

Functional Safety in Electric Power Industry Sector

Zdzisław Żurkowski

Institute of Power Systems Automation, Poland

zurako@isat.iase.wroc.pl

Abstract. Application of the standard IEC 61508 in any particular sector of industry raises two important issues specific for the sector. First issue it is full understanding the consequences in the event of failure of the safety-related systems applied in the sector. The second, it is determination of Safety Integrity Level for safety-related functions. This paper presents, the main types of hazards for personnel, equipment and electric power systems which should be taken into consideration in the design of computer-based systems. An emphasis is put on description of the hazard for safety of an electric power system, whose nature is fundamentally different from the nature of those occurring in the process industry and in all other sectors of industry. To illustrate the problems with hazards and risks identification and with the IEC 61508 standard application in electric power sector, the power substation software interlocking case study is described. The case study description is preceded by a short presentation of the results of an extensive review of available publications with the aim of identifying the current state of practice in assuring functional safety of computer systems applied in the sector.

1. INTRODUCTION

Safety as a crucial issue of computer applications in such fields as nuclear power stations, space industry, aircraft industry, chemical industry or railways is well recognized by wide circles of specialists of these fields as well as by specialists in software engineering and computer science.

Safety issues associated with computer system applications in electric power systems are considered very rarely during conferences. The same refers to professional journals, books and any other publications concerning this problem. One can get a wrong impression that functional safety of computer systems in this field is not important.

In fact, applications of computer-based systems in the conventional electric power sector (excluding nuclear power plants), are not regarded by a wide group of IT experts which are not involved with electric power sector by profession, as related to safety applications. The only opinions which author met are that these applications are related to reliability. But even when considering the reliability requirements, the applications of computers are not considered to be critical from a reliability point of view because in case of failure, as it is claimed, it is easy to provide additional, reserve power supplies due to a quite high degree of redundancy existing in power grids. The reality however is much more complex than this feeling at first sight might suggest.

Contemporary electric power systems (EPSs) are very complex and highly technologically advanced systems, which seems to be sometimes underestimated by those persons who are not engaged in the electric power sector. The vast, highly interconnected North American electric power system has been called the „greatest machine ever created”. Similarly one could say about contemporary electric power systems of other countries.

The aim of this paper is to present safety issues in designing of computer-based control systems for EPSs, which towards the end of this century emerged as the most critical national infrastructure in the sense that all other national critical and vital infrastructures depend on reliable electricity supply. At the same time application of computer-based systems in this sector offers researchers and practitioners a wide range of issues, which are both basic for the future of the sector and very interesting and challenging. Due to space limitation in the paper

only basic concepts and pieces of information are given. The paper consists of five parts. First, the physical and organisational structure of the electric power systems is briefly presented. Next examples of hazards for people and equipments in power stations and substations are given and the safety concept with reference to an electric power system is described. Then the power substation case study carried out in the frame of the EU Joint Research Project „Integration of Safety Analysis Techniques for Process Control Systems” (ISAT) is described and problems with functional safety analysis and with the application of the standard IEC 61508, which appeared in realization of the case study, are discussed. The case study description is preceded by a short presentation of results of extensive review of available publications with the aim to identify current state of practice in assuring functional safety of computer systems applied in electric power sector. At the end conclusions are given.

2. STRUCTURE OF ELECTRIC POWER SYSTEMS

The electric power industry in each country consists of many different companies involved in generating of electric power, bulk transmission of energy from power stations to loading centres and its distribution to customers. In order to perform their functions and to attain suitable effectiveness, all power stations, substations, power lines forming power grids, the related control centres and other components are interconnected, although they belong to various companies, forming an electric power system (EPS). Usually this interconnection is now the strongest at the national level, forming a national power system. However an increasing tendency can be observed, for example in Europe, aiming to build up more and more stronger connections between the separate EPS-s existing in the individual countries. Energy related policy of the European Union aims at building Trans-European networks in order to provide a sound basis for free and competitive electricity market in Europe and strengthening security of energy supply.

In the most general terms an EPS can be partitioned into generating stations and high-voltage power networks known as grids. Power networks consist of transmission networks, called extra-high voltage (EHV) networks, which are used to transmit power from generating stations to main load centres and distribution networks of lower voltages, also known as high-voltage (HV) networks, which are used to transmit power to customers. Both, transmission and distribution networks consist of power lines, substations and control centres.

Substations form vital nodes in the HV and EHV networks because they make possible modifications in the configuration of networks during the operation of the system by means of switching devices that can be controlled by computer-based control systems applied in the substations. Initiation of the control procedure may be performed locally by substation operators or remotely from the EPS control centres. They also are the points in which power is leaded out of the generation stations and supplied to the consumers.

The power network of generation, transmission and distribution subsystems forming an EPS is coupled with telecommunication and telecontrol systems that are used for communication and transmission of data between power generating stations, substations and control centres for remote operation and remote real-time signalling, metering, control and fault protection. Development of these EPS communication systems goes toward an integrated EPS telecommunication network. In the last decade due to the process of computerisation of the EPS-s the data network is used on increasingly larger scale for transmitting the data that are critical to safe and reliable operation of an EPS and for the power grid - related financial transactions.

To illustrate the degree of complexity imposed on a data network in EPS by the physical and organisational structure one can state that in the Polish EPS, being a middle – sized system, the transmission network includes 106 extra-high voltage substations (220 kV and

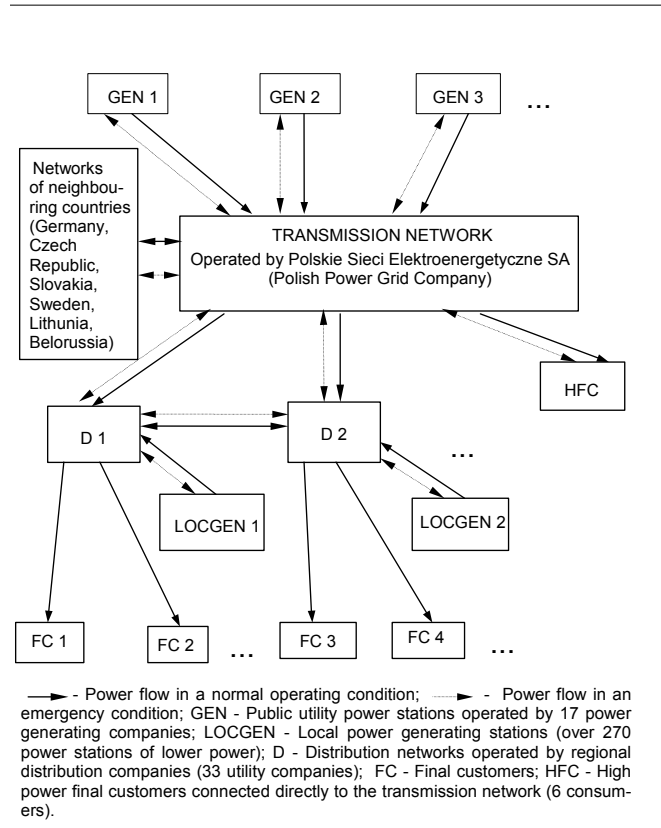


Fig. 1 Approximate block diagram of the Polish electric power system

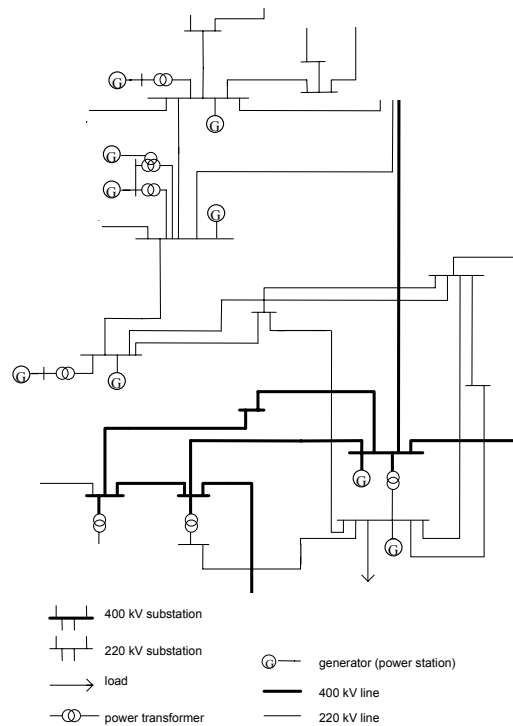


Fig. 2. A part of the transmission network of the Polish electric power system

above). Within the distribution network there are 1264 substations 110 kV and thousands substations of lower voltages. Majority substations in the transmission network and the most important substations of 110 kV are equipped with computer-based control systems or at least with equipment that allows for remote control. There are six control centres to operate the electric power system in the transmission network and several dozens local control centres in the distribution networks. Seventeenth power-generating companies operate power stations which are connected to national transmission system. At present in Poland there are no unmanned substations in transmission network. However in other countries many of these substations are already unmanned and fully remotely controlled from control centres through the data network. The control centres can also adjust the output power of power stations connected to the transmission network.

Approximate block diagram of the Polish EPS is shown in Figure 1. A simplified diagram of a small fragment of the transmission network of the Polish EPS is presented in Figure 2 (distribution networks in this area are not shown). The idea of an EPS control is shown in Figure 3.

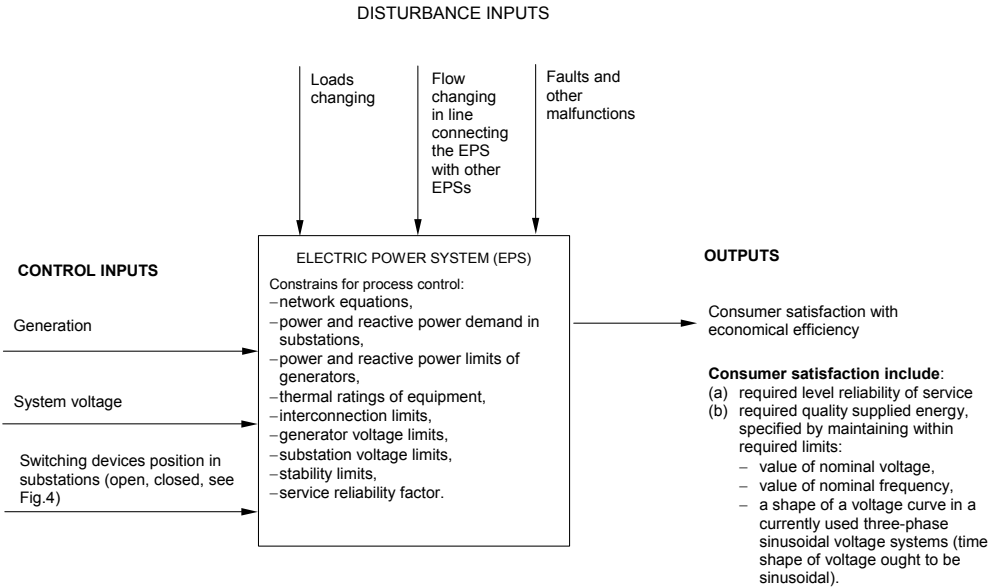


Fig. 3. The idea of an electric power system control

3. HAZARDS IN ELECTRIC POWER SYSTEMS

Most hazards connected with current application of computer-based systems in an EPS concern mainly some applications in power stations, substations and control centres.

Most hazards, which appear in power stations and substations, are hazardous for people and equipment and are connected with the technological process of energy production or switching operations performed at substations. Those kinds of hazards are approximate to the kind of hazards appearing in other sectors of industry. Their nature is rather obvious and due to space limitation in this paper they will not be analysed except of hazards connected with switching operations performed in substations, which were considered in the case study discussed in this paper.

Further on in this section an emphasis is put on description of concept of safety of an electric power system, whose nature is fundamentally different from the nature of those

occurring in the process industry sector and all other sectors of industry.

3.1. Hazards in substations

Electric power substations consist of two essential parts:

- main (high or extra-high voltage) circuits, also called primary circuits;
- auxiliary circuits also called secondary circuits.

Main circuit of a substation is composed of a busbar system (or busbar systems) and connections of power lines, power transformers, etc to the busbar system through switching devices. A busbar system it is set of three electric conductors of very low impedance¹⁾ that serves as a common connection for individual power lines, power transformers, etc. Substations are divided into bays. Bay of a substation it is a part of substation containing high (or extra-high) voltage switching devices and connections of individual power lines, individual power transformers, etc to the substation busbar system (or busbar systems) as well as protection, control, and measurement devices for the individual power line, the individual power transformer, etc. If it is a bay used to connect a power line to busbars it is called a line bay, if it is used for connection a power transformer it is called a transformer bay, etc. Simplified electrical diagram of a main circuit of an example of a typical line bay, which was considered in the case study described in this paper, is shown in Figure 4. Normally a substation contains a few or more line and transformer bays and sometimes also other bays. All bays are similar to the line bay.

Auxiliary circuits are electrical circuits contain measurement, signalling, control and protection devices.

Main hazard for substation staff and equipment is connected with the fact, that for design reasons, disconnectors used in substations are not able to switch on or off the current (e.g. to switch on or off the loaded line) and are used only to ensure the required isolation clearance between disconnected elements which due to design restrictions cannot be achieved by a circuit breaker. In order to take these limitations into consideration switching off a line for example must be performed according to the following sequence (see Figure 4):

- breaking of the current using a circuit-breaker (Q19);
- opening of the line disconnector (Q39) in order to achieve isolation clearance between the disconnected line and the circuit-breaker;
- opening of the busbar disconnector (Q31 or Q32, depending on which busbars, "1A" or "2", the line is connected to) in order to achieve the isolation clearance between the circuit-breaker and busbars.

If this sequence is carried out in an incorrect way, and for example the signal for opening would be sent at first to the disconnector (e.g. busbar disconnector), an electric arc will arise between the contacts of the disconnector accompanied by high rate optic and acoustic phenomena, spraying melted metal etc. The arc would travel to neighbouring phases, resulting in an inter-phase short circuit. It would look like an explosion. This failure would cause considerable material losses because of complete destruction of the disconnector and partially or complete destruction also other components in the substation, disturbance in substation operation and interruption of energy supply to consumers. Sprayed melted metal could seriously injure personnel if accidentally someone of the personnel is near an exploding disconnector.

Depending on the situation in a given EPS, the incorrect sequence of switching operation could also cause even large power system failure and collapse a part of the EPS, i.e. it could creates hazard for described below safety of the EPS.

¹⁾ In high voltage networks transmission lines have three wires, one for each phase. It concerns also busbar systems in substations. Each busbar system in a substation consist of three bars.

3.2. Concept of safety of an electric power system

In electric power systems engineering safety of an EPS is described by means of the word "security", although in less formal descriptions the word "safety" is also used. Because in computer science and software engineering the word "security" is used in a different meaning to avoid misunderstanding, later the paper refers to the safety of EPS by means of the word "safety" which according to widely accepted definition given by the North American Electric Reliability Council (NERC) means *the ability of the bulk power electric system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components*.

Generally speaking, if all generators connected to an EPS work synchronously and the voltage and the frequency in the EPS is within the required limits, then this is a normal, stable state of an EPS. In case of sudden disturbances, e.g. sudden increase of the load, or switching off an important transmission line due to a failure in a substation computer control or protection system, the stable state of operation is disturbed. Each EPS is designed with a certain stability margin. When the disturbance is greater than the stability margin it results in loss of stability and collapse of the EPS, which may be total, and this is called a black-out, or partial.

The loss of stability is understood in the sense applied in dynamical systems, it means generators connected to the EPS fall-out of synchronism. It causes an emergency shutdown the generators by automatic protection devices in order to protect them against destruction and emergency stop of the power stations. Economic and social results of the loss of stability by an EPS are always very serious and can be catastrophic. This is the reason why maintaining stability of an EPS is the main requirement for the EPS planning, operation and control. Hazard for stability is equivalent to hazard for safety of an EPS. Major blackouts are rare events, but as it has been stated in one publication, their impact can be catastrophic. In fact as it follows from the data published by CIGRE (Conference Internationale des Grands de Reseaux Electriques a Haute Tension) the events are not so rare.

A large system failure, which happened in 1977 in New York, blacked out the city that is caused that the city was without an electricity supply. Losses were estimated at 310 millions USD. The last large system disturbance in Poland occurred in January 1987, in effect the north-eastern Poland was without electricity. But even in case of not major blackouts, for example in case of 1000MW outage resulted in an EPS failure, i.e. rather little outage, damages caused by cost of interruption only can amount 4.69 millions USD [1]. The restart of an industrial plant after occurring a power failure with duration time longer than critical one lasts on average 17.4 hours [1].

In the history of the electric utility industry, safety as it is understood today is a relatively recent concept, which emerged after the famous 1965 blackout that left almost 30 million of people of north-eastern United States and Ontario, Canada, without electricity. Possibly the first mention in publications of "safety" in its present sense was in the *Proceedings of The Second Power Systems Computation Conference* in 1966 [2].

Through the first two-thirds of this century, the term "safety" was not used and the safety of an EPS was subsumed with its reliability and implemented into the system in the system planning process by providing a robust system that could withstand any "credible" sudden disturbances without a serious disruption. As it is given in the paper [2], perhaps the epitome of this approach was mid-century American Electric Power system, which in 1974 withstood five simultaneous major tornadoes, losing eleven 345 kV lines, one 500 kV line, two 765 kV lines, and three major switching substations, without interruption of service to customers. Such practices even if technically feasible are no longer considered economically or

environmentally feasible.

The focus in the safety concept was shifted from system robustness, which was designed into the system at the planning stage, onto risk aversion, which is based on automatic protection and control devices, and still to a considerably high degree on intervention of a system operator in real time in an emergency state.

4. CURRENT STATE OF PRACTICE IN ASSURING FUNCTIONAL SAFETY IN ELECTRIC POWER INDUSTRY

An extensive review of available publications made by the author has shown that there is almost the complete lack of documentation of existing practice with reference to design, validation and commissioning of computer-based control systems applied in electric power sector, including applied methods and techniques for ensuring functional safety of the systems. For example among several hundred papers which describe different aspects of computer applications in HV and EHV substations, only in one publication [6] there are some remarks on a safety analysis performed during the development of a substation computer control system to assure operating safety as an essential attribute of monitoring and control systems. The given remarks suggest the existence of rich current practice and certain novel projects on new safety validation techniques, unfortunately they are not understandable without any further explanation.

Apart from the mentioned paper [6] several other publications talk about the necessity to ensure such features of dependability of a substation computer system like functional safety or security, for example [6], [7], [8], and [9], however, without any guidelines what methods and techniques should be used during the design and validation process. Published by CIGRE guidelines [10] is focusing on ensuring quality of telecontrol systems from project management point of view only.

It is an essentially different situation not only from that one in nuclear industry, which as the first expressed safety requirements, but also such sectors as military, transport, chemical, medical, etc. in which for many years numerous papers have been published on assuring safety of computer systems applied in these sectors including issues associated with validation and certification of the systems. Adequate standards and guidelines for military sector, chemical industry or railway were published many years ago.

A general impression of the review is that the existing publications are mainly concerned with the issue of functionality (e.g. scope of performed functions, allocation of the functions, etc.) while not considering such critical dependability aspects of the systems like functional safety, reliability, availability or security.

In Poland there are no standards or regulations for design computer-based control system applied in electric power sector. The rules on validation and commissioning of the systems have not been published.

5. THE EHV SUBSTATION SOFTWARE INTERLOCKING CASE STUDY

5.1. Description of the case study

The case study was carried out in the years 1995 – 1997 as part of the EU joint research project entitled ‘Integration of Safety Analysis Techniques for Process Control Systems’ (ISAT). The aim of the case study was safety analysis of software interlocking applied in substation control system for assuring safety of switching operations which is carried out in the phase of requirements specification. The requirements were specified for 400kV ‘Mosciska’ substation in Warsaw (Poland) treated as an exemplary extra-high voltage

substation. The ‘Mosciska’ substation is a new built substation, built in the middle of the 1990s, which constituting an important node of the grid supplying energy to Warsaw.

Software interlocking system consist in mutual interlocking disconnectors, circuit breakers and earthing switches in order to assure safety of switching operations carried out in a substation during operation and maintenance of the substation with the aim to avoid hazards described in Section 3.1. The interlocking system must for example block the opening of a disconnector when circuit breaker interlocked with the disconnector is closed, or closing an earthing switch (e.g. earthing switch Q45 in Fig. 4) when circuit breaker interlocked with the earthing switch (Q19 in Fig.4) is closed, etc. All these requirements are described by the following basic safety-oriented interlocking rules:

- (1) load flows must not be switched on or off by disconnectors;
- (2) live nodes must not be grounded;
- (3) when connecting live nodes the synchronisation conditions must be fulfilled (this rule will not be considered in this paper).

Normally such a software interlocking system consists of:

- auxiliary contacts of disconnectors, circuit-breakers and earthing switches which transmit information about the status of main contacts to the computer system (closed or open);
- auxiliary relays, used for the control of switch drives (coils of these relays are connected to the outputs of the computer system, whereas contacts are connected to control circuits of switch drives);
- wiring system,
- intelligence of the software interlocking system implemented into the target system software.

The intelligence of the interlocking system can include for example:

- the above mentioned safety oriented interlocking rules;
- ability to tolerate a predefined set of failures;
- other requirements regarding the operation of interlocking.

The ‘Mościska’ substation consists of two busbar systems and eight bays. The case study focused on the bay number 1, to which the line to ‘Milosna’ substation is connected. Simplified electrical diagram of the bay is shown in Fig. 4. The idea how the bay switching devices are controlled by substation control system is shown in Fig. 5. All the substation bays are identical and to some extent typical for all extra-high voltage substations in Poland.

A safety analysis plays the main role in assuring safety of a computer-based system. Such an analysis is performed during the process of computer system design with the aim to identify the hazards and risks associated with application of a computer system, to identify the sequence of events leading to these hazards, to define means of reduction of the identified risks to an acceptable level, and to provide evidence that this level has been achieved.

The assumed approach to the safety analysis in the described below case study was the same one, which is assumed when a new system is being designed. The starting point was an idea of a target system that would control a considered bay and its definition by means of specification of requirements, including safety requirements for a considered interlocking system whose software would be implemented into the target system. Then a system model based on the specification of requirements was designed, and used to analyse the contribution of predefined set of failures, identified constraints (e.g. time constraints), and human factors to the identified hazards. So one can consider that the case study corresponded with first four phases of the Overall Safety Lifecycle in the IEC 61508 standard, namely: (1) Concept; (2) Overall scope definition; (3) Hazard and risk analysis; (4) Overall safety requirements.

The elaborated specification of requirements for the safety analysis included:

- a) Electrical connection diagrams of interlocking system elements.
- b) Boolean functions describing safety rules of switching operations.
- c) Mission requirements for the target system in relation to the operational control of the considered line bay.
- d) Data concerning failures of the interlocking system elements.
- e) Analysis of basic hazards and risks connected with interlocks.
- f) Requirements concerning an expected level of functional safety of interlocking and other attributes of the target system dependability (reliability, availability, and security).
- g) Requirements connected with interlocking described by standards, learned from experience gained during the use of conventional interlocks, etc.

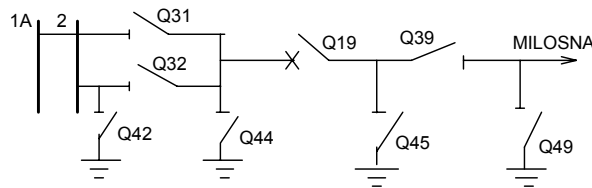


Fig. 4. Simplified schematic diagram of the bay number 1 in Mosciska 400 kV substation (compare Fig. 5)

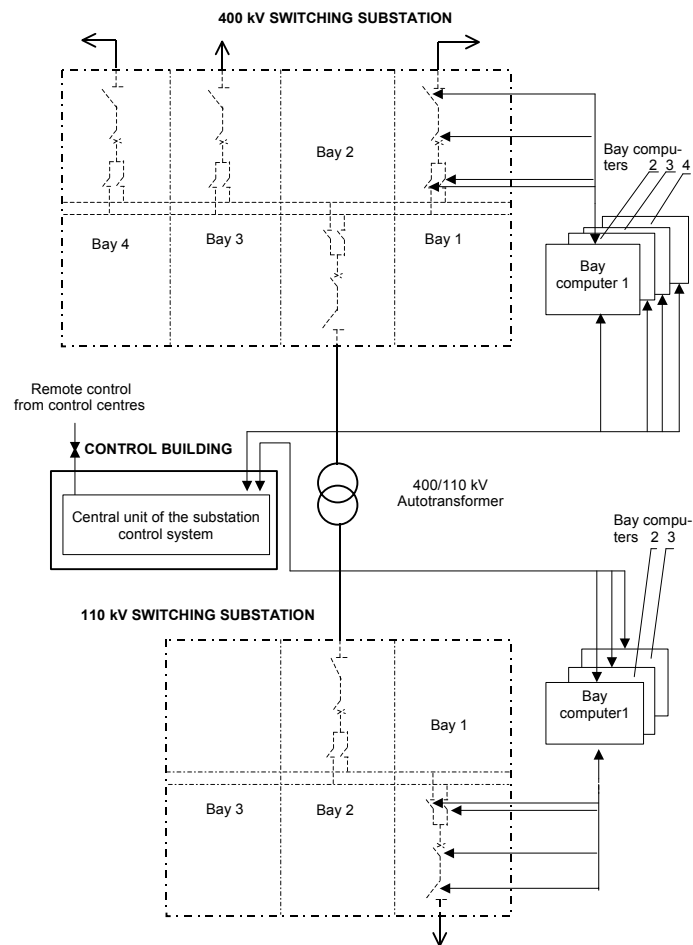


Fig. 5 The idea of switching operations control

The full description of the elaborated specification of requirements and the whole case study exceeds the scope of this paper. Sections below present a short outline of results of hazards and risk identification (item e) and discussion of problems with fulfilling the task. There are also some remarks there that concern availability of data (item d), which substantially contributed to the problems with hazards and risks identification, and definition of requirements mentioned in item f. Description of the case study is given in [11] (full description) and [12]. Object oriented models of the bay and results of safety analysis regarding the methods applied during safety analysis are presented in [13].

5.2. Analysis of hazards and risks connected with software interlocking system

The following typical examples of hazards have been analysed in the case study:

- A. Switching off the loaded line by the disconnectors Q31, Q32 or Q39.
- B. Switching on the line when an earthing switch (switches) is (are) closed, i.e. switching on the line by closing in turn: (1) the disconnector Q39, (2) the disconnector Q31 or Q32, depending on which busbars, 1A or 2, the line have to be connected, (3) the circuit breaker Q19, when one more of the earthing switches Q44, Q45 and Q49 are closed.
- C. Closing an earthing switch when the line or the busbar system, the earthing switch is connected to, is live.

In all these examples hazards potential consequences were considered for:

1. the bay (substation) equipment;
2. the Polish EPS;
3. the substation staff.

Potential consequences of the above hazardous events identified in a very approximate way on the basis of already existing data on failures of substation components, breakdowns and accidents at substations, and large failures of the national EPS are given below. Remarks are also given on probabilities of the hazardous events which might appear in case of not using interlocking. The remarks are given on the basis of existing experience and discussions with specialists. Discussion of the problems with identification of hazards and risks is presented in Section 5.3.

A. Switching off the loaded line by the disconnectors Q31, Q32 or Q39.

Case A1. Potential consequences for the bay (substation) equipment. The complete destruction of the disconnector only is of minimal consequence and damage includes:

- cost of a new disconnector: ca 21,000 USD (in Poland);
- cost of disconnector replacement (replacement time ca. 2 days);
- disconnecting the line in the bay number 1 within the replacement time of disconnector in case of the failure of the disconnector Q39.

Probability of a hazardous event. Exact data were not available. Intuitively, according to existed experience, frequency of this type of accident could be estimated as about one accident within each several years for the whole Polish EPS.

Case A2. Potential consequences for the Polish EPS. The consequences depend very much on the state of the EPS when the hazardous event occurs and such factors as:

- season of the year,
- weather conditions,
- level of industrialisation of the community,

– preparation level of the power sector and the community for big EPS failures, etc.

Exemplary consequences are as follows:

- (a) cascading outages resulting in a collapse of a part of regional EPS and considerable outages;
- (b) large EPS failure which causes sectioning of the national EPS and collapse of one or more system parts (islands) which had been formed as a result of this sectioning;
- (c) collapse of the national EPS (blackout).

The smallest damage generally would appear in the case (a). For 1000 MW outages for industrial plants the damage caused in this case by the kW interrupted only (not taking into account the kWh not delivered) would cost approximately 4.69 millions USD (average costs updated to July 1987 for all plants, small and large [1]). According to [1] Average Plant Restart Time for US and Canada after complete shutdown of a plant is 17.4 h.

In case of a big system failure, the total damage would strongly depend on the situation at the moment of this hazardous event, and it had not been yet identified for the Polish EPS. On the basis of existed experience, it was possible only to state that:

- material damages could be estimated as medium high (several to a dozen or so million US dollars) or high (more than that);
- social damages would depend on the level of industrialisation (management standard, applied technologies, etc.) and social development (utilisation of electric appliances, level of organisation of social life, value of individual and common time of society members etc.), and they had probably never been assessed by anyone; it seems that for Poland they according to the IEC 61508 standard could be estimated as small up to medium and higher ones, depending on a region of the country.

Probability of a hazardous event. Data were not available. Basing on existed experience it was possible to state only, that a big system failure happens in Poland every several up to a dozen or so years.

Case A3. Potential consequences for substation staff. The consequences concern the maintenance and repair staff which works in the direct vicinity of the disconnecter subject to failure. Typical possible consequences are personal injury, sometimes even very serious (e.g. eyes).

Probability of the hazardous event. No information about accidents of this type in the past had been found in publications. Due to strict regulations concerning people entering the area of a substation the probability of such an accident seemed to be small.

B. Switching on the line when an earthing switch (switches) is (are) closed.

Case B1. Potential consequences for an EPS. Smaller than in the Case A2, but in the worst case could be comparable.

Probability of a hazardous event. The probability strongly depends on situation at the moment of occurring of the event and had not yet been specified for the Polish EPS. Roughly, it could be stated that the probability of this type of hazard was comparable to Case A2.

Case B2 and B3. Potential consequences for bay (substation) equipment and substation staff. In a substation which is properly designed such an accident could cause only short circuit switched off by the substation protection system without any consequences. Therefore it was assumed that this violation of safety-oriented interlocking rules would not create hazard for substation staff and equipment.

C. Closing an earthing switch when the line or the busbar system, the earthing switch is connected to, is live.

Case C1. Potential Consequences for Bay (Substation) Equipment. The consequences were similar to the consequences in the Case A1 but for an earthing switch.

Probability of a hazardous event. Similar to those in Case A1.

Case C 2. Potential consequences for an EPS. Similar to the consequences in the case A2.

Probability of a hazardous event. Similar to those in case A2.

Case C 3. Potential consequences for substation staff. As in the Case A3

Probability of the hazardous event. In the reviewed Polish publications any information on this subject had been found. From the telephone contacts with institutions which deal with the problem of safety at work and gather data on accidents at industrial sites in Poland it followed that such data were not available. Very short period of the project did not allow running more exhaustive search for the information about accidents of this type in the past. However, to the contrary of the Case A3, the probability of such an accident seemed not to be small. The control of the earthing switches is carried out by substation staff by means of control buttons in a local control cabinet (in the bay) or control buttons at control boards located in earthing switches and not from the substation control room. In case of control by means of control buttons at control boards if accident occurred consequences could be serious in most cases.

5.3. Problems with the application of the standard IEC 61508 which appeared in realization of the case study

Exact specification of hazards and risks for a given EHV substation would require a full analysis of hazards and risks for the whole EPS and the monitoring of possible influence of interconnected EPS's on a given EPS. Such an analysis has never been carried out in Poland, because in fact such a need rather did not exist up to the present. In Poland, the national electric power system has only existed since the beginning of the 1960s (in leading countries the origins of first electric power systems came into being as early as in the 1930s). At the start of development of the electric power industry, there were separated power stations and local systems. From the 1960s, the Polish EPS, control systems applied in the EPS, and data network coupled with it have become more and more complex. At present, the situation is alleviated by a decrease in power demand, but nevertheless such an analysis is becoming more and more necessary.

The existing EPSs have been evolving for many years basing on another concept of its reliability assurance. Also they have never been designed for the free market of electricity. Hence, in present completely different conditions and with another concept of reliability assurance, their behaviour is to some extent unknown. It has been confirmed by published results a study of significant disturbances made in the USA [14]. It for example follows from the study that relays of EPS protection systems were involved in one way or another in 75% major disturbances which took place in the USA between 1984-1988. Common scenario of these disturbances was that a relay had an undetected (hidden) defect not detected during normal operation, calibration or maintenance that was exposed due to conditions created by other disturbances (e.g. nearby faults, overloads, or reverse power flows). The example is given that on December 14th, 1995, a fault occurred on a 345 kV line in southern Idaho, which

tripped correctly, followed by an incorrect trip of a parallel line and an overload trip of a third line. As a result:

- the system became unstable and divided into four system islands;
- 3,000 MW load was disconnected.

Similar situation could for example be caused by an incorrectly performed switching operation in a substation.

Exact specification of hazards and risks would also require exact data on failures of substation components, breakdowns and accidents at substations. These data similarly as requirements for such quality attributes of computer systems used in safety analysis as reliability, availability, and security were not available.

The data on failures of substation components used for traditional relay-based control systems design were insufficient. There were available certain data in foreign publications but they could be used only in a limited way, just to estimate roughly, because each national system has got its own characteristic formed by its history.

In Poland in traditional relay-based technology the quality attributes of computer-based systems were not considered except for reliability. And if they were (like reliability), they were considered in a very simple qualitative manner and rather intuitively. Therefore, requirements for these attributes are not expressed, and assumption of input data for these attributes has also created substantial difficulties. They were assumed roughly on the basis of foreign publications.

When the case study presented in this paper was carried out, there was published a very advanced draft version of the International Standard IEC 61508 which already during the phase of the draft had been considered very important as a summary of existing experience within the field of safety-related systems design and a base for development of industry sector specific standards.

This standard is based on the concept of necessary reduction of the identified risk to meet the tolerable risk for a specific situation and the relationship of risk to safety integrity. Decision on acceptance of a risk as tolerable risk is based on ALARP principle, that is on consideration whether it is "As Low As Reasonably Practicable" taking into account costs and benefits of further risk reduction.

For the safety integrity level assigned to a system the standard gives guidance on all aspects of system development including the lifecycle phases, the documentation required, software and hardware development methods, testing, etc. The standard include both quantitative and qualitative method which can be used where the risk or the frequency cannot be quantified.

However, even if in the considered case study potential consequences of accidents and their probability would be defined, it had not come up against any published guidelines or even discussion on risk classification for an EPS. If for example one would like to define the risk classes for examples presented in Section 5.2 according to the example of risk classification of accidents given in the standard IEC 61508 in Table B1 in Part V very tentative risk classes for interlocking used in Poland could be defined e.g. as follows:

- Case A1 - Risk Class III
- Case A2 - Risk Class I - III

However it would be intuitive and only very tentative classification (just for orientation) on the basis of discussion with specialists because at the time when the case study was carried out as well as at the present time it has not been come up against any published frame of reference for the following terms used in the standard for the risk classification:

- consequence (negligible, marginal, critical, catastrophic),
- frequency (incredible, improbable, remote, occasional, probable, frequent).

Similarly, it has not been come up against any published frame of reference for terms used in the above mentioned IEC standard for determination of safety integrity level of the computer system functions related to safety, for example in case of application of quantitative method described in Part V, Annex D for terms:

- consequence (C),
- frequency and exposure time (F),
- possibility of avoiding the hazardous event (P),
- probability of the unwanted occurrence (W).

The standard assumes that the Table B.1 is sector dependent and for specific sectors the classification of potential consequences and frequencies will be developed taking into account a wide range of social, political and economic factors.

Development of a guideline on the IEC 61508 standard application for EPSs would need collection of data for switching devices failures, accidents in substations and power stations, and failures of EPSs, collected in an appropriate way, preferably according to an international standard on data collection and cooperation on international level. At the time when the case study was carried out in Poland the data were not collected in appropriate and systematic way.

6. CONCLUSIONS

1. In studying the existing standards and legal regulations in the Polish electric power sector, one has no doubts that the electric power sector state-of-the-art (i.e. knowledge and experience) is appropriate for traditional control technologies. Awareness of the basic difference between software-based systems and traditional ones is insufficient. On the basis of observing how IT technologies are being introduced in Poland one can also state that also legal responsibility awareness that accompanied introducing traditional technologies, decreased in case of IT technologies. Suitable legal manners and practices referring to software-based technologies have not developed yet and there is often an impression as if these technologies were introduced beyond the traditional sense of legal responsibility.

2. The shift of the idea how to provide an EPS safety and reliability from robustness of the EPS into control of the EPS during an emergency state will increasingly challenge the state of the art in EPS monitoring, communications, and control based on high dependable computer systems. It seems that this fact together with the increasing technical and organisational complexity of the electric power sector, strongly heightens the necessity for legal regulations and standardisation in the field of design, validation, commissioning and maintenance of computer systems applied in the sector. One of the aims of the regulations would be enabling the supervision, by an independent organisation or by the government, of safety and security aspects in the EPS, which is the national infrastructure for energy supply, considered as the most critical for the national security, economic prosperity, and social well-being as well as for everyday life a society. Such a sector standard could probably be based on the international standard IEC 61508. Preparation of the sector standard or guidelines for the usage of the international standard in the electric power sector would require collection of data on failures and accidents in electric power sector in an appropriate and systematic way, preferably according to an international standard or guidelines on the data collection, and cooperation on international level.

3. Since electric power and telecommunications infrastructures are considered the most vulnerable to sabotage and cyber-attack, in specifying of functional safety requirements for substation automation systems and for computer-based systems used in power stations and control centres interaction of safety, security and availability requirements should be taken into account.

4. The automation of substations, similarly like automation of equipment and plants in other sectors of industry, is more and more based not only on hardware but also on software solutions. Software engineers are not able to design protection and automation systems used in electric power sector without co-operation with electric power systems engineers. It especially concerns requirements specification and safety analysis phases. It seems that these facts should have influence on curricula of electrical engineering faculties. The experience gained during the case study showed that the curricula should at least include *Requirements Engineering* (lectures, classes and laboratory) to the extent which enables graduates carry out specification of requirements on their own, co-operate with software engineers during validation of models used in a safety analysis, carry out the safety analysis, evaluate of results, and co-operate with software engineers in next phases of a project [15], [16].

REFERENCES

1. IEEE Recommended practice for the design of reliable industrial and commercial power systems, ANSI/IEEE Std 493-1990, May 1995.
2. Balu, N., Bertram, T., *et al.*: On-Line Power System Security Analysis. Proceedings of the IEEE, Vol. 80, No. 2, pp. 262-280, 1992.
3. Electric Power Research Institute (EPRI): Electricity Technology Roadmap: Powering Progress - 1999 Summary and Synthesis. EPRI, Palo Alto, 1999.
4. Electric Power Research Institute (EPRI): Issues and Solutions: North American Grid Operations (2000-2005). EPRI, 1999.
5. Executive Summary: EPRI/DOD Initiative On Complex Interactive Networks/Systems. www.epri.com, 1999.
6. Martin O., Messie M., and de Labrouhe G.: The digital monitoring and control of substations, in Proc. CIGRE Conf., paper no. 23/13-02, 1994.
7. de Labrouhe G.: Computer-based systems for transmission substations, Power Technology International, pp. 73-76, 1996.
8. Design and maintenance practice for substation secondary systems, CIGRE Working Group 23.05 Tech. Rep., April 1994.
9. Telecontrol equipment and systems, International Standard IEC 60870 Parts 1-6.
10. Guidelines for software project control, CIGRE Working Group 01 of Study Committee 35 Tech. Rep., August 1994.
11. Żurkowski Z.: Task B1b: Identification and Preparation of Case Studies – Extra-High Voltage Substation Software Interlocking Case Study, EC COPERNICUS JRP 1594, Technical Report TR ISAT 97/8, Institute of Power Systems Automation, December 1996, Updated: February and April 1997.
12. Żurkowski, Z.: Safety and Security Issues in Electric Power Industry. In Proceedings of the 19th Conference SAFECOMP 2000, Rotterdam, The Netherlands, October 2000.
13. Nowicki, B., Górski, J.: Object Oriented Safety Analysis of an Extra High Voltage Substation Bay. In Proceedings of the 17th International Conference SAFECOMP'98. Lecture Notes in Computer Science, Vol. 1516. Springer-Verlag, Berlin Heidelberg, pp. 306-315, 1998.
14. Phadke, A.G., Thorp, J.S.: Expose Hidden Failures to Prevent Cascading Outages. IEEE Computer Applications in Power, pp. 20-23, July 1996.
15. Żurkowski Z.: A Proposal of Computing Courses for Electrical Engineering Faculties, Proceedings of the International Symposium “Modern Electric Power Systems” MEPS'02, Wrocław, Poland, 2002.
16. Żurkowski Z.: A Suggestion of Courses on Computing for Electrical Engineering Faculties and to the Catalogue of Standard Knowledge of a Power Engineer, <http://www.epeeforum.org/contribution.asp?sujet=3> (file Żurkowski_Contribution.doc).