Mieczysław Borysiewicz

Aleksej Kaszko

Karol Kowal

Sławomir Potempski
National Centre for Nuclear Research (NCBJ)

Loss of offsite power caused by tornado in Surry NPP – a case study

Keywords

Surry NPP, tornado, loss of offsite power, emergency power system, probabilistic safety assessment

Abstract

The aim of this work was to perform the real case study for the US Surry Nuclear Power Plant which was touched down by tornado in 2011 causing the electrical switch yard destruction and loss of offsite power. Probabilistic methods have been applied to assess the reliability of the reactor shutdown and effective heat removal after this accident. The reactor protection system and auxiliary feedwater system were thoroughly analysed in the context of their safety features designed to prevent the reactor core damage. The emergency power system reliability has been also considered due to the fact that some components of the safety systems are electrically operated. Moreover, time-dependent analysis has been performed in order to address the level of damages after an extreme external event like tornado. Depending on the severity of such events the time required to restore the electrical grid may be significantly different and longer than 24 hours. The reliability and requirements for safety systems are changing with time and these changes have been taken into account as well.

1. Introduction

Surry Power Station is a nuclear power plant located in Surry County in south-eastern Virginia (USA). There are two triple-loop Westinghouse pressurized water reactors (PWR). Each of them generates 800 MW of electrical power. The single reactor has three steam generators, three coolant pumps, one pressurizer, and 157 fuel assemblies (*Figure 1*). Reactors of this type are operated also in other plants in the United States: in Beaver Valley, Farley, H.B. Robinson, North Anna, Shearon Harris, V.C. Summer, and Turkey Point. In this study the methods of Probabilistic Safety Assessment (PSA) Level-1 have been applied to access the core damage frequency of such a reactor following the loss of offsite power accident caused by tornado. This type of analysis provides insights into the design weaknesses and possible ways of preventing core damage, which in most cases is the precursor of accidents leading to severe radioactive releases with potential heals and environmental consequences.

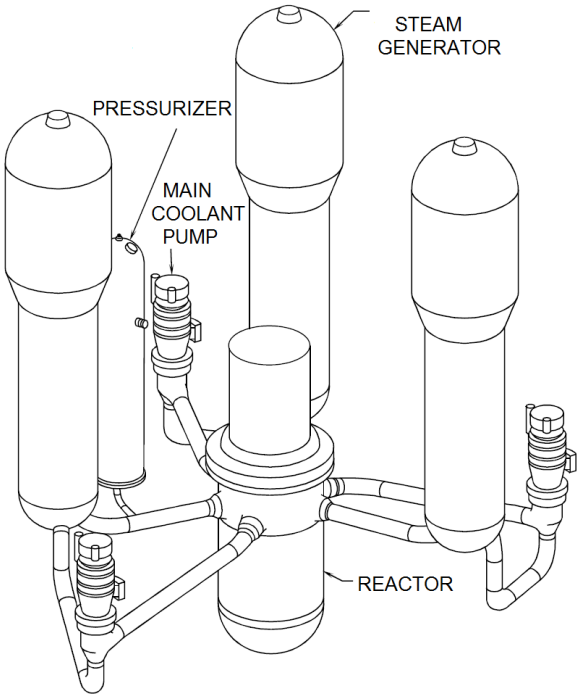

Figure 1. The triple-loop Westinghouse PWR

PSA Level-1 includes the event tree and fault tree modelling, determination of the minimal cut sets as well as the uncertainty assessment. Cut sets are unique combinations of component failures that can cause system failure following the assumed initiating event. Thus, the minimal cut sets can be used to understand the structural vulnerability of the whole system. Cut sets can also be used to discover single point failures (one independent element of a system which causes an immediate hazard to occur and/or causes the whole system to fail) [1]. The analysis described in this paper was performed using the SAPHIRE code developed by the U.S. Nuclear Regulatory Commission (NRC).

2. Loss of offsite power accident

On April 16, 2011 a tornado touched down in the switchyard of the Surry Nuclear Power Plant, cutting off external power to the plant. Both units of Surry NPP automatically shut down after losing offsite power. Because of loss of offsite power diesel generators started to supply units emergency loads to proceed shutdown and cooling of the plant. Soon after LOOP Surry NPP operator notified NRC of the situation and NRC declared an unusual event, the lowest of the four NRC emergency classification levels. On April 17 NRC reported that power has been partially restored and safety systems have operated as needed. [5].

Loss of offsite power (LOOP) is commonly analyzed initiating event in PSA for the nuclear power plants (NPP). It is associated with the loss of access to an offsite power grid, and can lead to unplanned reactor shutdown. Shutdown is performed as a precaution since availability of alternating current power is essential for safe operation and accident recovery. This shutdown requires decay heat removal with emergency power supplied by diesel generators.

Surry NPP response to the LOOP is to perform rapid shutdown of the reactor, which means termination of fission processes inside the core. This shutdown is achieved by the reactor protection system (RPS), by dropping the reactor control rods into the core. This happens automatically in no electricity state. After reactor achieves subcritical state, decay heat must be removed from the primary reactor loop, to prevent overpressure in the reactor coolant system (RCS) and subsequent reactor meltdown. The heat generated in the reactor core is transferred through the steam generator pipe to secondary loop water that turns into steam. Surry Unit 1 losses its power conversion capabilities during loss of offsite power, due to inoperability of the main feed water pumps, condensate pumps, circulation water pumps etc. Assuming that the RPS system performed its function, a total lack of feedwater delivery to the steam generators to remove heat generated by the core would result in the steam generators boiling dry on the order of about 30 minutes.

Therefore, in case of LOOP the auxiliary feedwater system (AFWS) becomes the primary feedwater supply. Steam from the generator is released to the atmosphere through the safety valves. Turbine bypass to the condenser is impossible in that case due to the loss of vacuum and condensate pumps. Successful operation of AFWS and safety steam release ensures sufficient cooling of the reactor core during such event like LOOP [4].

The event tree developed do describe the possible sequences of the accident progression is depicted in *Figure 2*. If RPS system and AFWS systems performed their function the End Stare 1 is obtained, in case if RPS performed its function and AFWS not, End State 2 (F01) is obtained in which decay heat cannot be removed. If RPS and AFWS would not perform their function worst case scenario is achieved in which reactor is still running and decay heat cannot be removed.

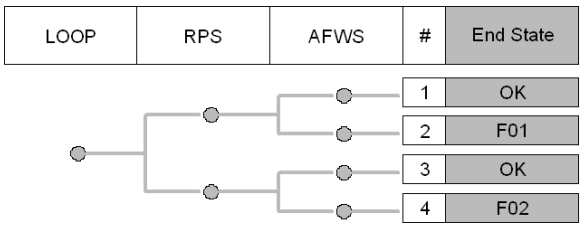

Figure 2. Event tree of LOOP event

3. Reactor Protection System

The reactor protection consists of a set of nuclear safety components designed to protect and/or safely shutdown the reactor while preventing the release of radioactive materials (*Figure 3*). The system can shut down the reactor automatically. This occurs when the parameters meet or exceed the set of applied limits. In PWR reactors the shutdown results in a full insertion of the control rods into the core. The insertion is performed by the gravity, thus no electricity is required to fulfil this function. The RPS is to ensure the pressure and thermal protection. The pressure protection systems have the responsibility to protect the reactor and various systems pressure integrity. The thermal protection systems have the responsibility to keep the reactor fuel elements covered and, when necessary, reduce the temperature of the reactor coolant to safe and stable state.

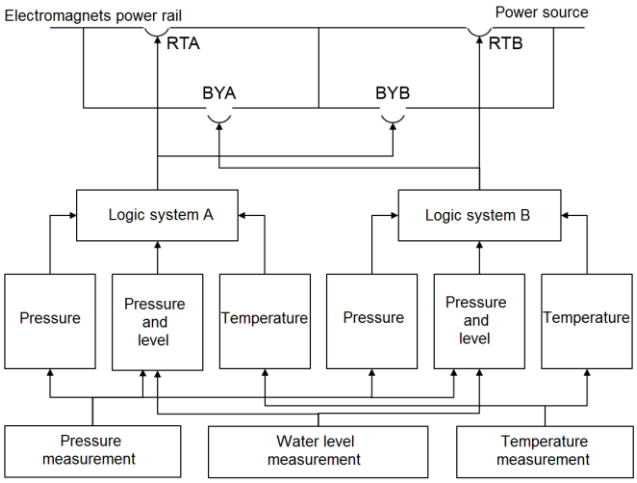

Figure 3. RPS functional scheme

For the availability of RPS system to fulfil its function during LOOP almost all control rods (at least 46 of 48) must be injected into the reactor core. Unavailability of RPS system mean such situations, in which more than two rods were not injected for some reason in the core. The reason for this state of RPS may be simultaneous failure of both power shut down subsystems A and B (*Figure 2*). This event includes both, logic errors and failures of electrical switches. In addition, in the RPS fault tree, loss of control over the switch BYA (BYB) while it is closed due to maintenance or RTA (RTB) tests is covered. Both subsystems, A and B may also have failure as a result of the inadequate calibration of measuring equipment. A distinct contribution to the probability of non-availability of the RPS (PRPS) are submitted by mechanical damages that are blocking the roads injection to the core. They are applied for both control roads and the reactor core.

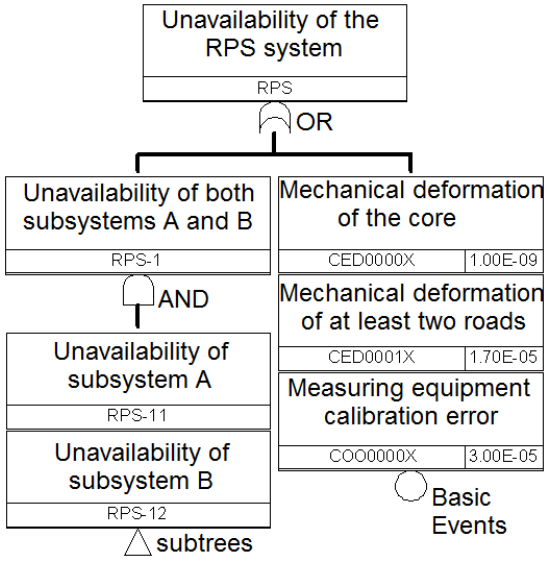

Figure 4. RPS system main fault tree

Table 1. List of cut-sets of RPS fault tree

No	Name	Description	P
1	COO0000X	Inappropriate calibration of equipment	3,00E-05
2	CED0001X	Mechanical deformation of the core	1,70E-05
3	CAD0001X CCB0003X	Fault of logic circuit B Switch BYA closed for conservation	6,04E-06
4	CAD0002X CCB0002X	Fault of logic circuit A Switch BYB closed for conservation	6,04E-06
5	CCB0004D, CCB0005D	Switch RTB not opens on demand Switch RTA not opens on demand	1,00E-06
6	CAD0001X CCB0005D	Fault of logic circuit B Switch RTA not opens on demand	9,90E-07

4. Auxiliary Feedwater System

The primary function of the auxiliary feedwater system (AFWS) is to supply feedwater to the steam generators following accident or transient conditions when the main feedwater system is not available. This system consists of external reservoirs of water, two motor driven emergency feedwater pumps, turbine driven emergency feedwater pump, and the required piping, valves, instruments as well as controls necessary for system operation.

In operation, the emergency feedwater pumps take suction from the tanks and discharge the water into the main feedwater piping between the steam generator feed nozzle and the last check valve in the main feedwater line. The steam supply line for turbine driven pump is connected to the main steam line from each steam generator. This line is fitted with a pneumatically operated steam admission valve arranged to fail-open on loss of air or electrical power. A primary emergency feedwater supply tank, to which the suction of the emergency feedwater pumps are normally aligned, is provided in each subsystem. The tanks are safety grade and seismically qualified. Tank contains a quantity of condensate quality water sufficient to allow the plant to be maintained in hot standby for 13 hours then enabling a 5 hour cool down of the plant. *Figure 5*

AFWS system unavailability during LOOP may be cased from a failure in the supply of water to the pumps, pumps failure (including also luck of power supply), insufficient water flow through the two main collectors (H1 and H2) or pipelines carrying water from the collectors to the steam generators.

The failure in the water supply for pomp system of the AFWS includes failure of TK-1A tank and interrupting of at least one of the three pipelines (A, B or C) during the first 8h from LOOP . In addition, due to the fact that considered exposure time is much longer than 8 hours, there is the additional need to cover in fault tree failure of fire protection bus, its pipeline, as well as manual valves XV120 and XV185.[2]

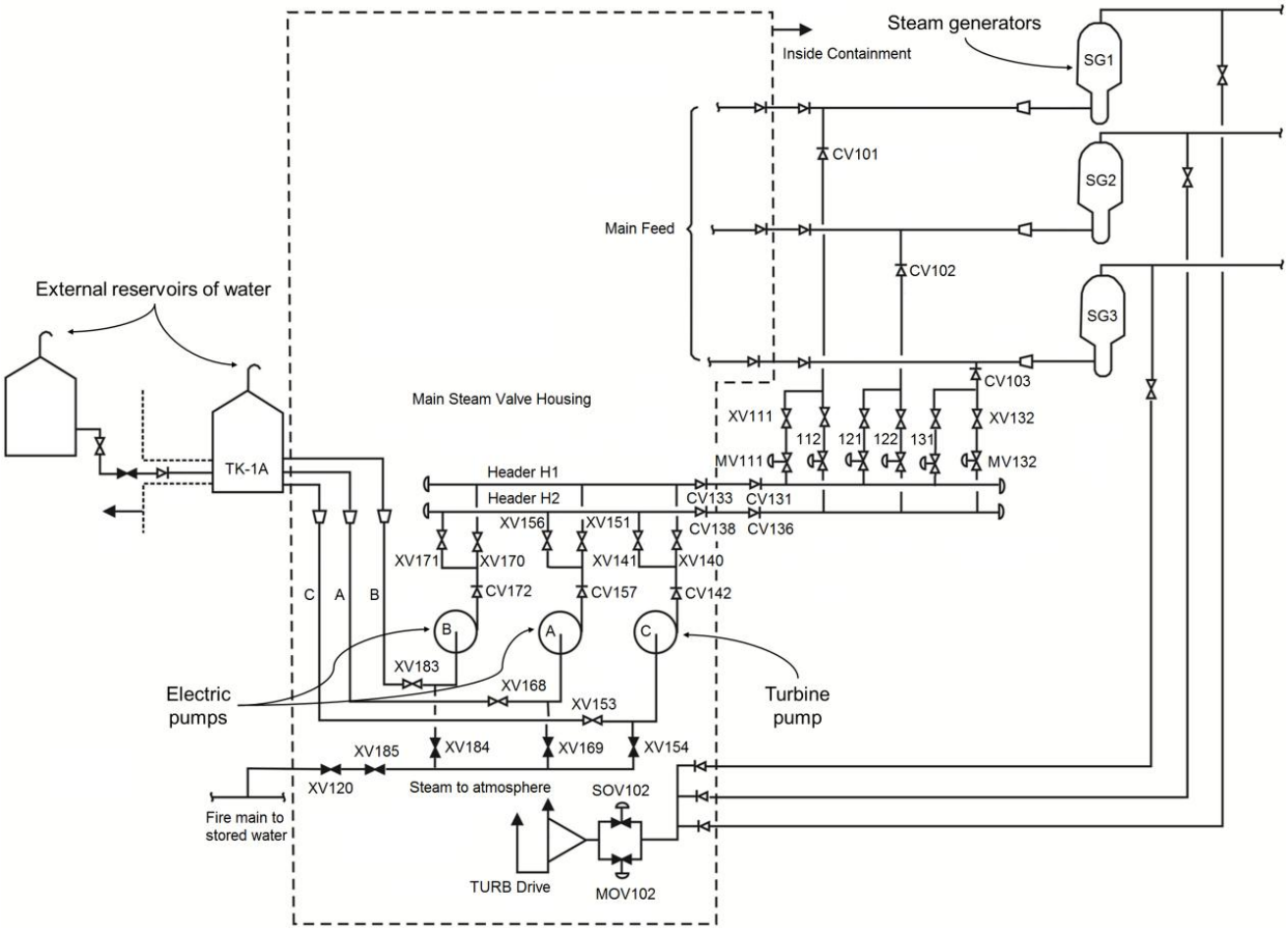

Figure 5. Auxiliary Feedwater System

Table 2. List of cut-sets for AFWS fault tree

Nr	Name	Description	P	Percentage
1	DXV0185C	Manual valve 185 closed	5,40E-04	42,52%
2	DXV0120C	Manual Valve 120 closed	5,40E-04	42,52%
3	DPP0000R	Main steam valve rupture	7,50E-05	5,91%
4	DOO0000X	Pump valves common cause failure	3,00E-05	2,36%
5	DXV0168Y, DXV0183Y	Manual valve 168 closed after conservation Manual valve 183 closed after conservation	9,00E-06	0,71%
6	DST0002T, DXV0168Y	Fault in electrical pump B circuit Manual valve 168 closed after conservation	8,34E-06	0,66%
7	DST0001T, DXV0183Y	Fault in electrical pump A circuit Manual valve 183 closed after conservation	8,34E-06	0,66%
8	DST0001T, DST0002T	Fault in electrical pump A circuit Fault in electrical pump B circuit	7,73E-06	0.61%

5. Emergency Power Supply

Emergency power system (EPS) is used to provide power to the safety systems in order to mitigate consequences of postulated accident. The most strict requirements for EPS are immediately after an accident. Those requirements are reduced with time after the accident occurring because number of tolerated failures for safety functions can increase before core outage. The EPS system of the considered reactor in Surry NPP consists of:

- two sources of offsite AC (alternative current) power,
- two sources of onsite AC power which consist of two diesel generators,
- two sources of DC (direct current) power consisting of two 125 volt batteries,
- additional equipment such as: transformers, buses, cables that are used for distribution of power to ESF loads.

Lack of adequate power supply can therefore lead to different effects depending on the point at which the EPS failure occurs. Detachment of the turbo generator coupled with external network leads to instability in this network due to the sudden loss of generation capacity. In this case, the only source of alternating-current that remains are two diesel generators, whose function is reception to full load within a few seconds. Then, a few large inductive drives energizes to act at simultaneously, and the value of the required start-up currents are so high that they could constitute a common cause of falling out of both generators.

During normal operation of the power plant, electric power is supplied from the main generator. The output voltage is transformed from 22kV to 230kV through the main transformer and transferred to the high voltage switching overhead through line 230kV and fed back to the external power grid through two 500kV lines. In emergency situations, the main generator of the reactor is shut down and cannot be a source or power neither for balance of plant nor for safety systems.

Electricity is then feed from the external power grid through high-voltage switchgear. The input voltage is reduced by winding of two autotransformers from 500kV to 4,16kV. The loss of external network leads to launch of diesel generators. Each of them has the power of 2,75kW and is activated by the control system automatically within 10 seconds after loss of the network occurs. Distribution of electricity within the EPS is performed by two redundant lines A and B. Each of them consists of a direct-current (DC) and alternate-current (AC) buses. Main AC buses (4.16kV) provide power to the largest engines of the safety systems. Other AC buses are supplied from the main buses after voltage changes from 4,16kV to 480V and provide power directly to several smaller motors. DC busses provide power supply for control systems. The failure of both DC busses (from line A and B) leads to a complete loss of control over switches in the control circuit systems.

Failure of the EPS system is defined as the inadequate power supply of safety systems during the accident. This state of EPS, which does not allow for full functionality of safety systems, may be the result of insufficient power supply of any pair of redundant rail from lines A and B, or insufficient power supply of DC bus on one line and any AC bus on second line [3].

6. Results

In Table 3, summarizing the results, we can see huge changes in probability after 8h, which is caused by insufficient amount of steam for turbine pump. Main contributors for such probability were manual valves (120 and 185) for time shorter than 8 hours and diesel generators for time longer than 8 hours. The study shows importance of including time dependent analysis of the reliability of electrical supply system into the PSA study for NPP.

Table 3. Obtained results for LOOP accident

Nr	Duration of LOOP	Probability/Frequency
1	1 hour	4.47E-5
2	4 hours	4.48E-5
3	8 hours	4.71E-5
4	after 8 hours	1.257E-4
5	24 hours	1.80E-4
6	144 hours	9.681E-4
7	360 hours	3.627E-3

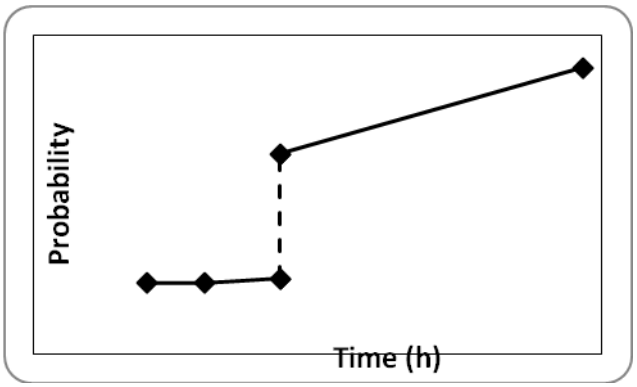

Figure 6. Results for LOOP accident 1-24h

Figure 6 shows the probability of core damage probability after lose of offsite power as a function of time required to the offsite power recovery. In case

of tornado in 2011 the greed power had been recovered in 24h which corresponds to the last point in *Figure 6*. Assuming the recovery time is shorter than 8 hours the core damage probability would be small (about 4,6E-5). On the other hand if power system would not be recovered during first 24 hours the core damage probability would increase rapidly as it is shown in *Figure 7*.

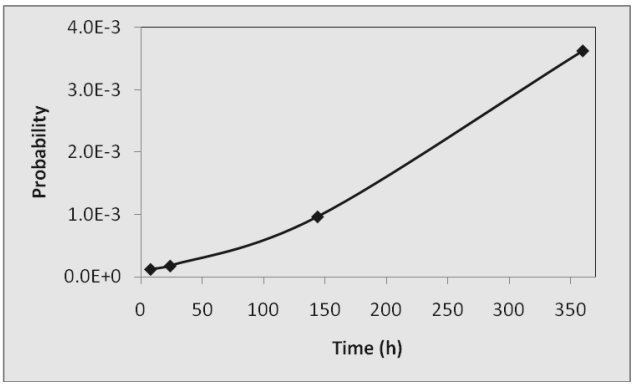

Figure 7. Obtained results for LOOP accident 8-360h

7. Conclusions

In 2011 tornado caused electrical switchyard destruction disabling primary power to the Surry NPP cooling pumps and causing the backup diesel generators to activate without incident. This paper was aimed to calculate reliability of safety systems for such accident, and core damage frequency. We have analyzed loss of offsite power for different times to obtain reliable data.

References

[1] Kececiogu, D. (1991). *Reliability Engineering Handbook*, Prentice Hall, Inc.,. New Jersey.
[2] Kowal, K. & Borysiewicz, M. (2015). Analiza niezawodności systemu zabezpieczenia reaktora typu PWR. *Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska* 5, 73-79.
[3] Poloski, J.P., Grant, G.M., Gentillon, C.D., Galyean, W.J. & Knudsen, J.K. (1998). *Reliability Study: Auxiliary/Emergency Feedwater System*, U.S. NRC, Washington, DC.
[4] U.S. NRC *NRC monitors events at Surry nuclear power plant after loss of offsite power and unusual event declaration,* NRC NEWS Aprill 17, 2011
[5] U.S. Nuclear Regulatory Commission (1975). *Reactor Safety Study - An assessment of accident risks in U.S. commercial nuclear power plants*, U.S. NRC, Washington, DC.