PSA APPLICATION IN THE DIVERSE ACTUATION SYSTEM DESIGN (Draft)

Zhan Wenhui[1] Zhang Binbin[2]

[1]*Shanghai Nuclear Engineering Research and Design Institute, Shanghai, China 200233,zhanwh@snerdi.com.cn*
[2] *Shanghai Nuclear Engineering Research and Design Institute, Shanghai, China 200233,zhangbb@snerdi.com.cn*

ABSTRACT: Diverse Actuation System (DAS) is designed as a diverse backup system for Protection and Safety Monitoring System (PMS) to perform the functions of reactor trip and engineered safety features actuation in AP1000 type nuclear power plants. However, not all of the PMS functions should be included in the DAS design. In this paper, the Probabilistic Safety Assessment (PSA) technique was used to identify the DAS functions by comparing the core damage frequency caused by initiating events in at-power internal event PSA. Furthermore, protection parameter signals of DAS to actuate mitigating systems are identified by accident progress analysis.

KEY WORDS: Diverse Actuation System (DAS), Probabilistic Safety Assessment (PSA), Protection Function Allocation

1. Introduction

Diverse Actuation System (DAS) is a non-safety Instrumentation and Control (I&C) system, and acts as a diverse backup system for Protection and Safety Monitoring System (PMS), to provide reactor trip and Engineered Safety Features (ESF) actuation, which works separately from PMS. After a presumed transient event with Common Cause Failure (CCF) between PMS and Plant Control System (PLS), DAS provides an alternate means of systems actuation, which lowers the frequency of severe core damage.

Based on the accident sequences and the Core Damage Frequency (CDF) results in at-power internal event Probabilistic Safety Assessment (PSA) model, systems that requires DAS to provide protection functions are screened, and the associated actuating signals are identified.

2. Identify the protection systems requiring DAS actuation

2.1 Brief introduction of DAS

To lower the risk of Anticipated Transient Without Scram (ATWS) condition, U.S. Code of Federal Regulations 10 CFR 50.62 requires that each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. 10 CFR 50.62 also requires each pressurized water reactor must have a diverse scram system from the sensor to cut of power to the control rods[1].

Refer to the federal regulations and the requirements from NRC, a no software-based DAS which had adequate diversity from PMS and PLS was designed by Westinghouse to provide a backup emergency reactor trip and engineered safety features actuation functions.

2.2 Plant risk without DAS

Firstly, risk without DAS is assessed. After getting the CDF results of each initiating event and screening particular initiating events with the CDF contribution more than a certain value (1.0E-07 per reactor year, which is 1% to the URD requirement, total CDF<1.0E-05/ry), event sequence analysis of these selected initiating events is carried out.

The internal event PSA model under at-power condition is set to be without DAS, and this model is considered as a basic model. The CDFs of each initiating events are calculated, and the results are listed in Table 1. It shows that 6 initiating events

are found to exceed the analysis criterion and have much more contribution to the total CDF than other events. They are Transient with Main Feedwater (TRANS), Loss of Feedwater (LMFW), Loss of Component Cooling / Service Water (LCCW), Loss of Condenser (LCOND), Loss of Feedwater to One Steam Generator (LMFW1), Loss of Offsite Power (LOSP). As a matter of fact, the design of DAS should be able to actuate relevant ESFs to mitigate such initiating events.

2.3 Identify the mitigation systems requiring DAS actuation

According to the descriptions in sections 2.1 and 2.2, the design of DAS should include 2 functions. One is to provide a backup reactor trip when PMS fails to shut down the reactor to lower the probability of ATWS, and the other is to provide a diverse actuation of ESF to mitigate 6 initiating events as described before.

For the first function, when PMS fails to shut down the reactor, DAS is considered to provide a backup reactor trip function, and according to the requirements of reactivity control and the Reactor Coolant System (RCS) pressure control during reactor shutdown process, the DAS actuation functions should include:

1) Reactor trip, e.g. Control Rod Drive Mechanism (CRDM) trip or Motor Generator Set (MGSET) trip
2) Turbine trip, to control RCS peak pressure value during ATWS
3) Passive Residual Heat Removal System (PRHR) and Incontainment Refueling Water Storage Tank (IRWST) recirculation check valve, to remove residual heat and control RCS peak pressure during ATWS
4) Core Makeup Tank (CMT) and Reactor Coolant Pump (RCP) trip, to control reactivity and makeup water storage by injecting boron water into RCS

The second DAS actuation function could be illustrated by an example of the TRANS event, which includes general transient events as turbine trip or spurious reactor trip. During this event, main feedwater flows into Steam Generator (SG) and removes the residual heat from SG secondary side. Promptly after turbine trip, reactor trip signal will be generated and the control rods will drop into reactor core. For the condition that both main feedwater and startup feedwater are failure, the water level in SG secondary side will decrease continually, and the residual heat will be removed from RCS by PRHR or feed-bleed cooling method. During this process, residual heat will be removed from RCS to containment, and the Passive Containment Cooling System (PCS) need to be actuated, and act as an ultimate heat sink that removes heat to environment.

According to the specific design and the event tree analysis, it can be concluded that lower CDF from this particular event can be achieved if certain ESF actuations are more reliable, such as PRHR and IRWST gutter isolation valves, CMT, RCP trip, Automatic Depressurization System (ADS), IRWST gravity injection, containment isolation, water recirculation to RPV from the reactor cavity (RECIRC), PCS, and etc.

By using the same analysis method that is described above, the systems that need DAS actuation in other 5 initiating events could also be identified. Besides the DAS functions as a backup for PMS, all the mitigation systems that need DAS actuation are listed as follows:

1) Reactor trip
2) Turbine trip
3) Opening PRHR valves and closing IRWST gutter isolation valves
4) CMT actuation and RCP trip
5) Opening ADS valves
6) IRWST gravity injection
7) Opening containment recirculation valves
8) Opening PCS valves

3. Identify protection signals of DAS to actuate the corresponding systems

The emergency reactor trip and ESF that need DAS actuation are identified in the previous sections, while identifying corresponding protection signals will be stated in this section. The identification process of DAS protection signals will refer to former description of initiating events and their accident sequences, and also will refer to the parameter signal sets of PMS on reactor trip and ESF.

Taking DAS actuation function on reactor trip and turbine trip as an example, loss of secondary heat sink, such as loss of main feedwater, and RCS LOCA are credited. Based on the relevant accident sequences and PMS protection signal configuration, the event mitigating process could be identified. As for mitigating loss of main feedwater, it requires SG wide range low water level signal to actuate reactor trip (e.g. CRDM or MGSET trip), turbine trip, PRHR (with closure of IRWST

gutter valves) and CMT (with RCP trip). As for RCS LOCA, it requires pressurizer low water level signal to actuate reactor trip, turbine trip and CMT (with RCP trip).

Considering all the accident sequences of the selected initiating events, the DAS actuation protection signals are finally determined, which include PRHR and IRWST gutter isolation valves, CMT, RCP trip, ADS IRWST gravity injection, containment isolation, RECIRC and PCS. And more detail information is listed in Table.2.

Moreover, as for the 6 initiating events that are described in this paper, it is considered that PMS or DAS will actuate PRHR to mitigate accident during loss of active heat sink conditions. As for totally loss of heat sink case, it is designed to remove residual heat in a mode of feed-bleed cooling from RCS primary side, which is realized by opening ADS valves and later IRWST injection, and recirculation valves. But，considering that the frequency of total loss of heat sink event is very low, and meanwhile spurious open the squib valves will directly lead to a loss of RCS pressure boundary condition and may cause a very serious accident consequence. It should be designed to prevent such spurious actuation events from happening as far as possible. So, only manual actuation by DAS on such systems and valves is considered, and the DAS manual actuation signal refers to PMS automatic actuation signal and follows in Emergency Operation Procedure (EOP). Except for conditions mentioned above, all other DAS actuation signals are set to be automatic, and manual actuations will be considered as backup when automatic actuation fails. The relevant DAS actuation set is listed in Table.2.

4. Plant risk with DAS

The relation between DAS protection signals and corresponding systems are listed in Table.3, and a practical design condition from a particular nuclear power plant is also shown in this table[2]. It should be noted that this paper does not analyze the case of DAS actuation on mitigating systems (such as hydrogen igniters) during severe accident. However, compared with the practical design condition in other parts, the analysis result in this paper is basically consistent with that of actual design, which particularly in terms of the design on reactor trip and ESF actuation that may relate to core damage. Although there is a slight difference in the design of the newly added DAS actuation on containment isolation and PCS under signal of containment high pressure, this difference is thought to be reasonable from the view of analysis process. This signal could provide further protection on the integrity of containment in case of LOCA with higher break size condition or secondly side pipe break accident.

Refer to the analysis result above and upgrade the basic PSA model with all the considerations of DAS actuation on protection systems, the CDF that is concerned with each of initiating event could then be calculated, and the results are listed in Table.4. As a matter of fact that DAS is not based on software and have much diversity from PMS and PLS, it could provide an effective backup when PMS and PLS fail due to software and hardware CCF. DAS could not only reduce the probability of ATWS, but also increase the reliability on actuation of relevant ESF that are needed for mitigating abnormal events. In terms of 6 selected initiating events TRANS, LMFW, LCCW, LCOND, LMFW1and LOSP, DAS lowers the CDF contribution from each of them to an extent less than limited CDF criterion. And as for other kinds of initiating events, DAS also lowers their corresponding CDF contribution. As a result, the total CDF of the nuclear plant decreased to a very low level.

5. Conclusion

By measuring the CDF results caused by internal events at power, PSA was applied to define the systems that require DAS to provide protection function, and corresponding protection signals are identified through accident sequence analysis.

Reference

[1] U.S. Nuclear Regulatory Commission Regulations: Title 10, Code of Federal Regulations, 50.62: Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants，10 CFR 50.62，U.S. NRC.
[2] AP1000 Probabilistic Risk Assessment, APP-GW-GL-022, Rev.8, Westinghouse Electric Company LLC, 2004.

Table 1 CDF Contributions for Each IE (Without DAS)

No.	Initiating Events		Frequency (1/ry)	CDF (1/ry)
1	IE-LLOCA	Large LOCA	5.04E-06	4.46E-08
2	IE-SPADS	Large Spurious ADS Actuation	5.40E-05	2.46E-08
3	IE-MLOCA	Medium LOCA	4.36E-04	2.53E-08
4	IE-CMTLB	Core Makeup Tank Line Break	9.31E-05	5.88E-09
5	IE-SI-LB	Safety Injection Line Break	2.12E-04	9.99E-08
6	IE-SLOCA	Small LOCA	5.00E-04	2.83E-08
7	IE-SGTR	Reactor Coolant System Leakage	3.88E-03	6.97E-08
8	IE-PRSTR	Passive RHR Tube Rupture	1.34E-04	2.50E-09
9	IE-RCSLK	Steam Generator Tube Rupture	6.20E-03	1.13E-08
10	IE-RV-RP	Reactor Vessel Rupture	1.00E-08	1.00E-08
11	IE-ISLOCA	Interfacing Systems LOCA	5.00E-11	5.00E-11
12	**IE-TRANS**	**Transient with MFW**	**1.40E+00**	**1.92E-06**
13	IE-POWEX	Loss of Reactor Coolant Flow	4.50E-03	8.72E-09
14	**IE-LMFW**	**Loss of Feedwater to One Steam Generator**	**3.35E-01**	**4.79E-07**
15	IE-LRCS	Core Power Excursion	1.80E-02	2.47E-08
16	**IE-LCCW**	**Loss of Component Cooling/ Service Water**	**1.44E-01**	**1.97E-07**
17	IE-LCAS	Loss of Main Feedwater	3.48E-02	4.88E-09
18	**IE-LCOND**	**Loss of Condenser**	**1.12E-01**	**1.89E-07**
19	**IE-LMFW1**	**Loss of Compressed Air**	**1.92E-01**	**2.64E-07**
20	**IE-LOSP**	**Loss of Offsite Power**	**1.20E-01**	**2.16E-07**
21	IE-SLB-D	Main Steam Line Break Downstream of the MSIV	5.96E-04	7.91E-09
22	IE-SLB-U	Main Steam Line Break Upstream of the MSIV	3.72E-04	5.07E-09
23	IE-SLB-V	Main Steam Line Stuck Open Safety Valve	2.39E-03	3.28E-08
24	IE-ATWS	ATWS – No MFW	4.81E-01	9.27E-08
25	IE-ATW-S	ATWS – SI events	1.48E-02	1.09E-08
26	IE-ATW-T	ATWS – With MFW	1.17E+00	1.40E-08

Table 2 Functions and Signals that Actuated by DAS

DAS Actuation on Mitigation System	Corresponding Protection Signal	Remarks
1) Reactor trip	SG wide range low water level or pressuizer low water level	Auto or Manual
2) Turbine trip	SG wide range low water level or pressuizer low water level	Auto or Manual
3) PRHR	SG wide range low water level, or RCS hot leg high temperature	Auto or Manual
4) IRWST gutter isolation	SG wide range low water level, or RCS hot leg high temperature	Auto or Manual
5) CMT	SG wide range low water level or pressuizer low water level	Auto or Manual
6) RCP trip	SG wide range low water level or pressuizer low water level	Auto or Manual
7) Open ADS valves	Refer to monitor display (e.g. PMS display CMT low water level signal), or follow EOP instruction	Manual
8) IRWST gravity injection	Refer to monitor display (e.g. PMS display CMT low water level signal), or follow EOP instruction	Manual
9) RECIRC	Refer to monitor display (e.g. PMS display CMT low water level signal), or follow EOP instruction	Manual
10) Containment isolation	Containment high temperature or high pressure	Auto or Manual
11) Actuation on PCS	Containment high temperature or high pressure	Auto or Manual

Table 3 Signals and Functions that Actuated by DAS

Protection Signals	Identified ESF Actuation from Analysis Conclusion	ESF Actuation Set of a Practical Nuclear Plant
SG wide range low water level	1) Reactor trip 2) Turbine trip 3) PRHR 4) IRWST gutter valve isolation 5) CMT 6) RCP trip	1) Reactor trip 2) Turbine trip 3) PRHR 4) IRWST gutter valve isolation 5) CMT 6) RCP trip
Pressurizer low water level	1) Reactor trip 2) Turbine trip 3) CMT 4) RCP trip	1) Reactor trip 2) Turbine trip 3) CMT 4) RCP trip
RCS hot leg high temperature	1) PRHR 2) IRWST gutter valve isolation	1) PRHR 2) IRWST gutter valve isolation
Containment high temperature	1) Containment isolation 2) PCS	1) Containment isolation 2) PCS
Containment high pressure	1) Containment isolation 2) PCS	N/A
Manual	1) Reactor trip 2) Turbine trip 3) PRHR 4) IRWST gutter valve isolation 5) CMT 6) RCP trip 7) Open ADS valves 8) IRWST gravity injection 9) RECIRC 10) Containment isolation 11) PCS	1) Reactor trip 2) Turbine trip 3) PRHR 4) IRWST gutter valve isolation 5) CMT 6) RCP trip 7) Open ADS valves 8) IRWST gravity injection 9) RECIRC 10) Containment isolation 11) PCS 12) Actuation on hydrogen igniter

Table 4 CDF Contributions for Each IE (With DAS)

No.	Initiating Events		Frequency (1/ry)	CDF (1/ry)	CDF Decrease (%)
1	IE-LLOCA	Large LOCA	5.04E-06	4.46E-08	0%
2	IE-SPADS	Large Spurious ADS Actuation	5.40E-05	2.46E-08	0%
3	IE-MLOCA	Medium LOCA	4.36E-04	1.43E-08	43%
4	IE-CMTLB	Core Makeup Tank Line Break	9.31E-05	3.30E-09	44%
5	IE-SI-LB	Safety Injection Line Break	2.12E-04	9.33E-08	7%
6	IE-SLOCA	Small LOCA	5.00E-04	1.60E-08	43%
7	IE-SGTR	Reactor Coolant System Leakage	3.88E-03	1.28E-08	82%
8	IE-PRSTR	Passive RHR Tube Rupture	1.34E-04	5.98E-10	76%
9	IE-RCSLK	Steam Generator Tube Rupture	6.20E-03	2.61E-09	77%
10	IE-RV-RP	Reactor Vessel Rupture	1.00E-08	1.00E-08	0%
11	IE-ISLOCA	Interfacing Systems LOCA	5.00E-11	5.00E-11	0%
12	IE-TRANS	Transient with MFW	1.40E+00	3.55E-09	100%
13	IE-POWEX	Loss of Reactor Coolant Flow	4.50E-03	1.49E-09	83%
14	IE-LMFW	Loss of Feedwater to One Steam Generator	3.35E-01	8.61E-10	100%
15	IE-LRCS	Core Power Excursion	1.80E-02	4.31E-11	100%
16	IE-LCCW	Loss of Component Cooling/ Service Water	1.44E-01	3.96E-10	100%
17	IE-LCAS	Loss of Main Feedwater	3.48E-02	1.79E-10	96%
18	IE-LCOND	Loss of Condenser	1.12E-01	1.03E-09	99%
19	IE-LMFW1	Loss of Compressed Air	1.92E-01	5.54E-10	100%
20	IE-LOSP	Loss of Offsite Power	1.20E-01	1.37E-09	99%
21	IE-SLB-D	Main Steam Line Break Downstream of the MSIV	5.96E-04	1.40E-11	100%
22	IE-SLB-U	Main Steam Line Break Upstream of the MSIV	3.72E-04	9.35E-11	98%
23	IE-SLB-V	Main Steam Line Stuck Open Safety Valve	2.39E-03	8.09E-10	98%
24	IE-ATWS	ATWS – No MFW	4.81E-01	8.05E-10	99%
25	IE-ATW-S	ATWS – SI events	1.48E-02	1.37E-10	99%
26	IE-ATW-T	ATWS – With MFW	1.17E+00	4.50E-12	100%