ISSN 1691-5402
Environment. Technology. Resources
Proceedings of the 9th International Scientific and Practical Conference. Volume 1I

Functional Safety of Power Plant's Technological Protections

Sergey Trashchenkov
Pskov State University, electromechanical faculty, Chair of Electric Power Industry.
Address: Lenin square 2, Pskov, Russian Federation.

***Abstract*. Functional safety is an important component of safety in general, has received increasing attention in the petroleum and chemical industry, railway and other industries which used a complicated process, in case of failure can cause major damage and loss of life. Electric engineering is also among these industries. But quantitative analysis shows that the equipment of power plants does not satisfy stringent requirements of functional safety.**

***Key words*: functional safety, safety related systems, technological protections.**

I Introduction

In the history of electric power can distinguish the individual stages of development, related to specific scientific and technological advances (the invention of the generator, the creation of a three-phase systems, nuclear energy, etc.). It is now one of the most actual areas of the industry is the introduction of power plants and substations digital multifunction systems automation technologies that could improve the efficiency of the plants and networks. But the application of such systems is possible only under strict safety requirements. It is considered from the standpoint of security the focus of this review of modern automation systems for the power industry.

II Materials and methods

The concept of security is extremely extensive. For complex continuous process using more specialized concept of functional safety (FS). FS is a part of an overall security, expressed in the absence of unacceptable risk to human health, their property, the environment from the functioning of the system. FS is provided by the so-called safety-related systems - systems that perform one or more specialized functions, to prevent the onset of dangerous failures. A dangerous failure meant crossing the equipment inoperable by an unpredictable or undesirable scenario. At power security systems are primarily technological protection.

Safety-related systems are interconnected by communication channels sensors that take readings of critical parameters, controllers that analyze the parameters and give commands, final elements that implement the controller's commands.

Initially, when the security-related systems were built on electromechanical relays, hardware protection functions were not associated with the functions of control. At present due to the development of automation systems safety functions are increasingly being integrated into a single framework automation, which, along with the safety function also performs:

- process control - local (actions performed by the controller without a command from the outside) and remote (commands come from the remote supervisory control);
- measurement - the collection and processing of sensor readings in real time;
- monitoring - recording of emergency processes and analysis of the current state;
- communication - the transfer of information between the field level and supervisory system, between the protection and monitoring for subsequent evaluation of emergency events.

The safety functionin spite of the integration at the hardware and software levels, continues to be an isolateds, locals, because of its independent actions depend lives and health of personnel, damage to equipment during the failure. Other automatic functions should not affect the effectiveness of safety functions.

There are few tens of technological protections in thermal power plants (a specific amount depends on the schema and power of thermotechnical equipment). Traditionally, protections are divided into two groups - that trigger when exist danger for life of personnel and safety of equipment (group A) and trigger when exist danger for equipment damage or a reduction in its resource (group B). Below, for example, here is a list of boiler and turbine units protections group A for a drum boiler:

- extinction of the flame in the firebox;
- lowering the gas pressure after regulating valve;
- disable all smoke exhausts;
- disable all blasting ventilators;
- lowering the pressure in the lubrication system;
- increasing vibration bearing housings;
- lowering of the level in the damper oil tank;
- increase the pressure drop in the last stage pressure turbine;
- increasing the level of high pressure heater to the 2nd limit.

As described above, any power TK as a security system is analog and digital sensor data, thermocouples, thermistors, followed by communication with the input device (CPI) providing a normalization signal preprocessing, the conversion of analog to digital values and their transfer to the controller. Modern programmable controllers perform many functions, logic operations, signal processing, control actuators, control, execution of commands from the user, etc. The controller provides signals to the final elements . The final elements of safety-related system on the block power plants with a drum boiler include:

- fuel supply device;
- ignition device;
- shut-off devices;
- valves;
- regulators;
- electric pumps.

General scheme of the security channel is shown on Fig. 1.

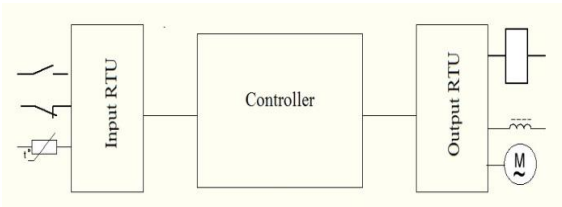

Fig. 1. Schematic diagram of the channel security system

To ensure safe and reliable safety-related systems use different architecture of this scheme, characterized by the redundancy. General architectures redundancy symbol is MooN, an M out of N. N - total number of redundant elements, M - the number of elements required to maintain the system in good working condition. Reserve are primarily controllers as the most critical elements of the systems that perform several functions, sensors to provide a system of reliable data, much less reserve final elements. According to the standard 61508 MooN concept applies to the channel - a full set of sensors, the controller and the final elements independently realizing safety function . Work if one of the channels is allowed only at the time of finding the cause and repair (18 hours).

There are several types of architectures:

- 1oo1 - the simplest not redundant architecture. Single failure results in failure of the entire system.
- 1oo2 - «one out of two». To perform the function of protection is sufficient to obtain a command from a single channel. In the event of failure of one of the channels, the work carried out on single-channel scheme, in 1oo1.
- 2oo2 - «two out of two». Circuit performs an operation to protect only when a command is received in two channels. Failure of one of the channels leading to the inability to carry out a protective function.
- 2oo3 - «two out of three» or majoritarian scheme. Made the implementation of thesafety function when receiving commands from any two channels. The failure of two or three channels leads to unhealthy state of the system.

In addition to these common architectures modifications MooND, which are distinguished by the presence of special diagnostic modules that increase the safety of the protection systems.

In real technological protection schemes are often used combinations of architectures. Sensors are built on a "two out of three", controllers - "one of the two", and is located directly in the work of a single controller, and the second is in hot standby, and the only one final element (Figure 2). To assess the safety of the combined architecture needs to be assessed individually set of input sensors and communication devices, controllers, input and output remote terminal unit (RTU).

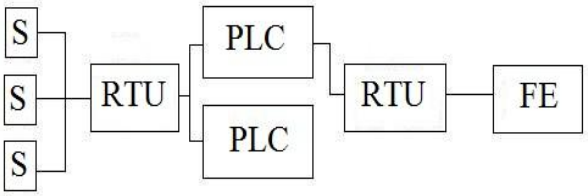

Fig. 2. The combined safety architecture

Such scheme is used in protection "increasing the level of high pressure heater to the 2nd limit", for example. Below is quantify assessment of functional safety for Fig. 2.

The main quantitative assessment of functional safety is the probability of failure on demand (PFD). It is probability of failure of the safety function when function should be triggered. The refusal of a failure is called a dangerous failure. The intensity of a dangerous failure is indicated λ_D. In contrast, there is a false alarm of a failure, called the safe failure, indicated λ_S. Dangerous and safe failures are divided into detectable internal diagnostics (λ_{DD} and λ_{SD}) and undetectable (λ_{DU} и λ_{SU}). Failures are divided into individual failures and common cause failures when the failure is more than one channel. Share of common cause failures is small, but it must be taken into account in the safety assessment, as the consequences of such failures are greatest. The shares of common cause failures are indicated β_D for detected and β_U for undetected.

Failure rate should be multiplied to their respective time intervals to find a probability.

These time intervals are:

- T – proof test interval;
- t – the time of appearance of undetectable failure in the system; equals t_{CE} –the average time a link failure;
- MTTR – Mean Time To Recovery;
- $t_{DU} = \frac{T}{2} + MTTR$ – time of undetectable dangerous failure;

- $t_{DD} = MTTR$ – time of dangerous detected failure;
- t_{GE} – average time of failure of all system.

Intervals are presented graphically in Figure 3.

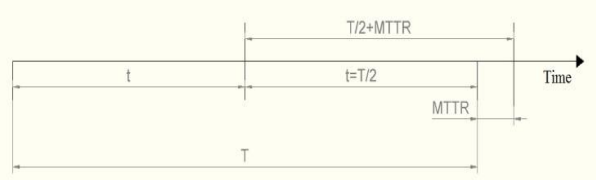

Figure 3. Graphical representation of appearance and detecting failures processes

The time t is assumed to be T/2 is taken as a uniform distribution of failure over time.

We define the rate for PFD sensor subsystem having architecture 2oo3.

$$PFD_s = 6[(1-\beta_D)*\lambda_{DD} + (1-\beta_U)*\lambda_{DU}]^2 * t_{CE} * tGE + \beta D * \lambda DD * MTTR + \beta U * \lambda DU * T2 + MTTR \quad (1)$$

The expression $(1-\beta_D)*\lambda_{DD} + (1-\beta_U)*\lambda_{DU}$ in this formula is nothing else but the failure rate of a dangerous failure λ_D. Coefficient 6 is a result of taking into account the three channels and that the time T more time t_{CE} twice. The values of the time intervals t_{CE} and t_{GE} determined by the expressions:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} * \left(\frac{T}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} * MTTR \quad (2)$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} * \left(\frac{T}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} * MTTR \quad (3)$$

Time of dangerous undetectable failure of the entire system in the last formula is accepted T/3 +MTTR, because the appearance of two faults during the proof test interval are also uniform, that is occurring every third proof test interval.

The probability of failure on demand for logic controller with architecture 1oo2 PFD_L is given by:

$$PFD_L = 2[(1-\beta_U)*\lambda_{DU}]^2 * t_{CE} * t_{GE} + \beta_D * \lambda_{DD} * MTTR + \beta_U * \lambda_{DU} * (\frac{T}{2} + MTTR) \quad (4)$$

Values t_{CE} and t_{GE} for 1oo2 architecture are defined as well as for 2oo3.

For the subsystem of final elements, which has architecture 1oo1, PFD_{FE} is:

$$PFD_{FE} = (\lambda_{DD} + \lambda_{DU}) * t_{CE} \quad (5)$$

Failure of channel in this case is the failure of a subsystem itself and therefore takes into account only the time t_{CE}.

III Results and Discussion

As an example, we take the controller TSXP572634M Shneider Electric. Its failure rate, as declared by the manufacturer is about 1.4 * 10^{-6} 1/hour. For convenience, it is assumed that $\lambda_D=\lambda_S=\lambda/2$. The ratio of λ_{DD} and λ_{DU} determined by the diagnostic coverage:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D} \quad (6)$$

Typically, DC takes 0%, 60%, 90%, 99%. For this calculation, we assume diagnostic coverage as 90%. Then $\lambda_{DD}=0{,}9\lambda_D=(0{,}9*\ \lambda)/2=0{,}63*10^{-6}$ 1/hour. For undetected failures $\lambda_{DU}=0{,}07*10^{-6}$ 1/hour.

Shares of detected and undetected common cause failures β_D=1% and β_U=2%.

$$PFD_L = 2[(1-0{,}02)*0{,}07*10^{-6}]^2 * 456 * 310 + 0{,}01 * 0{,}63 * 10^{-6} * 18 + 0{,}02 * 0{,}07 * 10^{-6} * \left(\frac{8760}{2} + 18\right) = 88{,}08 * 10^{-6} \quad (7)$$

$$t_{CE} = \frac{0{,}07*10^{-6}}{0{,}7*10^{-6}} * \left(\frac{8760}{2} + 18\right) + \frac{0{,}63*10^{-6}}{0{,}7*10^{-6}} * 18 = 456\ hours \quad (8)$$

$$t_{GE} = \frac{0{,}07*10^{-6}}{0{,}7*10^{-6}} * \left(\frac{8760}{3} + 18\right) + \frac{0{,}63*10^{-6}}{0{,}7*10^{-6}} * 18 = 310\ hours \quad (10)$$

As an final element of technological protection choose the main steam valve. It is known that its time between failures (MTBF) is approximately 5000 hours, then the failure rate λ = 0,002 1/hr. The values of DC, βD, βU accept the same as for the controllers respectively time t_{CE} will remain the same, λ_{DD}= 0,0009 1/hour, λ_{DU}=0,0001 1/hour.

$$PFD_{FE} = (0{,}0009 + 0{,}0001) * 456 = 0{,}456 \quad (11)$$

Using the same values of DC, β_D, β_U for subsystems of sensors count the safety of architecture 2oo3. The sensors pick differential pressure gauges DM-3583M. The failure rate for these devices will take 0.35 * 10-6 1/hour. Obtain that λ_{DD} = 0,1575*10^{-6} 1/hour, a λ_{DU} = 0,035*10^{-6} 1/hour.

$$PFD_s = 6[(1-0{,}01)*0{,}1575*10^{-6} + 1-0{,}02*0{,}035*10-6]2*456*310+0{,}01*0{,}1575*10-6*18+0{,}02*0{,}035*10-6*87602+18=5{,}447\ *10^{-6} \quad (12)$$

Thus, the resulting safety indicator is the sum of the three components.

$$PFD = PFD_s + PFD_L + PFD_{FE} = 0{,}45 \quad (13)$$

IV Conclusion

The probability of failure on demand of sensors and controllers are insignificant compared to the PFD_{FE}. It turns out that the final element is the weakest point in the consideration of technological protection. The resulting figure PFD does not meet modern safety

requirements for safety systems of complex processes (PFD= 0,001..0,0001).

Technological protection usually gives commands to multiple final elements that perform different functions of safe shutdown of the process are not duplicating each other. Therefore, despite the active attention to digital automation equipment, a translation of all systems on the microcontroller to provide safety management will not be succeed.

V ACKNOWLEDGMENTS

This study was partly supported by JSC Pskov Power Plant.

VI REFERENCES

[1] IEC 61508-4:2010 Functional safety of electrical/ electronic/programmable electronic safety related systems. Part 4: Definitions and abbreviations.

[2] IEC 61508-6:2010 Functional safety of electrical/ electronic/programmable electronic safety related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.

[3] Fedorov Y. *Handbook for ICS Engineer: Design and Development*. Moscow: Infra-ingeneria, 2008.

[4] Strauss C. Practical Electrical Network Automation and Communication Systems. Milpitas, CA: IDC Technology, 2004.