsystem or component can still continue to operate its intended function. The HFT is calculated according to Equation 2.8 (Rausand, 2014).

$$HFT_{sys} = \min_i HFT_i \quad (2.8)$$

2.2. Risk Analysis

Risk analysis is a process that occurs in analysis phase of the project management that includes gathering data and synthesizing information to develop an understanding of the risk of a particular system or subsystem. Within this scope, risk (R) is the combination of the frequency of the damage (F) and consequences of the damage (C). It is denoted as given in Equation 2.9 (IEC, 2006).

$$R = F\ x\ C \tag{2.9}$$

It would be possible to identify the risks in a realistic manner only when one can have thorough knowledge regarding the process. Failure records of many hydroelectric power plants with similar scale have been analysed in depth in this study so that the risks are analysed accurately. All the detected failures have been evaluated together with the experts in relevant sector. Besides, relevant standards have been taken as reference, results obtained have been compared with updated data numerous times and consistency of the results have been ensured accordingly.

2.3. Fault Tree Analysis

Fault tree analysis method is one of the most widely used reliability analysis methods. It is based on Boolean algebra, probability calculations and reliability theory such that the logical combination of unwanted situations are depicted graphically. IEC 61508-3 table B.4 and also IEC 61508-2 section 7.4.5.2 define that the method can be used both in software and hardware related failure analysis (IEC, 2006).

2.4. Safety Integrity Level Verification

The designed safety related functions must be verified according to the safety requirements. For this purpose, the standard takes into account Probability of Failure on Demand average (PFD_{avg}), probability of dangerous failure per hour, SFF and HFT measures in order to identify the safety performance of the safety related system. When the safety related function is active at low demand mode, PFD_{avg} is selected. On the other hand, probability of dangerous failure per hour is selected for high demand and continuous mode operations. IEC 61508-1 section 7.6.2.9 table 2 indicates a bounded probability interval for every safety integrity level (SIL) in case of low demand mode. Maximum allowable safety level that a system could achieve based on SFF and HFT is presented in IEC 61508-2 section 7.4.4.2.2 table 3 as well (IEC, 2010). In long discussions with experts in the sector and with reference to IEC 61508 Part 5 Annex B, it has been determined that the minimum safety integrity level of a governing system should be SIL 2.

3. Results and Discussion

3.1. Reliability Analysis Of Speed Governing System

Speed governing system functions in the synchronization of the turbine generator unit in the plant into the interconnected system. Thus, it ensures the transfer of the generated energy into the system and integrity of the grid system. Identifying the risks that could impact the performance of the governing system which plays a critical role within electrical energy generation process, and reducing the intolerable detected risks will significantly contribute to the correct functioning of the process.

For this study, the failure records of Suat Ugurlu, Hasan Ugurlu, Gezende, Berke, Midilli and Yavuz hydroelectric power plants located in Turkey have been examined. The risks that could delay the sustainability of frequency control cycle releasing at the digital speed governing system are determined in accordance with these detailed investigations. In this perspective, the frequency of failure occurrences, damages to be caused and technical analysis were evaluated with expert technical personnel. As a result of this intense collaborative work, the risk matrix has been formed concerning failures. In the matrix, the likehood of hazard is given under the frequency tab such that it is classified in five intervals as *very likely*, *likely, possible, unlikely and very unlikely*. Similarly, severity of the accident that will occur if the relevant danger is revealed is described under the consequence tab and it is classified in five levels, starting from *insignificant* to *catastrophic*. In addition, the risk scores are calculated according to Equation 2.9 such that these scores are classified in four main groups. The risks with a score in the range of 1..4 are considered *Low*, on the other hand the risks with a score in the range of 5..8 are considered *Moderate*, those with a score in the range of 9..15 are considered as *High*, and finally those with a score of 16 and above are classified as *Extreme*. While making this classification, the opinions of the sector experts were taken into consideration and a conservative approach was adopted during the classification phase. The corresponding risk matrix is given in Table 1.

Table 1.
Risk matrix

Frequency	**Consequence**				
	Insignificant (1)	*Minor (2)*	*Moderate (3)*	*Major (4)*	*Catastrophic (5)*
Very likely (5)	Moderate (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
Likely (4)	Low (4)	Moderate (8)	High (12)	Extreme (16)	Extreme (20)
Possible (3)	Low (3)	Moderate (6)	High (9)	High (12)	High (15)
Unlikely (2)	Low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)
Very Unlikely (1)	Low (1)	Low (2)	Low (3)	Low (4)	Moderate (5)

As mentioned before, the obtained technical data have been analysed by operation maintenance engineers, power generation process operators, experts and specialists who have been working in energy sector for many years. As a result of in-depth examinations, 26 major hazard scenarios have been identified but ten of them with a *high* and above risk score are listed in Table 2. Here the relevant hazards are enumerated and each hazard is briefly described. In addition, the frequency value and consequence of each hazard are also expressed. These values were intuitively generated as a result of field studies and were submitted to the approval of industry experts. In addition, the risk scores are calculated according to Equation 2.9

Table 2
The hazard scenarios and their risk scores

No	Hazard	Frequency		Consequence		Risk score	Risk
Hzd.01	Over speed	Likely	4	Catastrophic	5	20	Extreme
Hzd.02	Frequency cannot be balanced	Likely	4	Major	4	16	High
Hzd.03	Programmable logic controller failure	Possible	3	Major	4	12	High
Hzd.04	Main distribution valve failure	Possible	3	Major	4	12	High
Hzd.05	Step motor failure	Likely	4	Moderate	3	12	High
Hzd.06	Power supply failure	Possible	3	Major	4	12	High
Hzd.07	Disruption in grid frequency	Unlikely	2	Catastrophic	5	10	High
Hzd.08	Required water level can't be supplied	Possible	3	Moderate	3	9	High
Hzd.09	Servo motor failure	Possible	3	Moderate	3	9	High
Hzd.10	Pump works too loudly	Possible	3	Moderate	3	9	High

It is also be noted that risk analyses and evaluation may vary depending on time, working conditions and opinion of the experts who assess the subject matter. As some of the failures that are likely to emerge in the governing system could be due to hydraulic oil impact based on expert view, pressurized oil system has been accepted as the auxiliary system within the speed governing system, and included in the risk evaluation accordingly (Başeşme, 2003; Boardman, 1994; Cebeci, 2008; Naghizadeh et al., 2012).

Because of the scores given in Table 2, the safety function should be actuated against risks with extreme and high significance so that system can work in a safe mode in actual setting and practice. This study, however, presents the solution for the most critical ones. Besides, PFDavg, SFF and HFT values of safety related system are calculated and safety integrity level are identified.

The suggested speed governing safety system consists of fail-safe programmable logic controller, different type of sensors and actuators. It is clear that the exact failure rates of the subsystems are needed in order to calculate the SIL of the safety related functions precisely. For this reason, the corresponding reliability parameters of the fail-safe programmable logic controller have been acquired from its supplier. Also the failure rates of the other components are obtained from the suppliers and the OREDA handbook (OREDA, 2002). The failure rate values of these components are provided in Table 3.

Table 3.
The failure rate values of system components

Devices	λ (FPMH)	MTTF (h)	DC (%)	S (%)	MTTR (h)
Speed sensor	6.64	150517	75	50	8
Proximity sensor	5.24	190682	90	50	8
Pressure sensor	4,456	224405	75	50	8
Emergency Shutdown Valve	5.48	182287	70	50	8
Control valve	37,38	26747	75	50	8
Safety Relief Valve	7,01	142654	90	50	8
Fail-safe CPU	2,439	446627	99,63	50	8
Fail-safe Input Module	1,517	659195	99,31	50	8
Fail-safe Output Module	2,592	385802	99,24	36	8

Safety related function suggestion has been made for 3 critical situations that have the highest risk potential for speed governor. Relevant safety related function is as follows. The proposed safety related function is designed in order to realize imbalance at the frequency, over pressure and over speed protection functionalities. The proposed block diagram for the safety-related system suggested for safety related function is illustrated in Figure 1. The safety architectures of the components are also given. The safety function consists of inputs with 1oo2 and 2003 safety architectures, outputs with 1oo2 safety architecture and a fail-safe controller with 1oo2D safety architecture. Here all sensors, actuators and controller are designed with redundant architectures so that the system does not crash due to single failures. Three different types of sensors are used as inputs, including speed sensor (SS), proximity sensor (PRS) and pressure sensor (PS). The turbine speed and frequency data are measured by speed sensors. On the other hand, if the turbine speed exceeds the critical speed limit, the proximity sensors generate fail-safe outputs by opening normally closed contacts. The oil pressure in the pistons are measured pressure sensors.

The fail-safe controller consists of CPU module, input modules and output modules. CPU, input modules and output modules used in the system are equipment, which embody advanced technology, have diagnostic capabilities of 99.99% and work in accordance with the inherent 1oo2D architecture.

Emergency shutdown valve, safety relief valve and control valve have been integrated to the safety related system in order to safely stop the system in different risk scenarios. Each actuator is designed into the system in a redundant architecture, ensuring that the system is still safe in case of a single failure.

Over speeding of the turbine that is targeted to be prevented within safety related function scope is an undesirable critical scenario. For this purpose, an electronic proximity sensor system with a high level of safety obtained with 2oo3 safety architecture is used in order to be able to identify the over speeding of the unit. In the event of over speed, it is aimed that emergency shutdown valve is activated and deactivates the governing system safely. Also the high oil pressure in pistons that move main control valve cause a treat for speed governing system availability. Another aim of the safety related system is to deactivate the system safely in case of high oil pressure. The safety related function activates the safety relief valve in this situation. Finally, the imbalanced frequency poses serious risk over the governing system. Here the proposed safety related function cope within this risk and in the event of imbalanced frequency, the control valve is activated by safety related system.

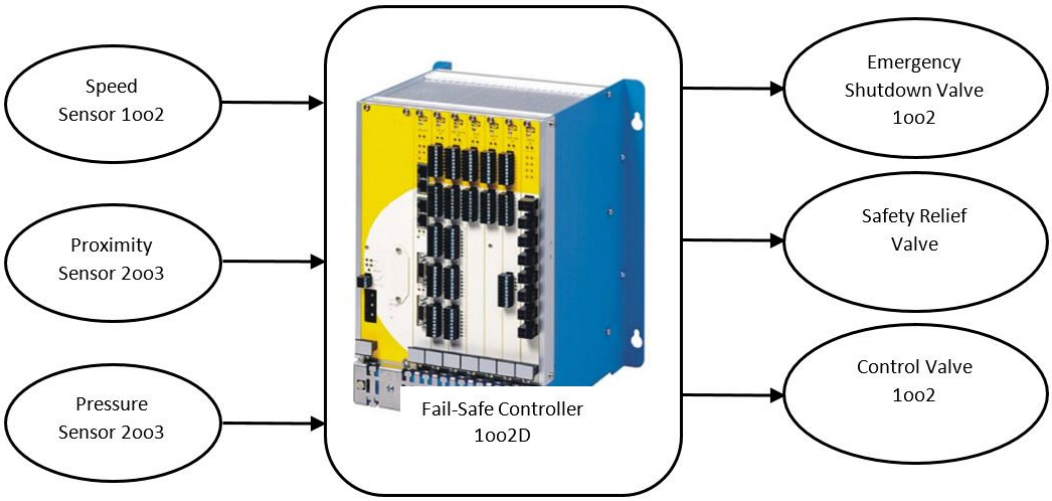


Figure 1 - The block diagram of the system

In order to calculate the safety integrity of the system, some non-conservative assumptions are made. There ones are as follows. The most of the components' periodic maintenance interval is 1 year. It is assumed that the proof test interval is 1 year and the testing is perfect. Failures regarding instalment and commissioning have been ignored. Similarly, it has been acknowledged that all the equipment, which has completed their useful life cycle, will be replaced by their equivalent counterpart. For this reason, failures that emerge during worn out phase have not been taken into account. The electrical connection and cabling failures have been ignored. The beta factor for common cause failure is calculated as 2% according to the IEC61508-6 annex D. The failure rates of all redundant components are assumed to be equal. It is supposed that the mean time to repair is 8 hours and the repair is perfect.

Some parts of possible failures can be easily detected by the help of relevant feedback obtained from speed sensor, pressure sensor, proximity sensor, safety relief valve, control valve and emergency shutdown valve elements. Diagnostic capability has been included in such elements through the control system used. In light of information obtained from the supplier, PFDavg calculation of the fail-safe controller has been made based on IEC 61508 annex B.3.2.2.4 as the reference. The fault tree analysis of the safety related function is given in Figure 2 .

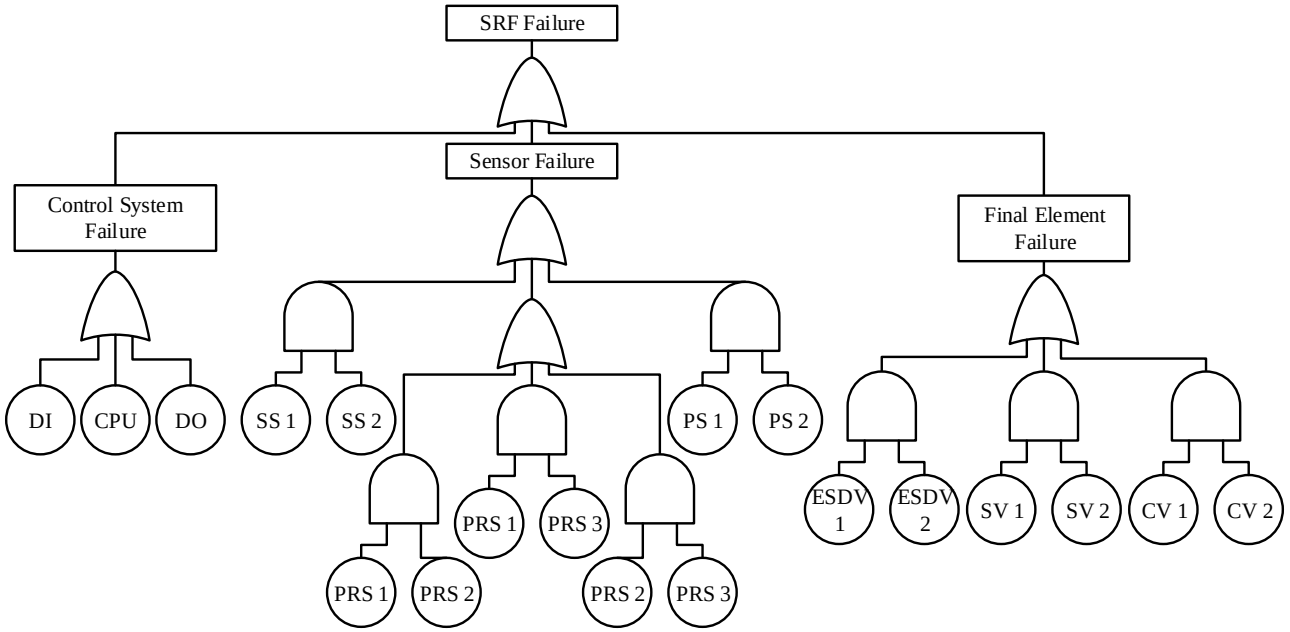


Figure 2. The FTA Analysis of the safety related function

Safety related function is assumed to fall into error upon demand when conditions defined below occur:

- Turbine speed and frequency data are perceived through speed and proximity sensors in the system. In case of a failure in sensors, speed data cannot be perceived, thus the frequency cannot be balanced. This leads the system to fall into error upon demand.
- The system has two ESDVs with 1oo2 architecture. Both of the ESDVs should fall into error so that the system gets into error.
- The system has two SRVs with 1oo2 architecture. If both of the SRVs should fall into error, the system gets into error.
- The system has two control valves with 1oo2 architecture. Both of the control valves should fall into error so that the system gets into error.
- If a common cause failure occurs at the subsystems with 1oo2 architecture, the system gets into error.

The corresponding failure rates of the devices and PFD_{avg} values calculated according to IEC 61508-6 annex B3.2.2 are given at Table 4. Considering the safety architectures, hardware fault tolerances are also listed separately.

Table 4.
PFDavg and HFT values of the subsystems

Devices	λ (FPMH)	PFD_{avg}	Architecture	HFT
Speed sensor	6.64	$9{,}06.10^{-5}$	1oo2	1
Proximity sensor	5.24	$2{,}86.10^{-5}$	2oo3	1
Pressure sensor	4,456	$5{,}69.10^{-5}$	1oo2	1
ESV	5.48	$8{,}95.10^{-5}$	1oo2	1
Control valve	37,38	$9.66.10^{-4}$	1oo2	1
SRV	7,01	$1{,}85.10^{-5}$	1oo2	1
Fail-safe CPU	2,439	$1{,}96.10^{-5}$	1oo2D	1
Fail-safe DI	1,517	$2{,}09.10^{-7}$	1oo2D	1
Fail-safe DO	2,592	$3{,}86.10^{-7}$	1oo2D	1

Based on Equation 2.8 and 2.4, it is obtained that a SFF of 98.60%. According to IEC 61508-2 section 7.4.4.2.2 Table 3, for 99% > SFF > 90% and HFT=1 the maximum allowable SIL that the system could have is 3. Given that PFD_{avg}=1,27.10^{-3} for the relevant safety related function 1, within 10^{-3} and 10^{-2} range, the safety level of safety related function is SIL 2 according to IEC 61508-1 section 7.6.2.9 Table 2.

This value is the minimum required safety level that should be possessed by the safety side of the governing system. Accordingly, it is seen that the proposed safety system ensures the required minimum safety level.

It must be stated that the risk reduction factor (RRF) is the inverse of PFD_{avg} according to IEC 61508 and IEC 61511. Then if a system is SIL 2 then its PFD_{avg} have to be between within 10^{-3} and 10^{-2} range so the risk reduction factor varies between 100 and 1000. For the proposed safety related system, as the PFD_{avg} value is equal to 1,27.10^{-3} then the risk reduction value is approximately 787. In other words, the risk was reduced by an average of 787 times.

In a qualified and reliable power system, it is desirable that the output frequency of the system be constant in an acceptable range. For this purpose, speed control is performed in hydroelectric power plants. Both the speed of the turbine generator system and the power of the electrical energy to be produced are controlled with the speed governor system. On the other hand, any malfunction in the speed governor system may cause the unit to go over speed or break down. As a result, it can cause many accidents, from not being able to synchronize with the network, to serious damage to the power plant.

At this point, the reliability of this critical system, which plays a role in the operation of hydroelectric power plants, is of great importance for the sustainability of the overall system.

With this motivation, in this study, the reliability of digital speed governor systems in river-type hydroelectric power plants was examined according to IEC 61511 and IEC 61508 standards. The "Over Speed" failure, which can be considered as the most critical hazard for speed governor systems, has been examined and a safety function that increases the safety integrity level is proposed. Different safety architectures such as 1oo2, 1oo2D and 2oo3 were used for the sensors, actuators and controller side, as a result, a fail-safe solution was proposed. With this solution, the hardware fault tolerance of the system was increased to 1, and the average probability of failure on demand was reduced by an average of 79 times. As a result, it is calculated that the solution has SIL 2 safety integrity level.

In this study, a safety function that increases the safety reliability level is proposed for the "Over Speed" error, which can be considered as the most critical error for regulator systems. As can be observed from Table 4, a safe solution to the fault has been proposed by using different safety architectures such as 1oo2, 1oo2D and 2oo3. With this solution, the tolerance of the system to error was increased to 1, and the average error probability during the demand was reduced by an average of 787 times. As a result, the solution was calculated to have a SIL 2 safety integrity level.

Thus, as a result of possible risks, the possibility of a safe stop of the system increases significantly and the useful life of the facility is guaranteed to be longer.

4. Conclusion

In this study, the incidents leading to the failure of turbine speed governing system has been examined and a new safety related system architecture has been proposed for the critical scenarios based on IEC 61508 perspective. For this purpose, the failure records of Suat Ugurlu, Hasan Ugurlu, Gezende, Berke, Midilli and Yavuz hydroelectric power plants located in Turkey have been examined and the obtained data have been evaluated by experts and specialists who have been working in energy sector for many years and risk scores were determined with the support of relevant experts. It is revealed that the governing system incorporates unacceptable risks and the safety integrity level of the currently used control systems does not cover the desired safety level. Neither the corresponding international standards nor the local technical specifications express the safety of the speed governing systems within the scope of functional safety. So in order to overcome these unacceptable risks and define a new perspective for the safety of the governing systems, an innovative safety related system suggestion has been made based on IEC 61508. The proposed speed governing safety system has been designed with reference to the Midilli hydroelectric power plant in Amasya. It should also be stated that the proposed can be used in other hydroelectric power plants with minor modifications if the technical specifications meet the plant requirements.

It is also proofed that the safety integrity level of the proposed system is SIL 2, which is the minimum level of safety demanded by the sectorial experts. As a result, the risk reduction factor of the prosed speed governing system reduces the risk at least 100 times.

Acknowledgement

The author received no specific funding for this study.

Author Contributions

Özgür Turay Kaymakçı: Validated the analysis, wrote the manuscript

Nezihe Merve Balcı: Collected data, performed reliability analysis, wrote the manuscript

Conflicts of Interest

The authors declare no conflict of interest.

References

Başeşme, H. (2003). *Hidroelektrik Santraller ve Hidroelektrik Santral Tesisleri* (2. Baskı ed.). Ankara: Hidrolik Santraller Daire Başkanlığı Yayınları. https://divit.library.itu.edu.tr/record=b1147743

Billinton, R., & Wang, P. (1999). Teaching distribution system reliability evaluation using Monte Carlo simulation. *IEEE Transactions on Power Systems, 14*(2), 397-403. doi: https://doi.org/10.1109/59.761856

Boardman, J. R. (1994). Operating experience feedback report - reliability of safety-related steam turbine-driven standby pumps: US Nuclear Regulatory Commission. 27005885.pdf (iaea.org)

Brennan, R. L. (2001). An Essay on the History and Future of Reliability from the Perspective of Replications. *Journal of Educational Measurement, 38*(4), 295-317. doi: https://doi.org/10.1111/j.1745-3984.2001.tb01129.x

Brown, R. E., Gupta, S., Christie, R. D., Venkata, S. S., & Fletcher, R. (1996). Distribution system reliability assessment using hierarchical Markov modeling. *IEEE Transactions on Power Delivery, 11*(4), 1929-1934. doi: https://doi.org/10.1109/61.544278

Bulut, M., & Özcan, E. (2021). A new approach to determine maintenance periods of the most critical hydroelectric power plant equipment. *Reliability Engineering & System Safety, 205*, 107238. doi: https://doi.org/10.1016/j.ress.2020.107238

Cebeci, M. E. (2008). *The effects of hydro power plants' governor settings on the turkish power system frequency.* (M.S. - Master of Science), Middle East Technical University, Ankara. Ulusal Tez Merkezi | Anasayfa (yok.gov.tr)

Chowdhury, A. A., Bertling, L., Glover, B. P., & Haringa, G. E. (2006). *A Monte Carlo Simulation Model for Multi-Area Generation Reliability Evaluation.* Paper presented at the 2006 International Conference on Probabilistic Methods Applied to Power Systems. doi: 10.1109/PMAPS.2006.360430

Danciu, D., Popescu, D., & Rasvan, V. (2020, 2020-10-27). *Stability and Control Problems in Hydropower Plants.* Paper presented at the 2020 21th International Carpathian Control Conference (ICCC). doi: https://doi.org/10.1109/ICCC49264.2020.9257294.

Fleming, K. N. (1975). A reliability model for common mode failures in redundant safety systems. San Diego, California, USA: General Atomic Co. https://inis.iaea.org/search/search.aspx?search-option=everywhere&orig_q=RN%3A6204768

Glavitsch, H., Reichert, K., Peneder, F., & Singh, N. (2003). Power System Operation and Control *Electrical Engineer's Reference Book* (pp. 40-41-40-50): Elsevier. doi: 10.1016/B978-075064637-6/50040-X:

Gubbala, N., & Singh, C. (1995). Models and considerations for parallel implementation of Monte Carlo simulation methods for power system reliability evaluation. *IEEE Transactions on Power Systems, 10*(2), 779-787. doi: https://doi.org/10.1109/59.387917

IEC. (2003). IEC 61511 - Functional Safety - Instrumented Systems for the Process Industry Sector, Parts 1-3. Genoa, Switzerland: International Electrical Commission. https://webstore.iec.ch/publication/5527

IEC. (2005a). IEC 60308 - Hydraulic turbines testing of control systems. Genoa, Switzerland: International Electrical Commission. https://webstore.iec.ch/publication/1312

IEC. (2005b). IEC 62061 - Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems. Genoa, Switzerland: International Electrical Commission. https://webstore.iec.ch/publication/59927

IEC. (2006). IEC 61025 - Fault tree analysis (Second Edition ed.). Genoa, Switzerland: International Electrical Commission. https://webstore.iec.ch/publication/4311

IEC. (2010). IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems. Genoa, Switzerland: International Electrical Commission. https://webstore.iec.ch/publication/5515

IEC. (2011). IEC 61513 - Nuclear power plants-Instrumentation and control important to safety-general requirements for systems. Genoa, Switzerland: International Electrical Commission. https://webstore.iec.ch/publication/5532

IEC. (2012). IEC 61362 - Guide to specification of hydraulic turbine control systems. Genoa, Switzerland: International Electrical Commission. https://webstore.iec.ch/publication/5383

IEEE. (2007). Recommended practice for preparation of equipment specifications for speed-governing of hydraulic turbines, intended to drive electric generators. New York, USA: Institute of Electrical and Electronics Engineer. https://standards.ieee.org/ieee/125/3394/

IEEE. (2011). Guide for the application of turbine governing systems for hydroelectric generating units. New York, USA: American National Standards Institute. https://ieeexplore.ieee.org/document/6042284

Khosravi, F., Azli, N. A., & Babaei, E. (2010, 11/2010). *A new modeling method for reliability evaluation of Thermal Power Plants.* Paper presented at the 2010 IEEE International Conference on Power and Energy (PECon). doi: 10.1109/PECON.2010.5697644

Kilic, L., & Basa Arsoy, A. (2013, 10/2013). *A reliability study of medium voltage grid with private sector power plants.* Paper presented at the 2013 3rd International Conference on Electric Power and Energy Conversion Systems (EPECS). doi: 10.1109/EPECS.2013.6713045

Kuznetsov, N. V., Yuldashev, M. V., & Yuldashev, R. V. (2021). Analytical-numerical analysis of closed-form dynamic model of Sayano-Shushenskaya hydropower plant: stability, oscillations, and accident. *Communications in Nonlinear Science and Numerical Simulation, 93*, 105530. doi: https://doi.org/10.1016/j.cnsns.2020.105530

Leonov, G. A., Kuznetsov, N. V., & Solovyeva, E. P. (2015). A simple dynamical model of hydropower plant: stability and oscillations. *IFAC-PapersOnLine, 48*(11), 656-661. doi: https://doi.org/10.1016/j.ifacol.2015.09.262

Naghizadeh, R. A., Jazebi, S., & Vahidi, B. (2012). Modeling hydro power plants and tuning hydro governors as an educational guideline. *International Review on Modelling and Simulations (I.RE.MO.S.), 5*(4), 1780-1790. https://www.researchgate.net/publication/235675537_Modeling_Hydro_Power_Plants_and_Tuning_Hydro_Governors_as_an_Educational_Guideline

Nalley, S., & LaRose, A. (2021). International Energy Outlook. In S. Nalley & A. LaRose (Eds.): U.S. Energy Information Administration. International Energy Outlook 2021 - U.S. Energy Information Administration (EIA)

Naymushin, I. (2009, 17 August 2009). Russian dam disaster kills 10, scores missing, https://www.reuters.com/article/worldNews/idUSTRE57G0M120090817?sp=true

OREDA. (2002). *OREDA: Offshore Reliability Data Handbook*. Norway: OREDA Participants : Distributed by Der Norske Veritas. https://www.oreda.com/

Pan, W., Zhu, Z., Liu, T., Liu, M., & Tian, W. (2021). Optimal Control for Speed Governing System of On-Grid Adjustable-Speed Pumped Storage Unit Aimed at Transient Performance Improvement. *IEEE Access, 9*, 40445-40457. doi: https://doi.org/10.1109/ACCESS.2021.3063434

Perman, M., Senegacnik, A., & Tuma, M. (1997). Semi-Markov models with an application to power-plant reliability analysis. *IEEE Transactions on Reliability, 46*(4), 526-532. doi: https://doi.org/10.1109/24.693787

Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and Applications*. Hoboken, NJ, USA: John Wiley & Sons, Inc. Reliability of Safety-Critical Systems: Theory and Applications | Wiley

Tripathi, M., Singh, L. K., Singh, S., & Singh, P. (2021). A Comparative Study on Reliability Analysis Methods for Safety Critical Systems Using Petri-Nets and Dynamic Flowgraph Methodology: A Case Study of Nuclear Power Plant. *IEEE Transactions on Reliability*, 1-15. doi: https://doi.org/10.1109/TR.2021.3109059

Wang, C., Wang, D., & Zhang, J. (2021). Experimental study on isolated operation of hydro-turbine governing system of Lunzua hydropower station in Zambia. *Renewable Energy, 180*, 1237-1247. doi: https://doi.org/10.1016/j.renene.2021.09.014

Wang, L., Sun, W., Zhao, J., & Liu, D. (2019). A Speed-Governing System Model with Over-Frequency Protection for Nuclear Power Generating Units. *Energies, 13*(1), 173. doi: https://doi.org/10.3390/en13010173

Yu, Y., Tong, J., Zhao, R., & Zhang, A. (2009, 07/2009). *Reliability analysis for continuous operation system in nuclear power plant.* Paper presented at the 2009 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009). doi: 10.1109/ICRMS.2009.5270214

Zhang, Y., Chowdhury, A. A., & Koval, D. O. (2010, 05/2010). *Probabilistic wind energy modeling in electric generation system reliability assessment.* Paper presented at the 2010 IEEE Industrial and Commercial Power Systems Technical Conference - Conference Record. doi: 10.1109/IREP.2010.5563301

Zhu, L., Si, P., Liu, S., Xie, C., Zhang, T., Hu, Y., & Qiu, X. (2021). The Design of Parameter Modeling Software Applicable for Turbine Control Systems of Power Units Operated at Deep Shaving States. *Journal of Physics: Conference Series, 2076*(1), 012106. doi: https://doi.org/10.1088/1742-6596/2076/1/012106

Zio, E. (2013). *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*. London: Springer London. The Monte Carlo Simulation Method for System Reliability and Risk Analysis | SpringerLink