CrossMark

Success criteria analysis in support of probabilistic risk assessment for nuclear power plants: application on SGTR accident

Seyed Mohsen Hoseyni[1] · Kaveh Karimi[1] · Seyed Mojtaba Hoseyni[1] ·
Meisam Mohammadnia[1]

Abstract Success criteria analysis (SCA) bridges the gap
between deterministic and probabilistic approaches for risk
assessment of complex systems. To develop a risk model,
SCA evaluates systems behaviour in response to postulated
accidents using deterministic approach to provide required
information for the probabilistic model. A systematic
framework is proposed in this article for extracting the
front line systems success criteria. In this regard, available
approaches are critically reviewed and technical challenges
are discussed. Application of the proposed methodology is
demonstrated on a typical Westinghouse-type nuclear
power plant. Steam generator tube rupture is selected as the
postulated accident. The methodology is comprehensive
and general; therefore, it can be implemented on the other
types of plants and complex systems.

1 Introduction

Probabilistic safety assessment (PSA) is a powerful tool
for quantitative estimation of risk and examination of
process safety in different industries. This methodology is
first introduced in nuclear power plant (NPP) industry [1].
It appealed major attention after the TMI (Three Mile
Island) accident in 1979 [2]. PSA was extensively used

thereafter in nuclear industry [3–8], matured in aerospace
industry [9] and then used in other industries [10–13].
Nowadays, following Fukushima accident, PSA method-
ology and its application is attracting much more attention
[14].

In general, triple risk questions are addressed in the PSA
methodology, i.e., "What can go wrong? What is the
likelihood of that happening? What are the consequences?"
[15]. Deterministic evaluation of the physical phenomena
helps PSA to answer the first question, mainly for external
events [16]. However, it plays the major role in answering
the third question for postulated accidents and unmitigated
scenarios leading to severe accidents [17]. Our main focus
here is on the third question which also deals with human
errors, for which the human reliability analysis (HRA)
analyst should know how much time is available for the
specific action to be performed [18–20].

The elements of a comprehensive Level 1 PSA are
demonstrated in Fig. 1. In this process, success criteria
analysis (SCA) provides PSA with supportive thermo-hy-
draulics (TH) calculations. It tries to answer a set of
questions needed by the PSA experts for developing a
high-quality PSA. Strictly speaking, SCA should be per-
formed by TH calculations in order to confirm PSA
assumptions in the following areas:

- Accident sequence modelling (what are the end states
  in event trees?)
- System modelling (what are the conditions for the success
  of systems/functions appeared in the event trees?)
- Human reliability analysis (how much time does the
  operator have to perform the intended task?)

To do so, the plant behaviour is predicted using the
insights gained from thermo-hydraulics calculations for

✉ Seyed Mohsen Hoseyni
  mohsenhoseini59@gmail.com; m.hoseini@srbiau.ac.ir

[1] East Tehran Branch, Islamic Azad University, Tehran, Iran

Fig. 1 Elements of a comprehensive Level 1 PSA
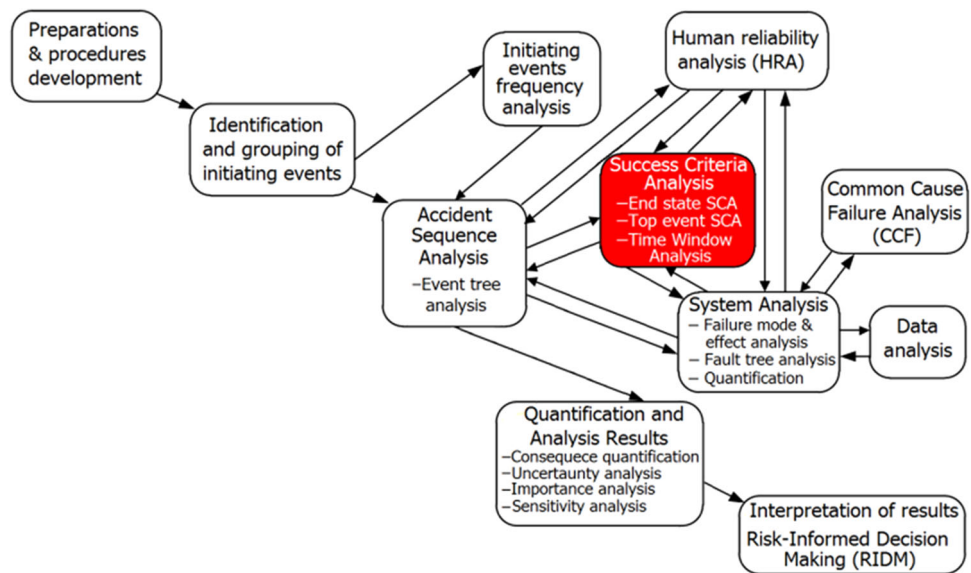
particular scenario. Normally, after development of an event tree by PSA analyst (through expert judgment), the TH results are used as an evidence to confirm (or reject) PSA assumptions. These specific PSA supportive TH calculations are entitled success criteria analysis and are the main tool for the development of event trees in a complex system.

The article is organized as follows. In Sect. 2, challenges facing SCA are reviewed. In Sect. 3, a review on common approaches is provided. Section 4 discusses the necessity for the consideration of containment role in definition of PSA core damage. A methodology is proposed in Sect. 5 for effective SCA in support of PSA. Section 6 is devoted to the application of the proposed methodology on steam generator tube rupture (SGTR) accident in a typical pressurized water reactor (PWR)-type NPP. The results are discussed in Sect. 7, and the concluding remarks are in Sect. 8.

2 Challenges in SCA

The following challenges are crucial for performing an effective SCA as a part of PSA in NPP applications.

2.1 Exact definition of end state

Success criteria are directly extracted from deterministic safety assessment (DSA) calculations in terms of the required configuration for critical safety systems. As the first step in SCA, acceptance criteria should be established clearly to provide a quantitative measure for interpreting the consequence of a given scenario [21]. Meeting acceptance criteria ensures that the following safety functions are

fulfilled in a given NPP: reactivity control, reactor coolant system (RCS) pressure control, RCS inventory control, decay heat removal and containment heat removal.

The key question in the risk model structure (event tree branches) is how to provide a quantitative measure to categorize a given scenario with particular configurations of the front line systems into success or failure. For an NPP, ASME/ANS PRA standard [22] defines the failure end state, i.e., core damage, as "uncovery and heat-up of the reactor core to the point at which prolonged oxidation and severe fuel damage are anticipated and involving enough of the core, if released, to result in offsite public health effects"; however, no consensus quantitative definition exists in the literature.

2.2 Contribution of TH uncertainties to the PSA uncertainties

Reference [23] discusses the uncertainty sources and the methods to treat them. One challenge in this area is model uncertainty assessment with limited researches available [24].

There are approaches for treatment of this uncertainty source in PSA model [25–27]; however, they are limited to the academic artwork and their industrial implementation is not present. There are misunderstandings about this concept in the technical community. For example, Ref. [28] claims on the introduction of an approach to quantify the effect of TH uncertainty on core damage frequency (CDF). The relation of TH uncertainty to accident sequences modelling and PSA, as declared in this article, is criticized by the comments provided in Ref. [29].

Here this challenge is mentioned to highlight its importance and pointing out that the extension of the

research in success criteria analysis would be quantification of TH uncertainty contribution to the PSA total uncertainty.

2.3 Tools for SCA

TH calculations in support of PSA involve a wide range of complicated phenomena and their dynamic interaction. They must be taken into account for prediction of the plant behaviour. Therefore, use of complex computer codes is inevitable in the process. However, for the selection of computer code, three factors must be assessed: (1) availability of verified and validated thermo-hydraulics code, (2) PSA team capabilities and (3) PSA scope.

2.4 Development of a qualified deterministic model

Development of a qualified deterministic model is the foundation for SCA. For TH codes with complex structure and complicated input models, recommendations encourage users to follow quality assurance procedures and verification and validation of input deck by independent reviewers. The procedure suggested by IAEA SRS-23 [30] used for development of the base case for the deterministic model. Large number of calculations is needed for the extraction of success criteria, as a time-consuming process. Besides, requirements of PSA models are less sophisticated than those of the licensing analyses. Therefore, it is suggested to use coarse nodalization for the plant model. The analyst must assure that this coarse nodalization approach is accurate enough for this purpose. This is formally done through verification and validation of the plant model.

Modelling must be performed by taking the steps given in Fig. 2, a general flow chart illustrating this procedure. These steps need not always be sequential; some can be carried out in parallel.
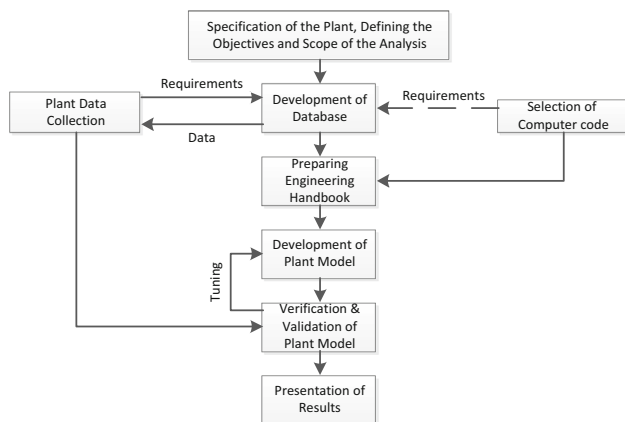

Fig. 2 Flow chart of basic steps in model development

2.5 Discussion on the requirements for SCA

ASME/ANS PRA standard [31] has established itself as the main framework for development of recent PSA studies in NPPs. Based on this standard, any expert judgment must be avoided in the process of SCA. Instead, it is required to extract all data from the results of best estimate TH calculations. The analysis must be plant specific and free from conservative assumptions. IAEA TECDOC-1511 [32] is another reference which addresses the requirements for a qualified PSA.

NUREG 1953 [21] shows the implementing of standard requirements for SCA. Table 1 in the Regulatory Guide 1.200 [22] compares the attributes of the analysis required by the ASME PRA standard with those of the so-called SPAR model.

3 Review of common PSA approaches

The use of design information, expert judgement and design basis accident (DBA) results are inevitable in SCA of the PSA model, especially in the case that no other data are present. In this section, we critically review the approaches used by some past PSAs (e.g. Ref. [33]) and discuss how the sole reliance on these approaches could end up with technical errors. What we are going to recommend is to use plant-specific data extracted from the detailed SCA whenever there is no technical limitation.

3.1 Approach 1, use of design information

A first step in the assessment of front line success criteria is to review the relevant design data. However, criteria derived from design information turn to be overly conservative. More realistic success criteria are obtained by performing a number of best estimate TH or physical calculations. While very conservative success criteria are initially derived from design information, it should be recognized that additional analyses are necessary to support realistic success criteria for the final risk models.

Table 1 Main properties of the PWR under study

Parameters	Value
Reactor full power (MW)	3100.0
RCS pressure at steady state (MPa)	15.41
Core coolant mass flow rate(kg/s)	6938.0
Hot-leg temperature at steady state (K)	313.6
Cold-leg temperature at steady state (K)	283.8

3.2 Approach 2, use of expert judgment

In addition to the front line success criteria, any other special conditions imposed by the initiating events must be assessed and recorded. Such special conditions may have effects on support systems, symptoms displayed to the operators, automatic actuation of the systems and/or the potential for inducing dependent failures. Considering complexity of the accidents and dependency of the mitigating systems, the judgments by experts could not be reliable for the extraction of success criteria. Although this approach is unavoidable for under design plants and it is sometimes useful in early phases of PSA development, by the accomplishment of the design, these assumptions should be updated using realistic evidences of TH calculations.

3.3 Approach 3, use of TH calculations for DBA

Performing DBA analyses is mandatory for each NPP to be built. TH calculations are normally available in Chapter 15 of final safety analysis report (FSAR) of the plants. In most cases, the calculations are based on conservative assumptions; therefore, using these calculations for extraction of success criteria could reduce the technical quality of PSA. Another deficiency is that DBA analyses are limited to one or a few sequences for every initiating event which makes it non-informative for other sequences of the event tree. Moreover, the assumptions made in the modelling process may be different from those of PSA (e.g. the initiating events). It is emphasized that in general the calculations do not reveal sufficient data for PSA needs, though they provide some useful information for some cases.

4 The containment role in definition of core damage

PSA analyst might neglect the containment role in Level 1 PSA as a result of misjudgement. Since "core damage" is defined based on quantitative parameters like PCT (peak clad temperature) in the SCA process, some PSAs neglect the role of containment in the definition of success criteria (see Sect. 2.1). Although this approach is acceptable in most cases, for some scenarios like "feed and bleed" and loss of coolant accident (LOCA), it needs special treatment. For cases that containment heat removal function is not available, the PCT might be within the acceptable limit and much below 1204 °C criteria. However, the containment pressure may rise up continuously. This condition is predicted by TH code calculations, and the results are illustrated for a typical PWR in Fig. 3. Both cases can be interpreted as successful sequences regarding PCT limit; however, this is believed to be misleading. In the case of containment pressure build-up, there are two possibilities:

Possibility 1 Containment will remain intact despite of passing the design pressure If this is the case, the water temperature inside containment will grow gradually. In primary feed and bleed (PF&B) process, emergency core cooling system (ECCS) injects water to the core. This water passes over the core, removes the decay heat and finally discharges to the containment. In long-term, if the containment heat removal function remains irrecoverable, water temperature [recirculation water in old designed PWR and In-containment refuelling water storage tank (IRWST) in new designs] will exceed the design temperature of the ECCS pumps. This may result in the ECCS pumps degradation. The outcome will be termination of PF&B process and finally core damage.

Possibility 2 Containment fails by exceeding the design pressure If the containment integrity is jeopardized by passing the design pressure, high-pressure and high-temperature atmosphere of the containment will be exposed to the ambient pressure (approximately 1 bar). In this case, the containment water will be imposed to boil off and flashing at the instant of containment failure. Again here, the PF&B process will be terminated because of evaporation of source water inside containment and the core will be degraded.
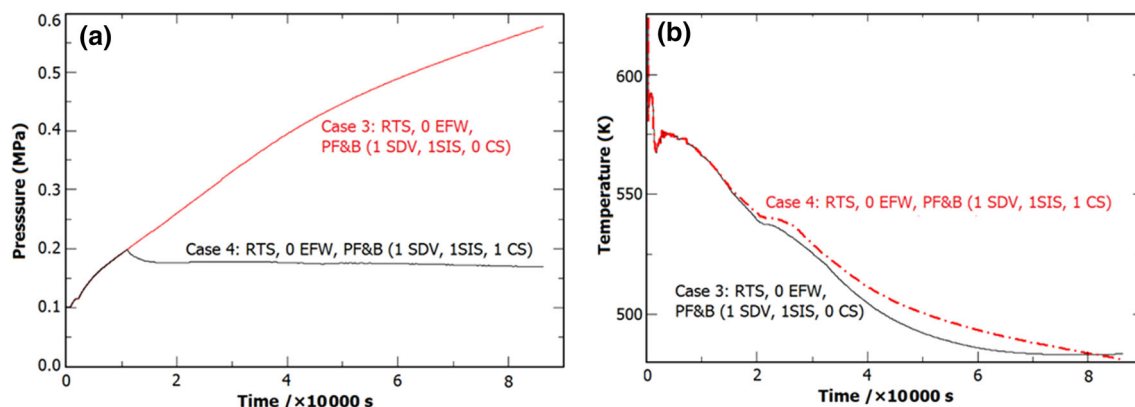

Fig. 3 Containment pressure in PF&B process (**a**) and the hot cell cladding temperature profile (**b**)

5 Proposed methodology

5.1 Elements of the proposed methodology

5.1.1 Definition of core damage

NUREG-1953 [22] studies the issue of core damage definition and proposes a number of possible core damage surrogates including collapsed water level on top of active fuel, core exit temperature greater than 1200 °F and PCT greater than 2200 °F. Based on this assessment, on merits and deficiencies of different surrogates on PWR and BWR-type reactors, PCT greater than 1204 °C (2200 °F) is suggested as the quantitative measure for the core damage definition. However, based on the discussions provided in Sect. 4, to include the containment role, we propose to set the criteria for core damage as occurrence of PCT greater than 1204 °C or containment pressure greater than containment pressure capacity.

5.1.2 Qualified deterministic model development

Since deterministic safety analysis (DSA) is not reliable without validation of the results, it is necessary to qualitatively analyse the developed model by the process suggested in Sect. 2.4. The modelling error is as a proper criterion for the qualification process. A model is considered qualified whenever its error is below the acceptable error suggested by the standards like IAEA SRS-23 [30]. In this step, for the development of qualified MELCOR code, the procedure in Fig. 4 is suggested. After ensuring the qualification and soundness of the considered code, building process of the volume network is carried out via a qualified user. This process is performed using power plant design data under normal steady-state conditions of the plant. The results obtained from running the model are analysed in MELCOR code. In fact, by comparing the results of TH parameters obtained from model with design values, the error originated from modelling is quantified.

Details of qualification process in the proposed methodology will be elaborated in Sect. 6.2 while demonstrating the SCA application for SGTR accident.

5.2 Flow chart of methodology for effective SCA

Although the methodologies are known for industrial and technical communities, a systematic explanation of the procedure for SCA is missing in the literature. To fill the gap in this area, a procedure is developed in compliance with ASME/ANS PRA standard [31]. Steps for an effective SCA are depicted in Fig. 5. It shows three tasks of the proposed methodology in different colours.
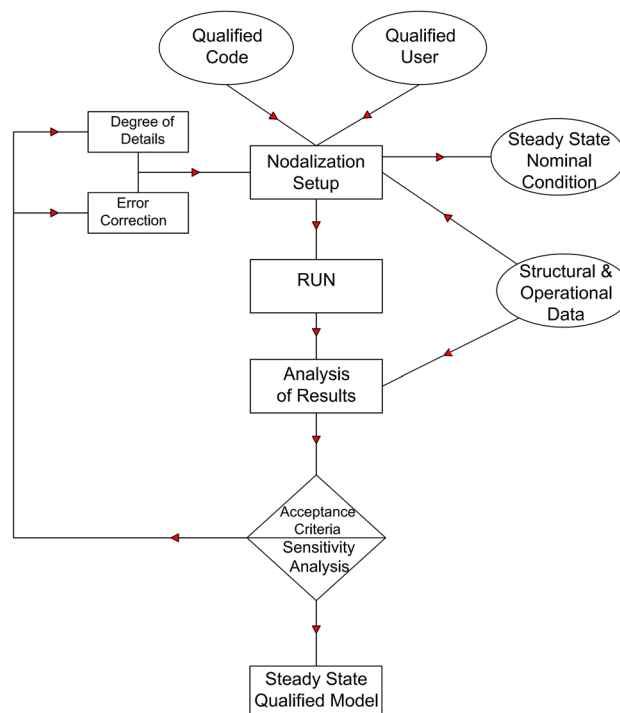

Fig. 4 Procedure for confirming qualification and validity of model

Task 1 Review of the proposed event tree and assumptions in the PSA model This task includes review of initiating event group and selection of the representative event. The initial event tree, proposed by the PSA team, is studied first. Meanwhile, the progression of the accident sequences and event tree top events is clearly identified for the modelling purposes.

Task 2 Implementation of PSA assumption to deterministic plant model In the second task, insights from the first task are implemented into the DSA model of the plant which is the basis for supportive TH calculations. The first branch of each event tree represents the sequence in which all of the required mitigating systems are available. In this task, the first sequence is analysed by selected TH code (based on Sect. 2.3) and the results are interpreted by an expert panel. For further assessment, the DBA results (if available) can be used for confirmation of the results; however, the analysts must be aware of the differences in the assumptions of these approaches.

Task 3 TH calculations and documentation of the results In this task, plant thermal/hydraulic analyses are performed for all sequences of the event tree. The code calculated TH results are used for the extraction of success criteria of each top event as well as prediction of the final consequence of each scenario. The minimum requirements of the systems are considered as the final success criteria.

Fig. 5 Flow chart of the
proposed methodology for SCA
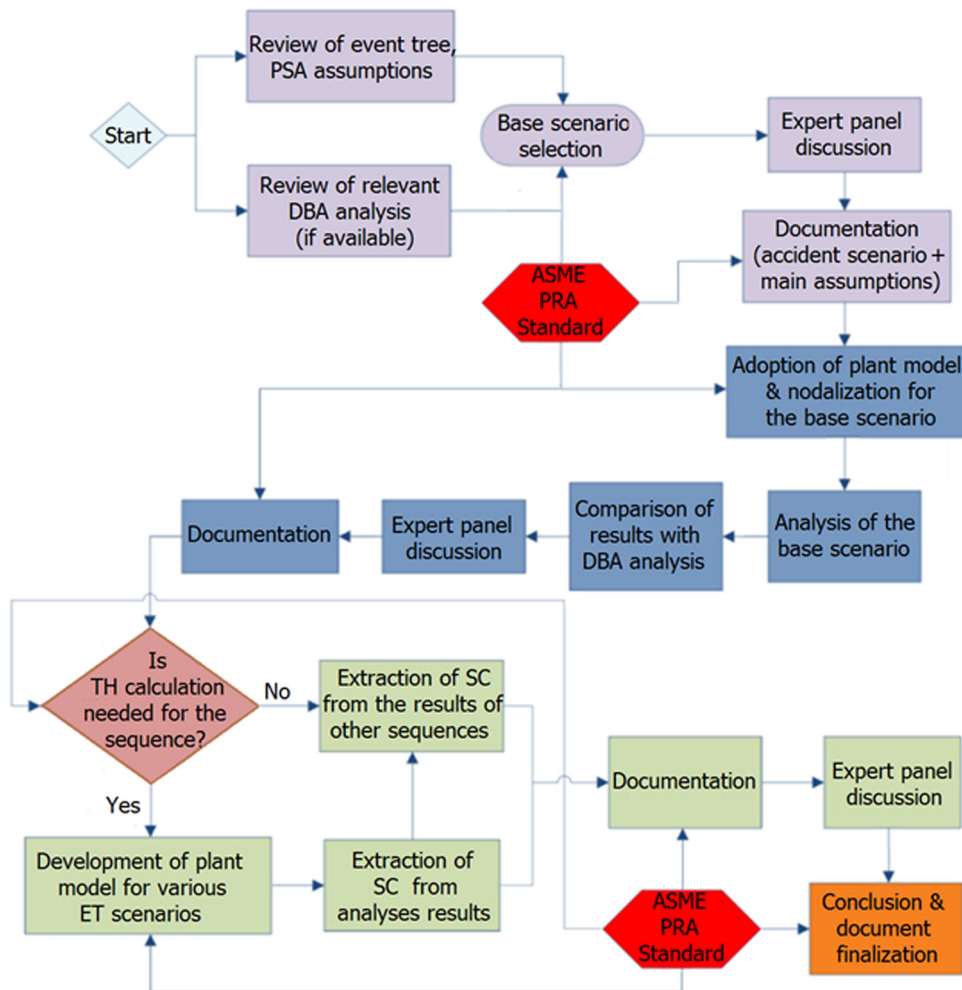
It is noteworthy to indicate that each task should undertake quality assurance procedure by fulfilment of the requirements in AMSE PRA standard. For each task, documentation is of crucial importance as depicted in the proposed flow chart. The box "expert panel discussion" stands for technical meetings devoted to each task of the methodology. In the technical meetings, experts of PSA and DSA teams review the results and draw conclusions.

6 SCA of SGTR

In the sequel, application of the proposed methodology is demonstrated on a real case for steam generator tube rupture accident in a typical Westinghouse-type PWR, with the specification provided in Table 1. First, the probabilistic model of the accident is introduced in a concise manner. Then, the proposed methodology is implemented on SGTR accident for the extraction of success criteria.

6.1 SGTR accident and its probabilistic model

SGTR is a small LOCA that has the potential to bypass containment and therefore is treated separately from LOCA. The main difference why the single steam generator tube rupture is handled separately from other more extensive leakages between the primary and the secondary loops is that in this case the operation of ECCS is not required or can be prevented by right operator actions. If the operators fail to depressurize the reactor coolant system in a timely manner, there is a high probability that water will be forced through main steam safety valves (MSSVs) on the steam line from the affected steam generator. The probability of MSSVs failure to reclose is estimated at ~ 1.0 (very high) for this condition. This will result in a non-isolable path from the RCS to the environment. The core uncovers once the entire content of the refuelling water storage tank is pumped through the broken steam tube.

The developed event tree for steam generator tube rupture accident is presented in Fig. 6, with assumptions of

The event tree headers (vertical column labels) are:

- Steam Generator Tube Rupture — SGTR
- Reactor Trip System 1)Other 2)LOOP — RTS
- Steam Generator Isolation — SGI
- 1)1/2 2)1/2 SLBO 3) 1/1 4)SGTR 5)ISGTR 6)PLOCCW 7)LOOP 8)SBO 9)LP REC 10) — EFW SHR
- Safety Injection System 1)1/4 2) 2/4 3)1/3 4)1/2 5) VSLOCA 6)LOOP 7) — SIS
- Operator Pressure Equalization of Primary and Secondary Sides — OPE
- Operator Depressurization of Primary side — OPD
- 2/4 Residual Heat Removal System — RHR
- RCS Deppresurization by SDVs 1)1/2 2)LOOP 3)LP REC 4)LODC — BLEED
- 1)1/2CSS2) 1/4CS/RHR3) 2/4CS/RHR4) 1/2CS/RH5)1/3CS/R — CS HR

No.	Freq.	Conseq.	Code
1	4.00E-03	OK	
2	1.61E-07	CD	OPE
3	3.57E-07	OK	SIS
4	2.34E-05	OK	EFW SHR
5	1.30E-09	CD	EFW SHR-CS HR
6	2.98E-07	CD	EFW SHR-BLEED
7	1.05E-08	CD	EFW SHR-SIS
8	1.91E-05	OK	SGI
9	9.87E-08	OK	SGI-RHR
10	7.41E-10	CD	SGI-RHR-CS HR
11	9.93E-10	CD	SGI-RHR-BLEED
12	7.81E-08	CD	SGI-OPD
13	1.70E-09	CD	SGI-SIS
14	4.41E-07	OK	SGI-EFW SHR
15	1.03E-09	CD	RTS

Fig. 6 Developed event tree for SGTR accident

(1) SGTR initiating event being as rupture of only one steam tube and (2) emergency feedwater (EFW) system actuation occurring before safety injection system (SIS). This is the reason that EFW SHR top event precedes the SIS top event in the event tree.

More explanation on the required safety functions for this event and their related safety systems is out of the scope of the current work. Reactor trip system (RTS) and EFWS perform reactivity control and decay heat removal, respectively. Moreover, since there is a break in steam tube side, RCS inventory needs to be controlled.

Figure 6 demonstrates 15 sequences of SGTR event tree, consisting of 5 OK and 10 CD sequences. In Sequences 1, 3, 4, 8 and 9, all required safety functions are fulfilled and the core is in safe and secured state. Due to the failure in RCS inventory control function, Sequences 2, 12 and 13 lead to core damage. In Sequences 6, 7, 11 and 14, failure of decay heat removal, via EFWS, residual heat removal (RHR) or PF&B, resulted in CD consequences.

Also failure of containment spray system (CS HR) in primary feed and bleed (PF&B) process ends up with CD in Sequences 5 and 10. RTS has failed in Sequence 15, and thus, core reactivity could not be controlled.

6.2 Development of deterministic model for simulation of SGTR accident

The procedure presented in Sect. 2.4 is implemented here. The hydraulic volumes and their associated flow paths are shown in Fig. 7. Reactor pressure vessel (RPV), downcomer, lower plenum, core, core bypass and upper plenum (including the upper head) are each represented by a single node. Front line systems are included in the model as well. Their modelling is completely in accordance with the assumptions of the plant PSA model. To summarize this work, the plant model includes: (1) primary loop and the connecting piping, (2) main steam system, (3) containment, (4) control logics and signals and (5) front line systems.
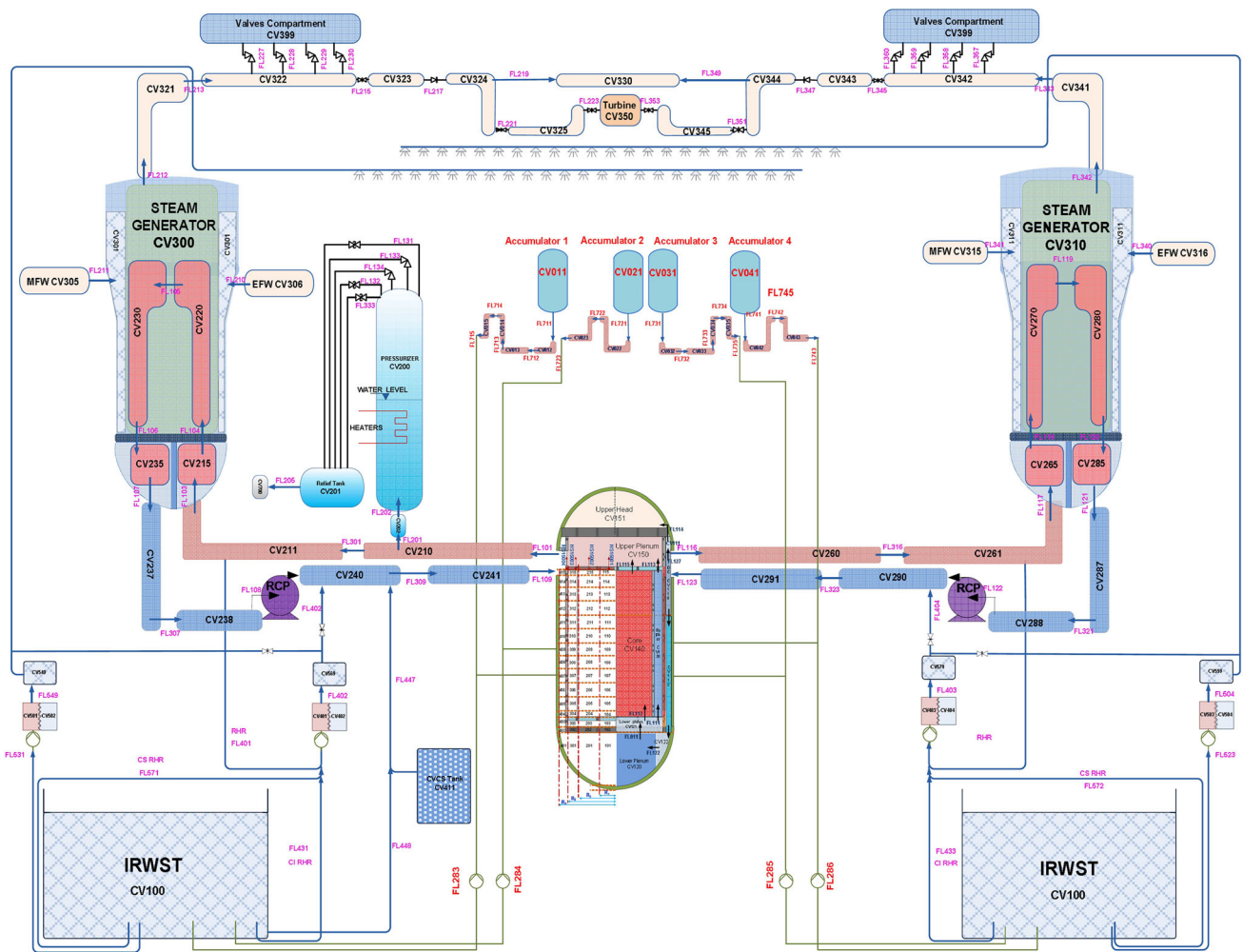
Fig. 7 Schematic of TH model nodalization for SGTR

Adopted nodalization is illustrated in Fig. 7. Break is located at top of the U-tubes and is modelled using two flow paths from one of the steam generators U-tubes to the secondary side of that steam generator.

The steady-state qualification includes different checks: one is related to the evaluation of the geometrical data and of numerical values implemented in the nodalization; the other one is related to the capability of the nodalization to reproduce the steady-state qualified conditions. Table 2 shows thermal hydraulic parameters. They are all checked against their designated values in design documents and are summarized in this table. For the geometrical values, the input deck has been rechecked to assure the plant nodalization. Thermal hydraulic parameters are all the output of the code and must be shown to have error values below the acceptable error.

Table 2 also summarizes the calculated parameters that are crucial for the qualification of the steady-state model. The steady-state parameters are given with their error calculated based on the plant design data. The errors are

below the acceptable errors, which confirms the credibility of steady-state model.

So, this model truly describes the plant steady-state conditions and can be the basis for deterministic calculations in the SCA.

6.3 SGTR scenarios for success criteria analysis

For the SCA of SGTR, assumptions are the same as those considered for the PSA accident sequence modelling. The first step of the methodology is to analyse the base scenario. For that we start with the evaluation of TH response of Sequence 1 in the event tree. The TH results confirmed Sequence 1 as a successful sequence; therefore, Case 1 in Table 3 is defined as second sequence of the event tree in order to find out the role of OPE (operator depressurization of primary system by MSDV) for mitigation of SGTR. In addition, the following questions must be answered by the deterministic evaluation of SCA:

Table 2 Design and modelling values and the acceptable errors

Items	Design value	Model value	Acceptable error	MELCOR model error
Primary mass flow rate (kg/s)	6938.0	6905.8	2.0%	0.46%
Steam generator secondary side steam mass flow rate (kg/s)	304.4	302.9	2.0%	0.49%
Steam generator primary side mass flow rate (kg/s)	3469.0	3454.8	2.0%	0.41%
Core bypass mass flow rate (kg/s)	277.0	273.2	10%	1.37%
Heat transfer from primary to secondary side (MW$_{th}$)	3100.0	3135.2	2.0%	0.46%
Hot-leg temperature at steady state (K)	586.75	586.82	0.5%	0.012%
Cold-leg temperature at steady state (K)	556.95	556.87	0.5%	0.014%
Steam generator secondary side pressure (MPa)	5.550	5.548	0.1%	0.036%
Pressurizer pressure(MPa)	15.520	15.517	0.1%	0.021%
RPV pressure loss (MPa)	0.199	0.201	10.0%	1.005%
Steam generator primary side pressure loss (MPa)	0.216	0.207	10.0%	4.17%
Pressurizer level (m)	16.227	16.222	0.05 m	0.005 m
Steam generator secondary side level (m)	17.605	17.601	0.1 m	0.004 m

- Is the termination of SIS or failure of this system, enough for the termination of the accident in Sequence 3?
- What goes wrong if SIS is under operation?
- How OPE can mitigate the accident in the case of SIS operation?
- What is the success criterion for EFW in the affected line?

These top events are studied in order to obtain minimum requirements of the systems under different configurations of the front line systems. For each of the sequences in the event tree, at least 1 MELCOR code calculation is performed.

Table 3 shows the 20 cases considered in SGTR success criteria analysis and determines for each case the configuration of different safety systems. It is noteworthy to add that Cases 16 and 17 consist of two scenarios, one with containment spray system and the other without it.

6.4 Results of selected thermal hydraulic calculations for SGTR analyses

The first sequences in Table 3 are devoted to the SCA for three top sequences of the proposed event tree (Fig. 6). Accordingly, if SIS is not available and the reactor is tripped (successful RTS), isolation of the steam generator and operation of one of EFWs in the intact line will eventuate in success (OK consequence in the event tree).

To find out success criteria, a number of calculations are performed and summarized in the following subsections. To explain the results in a concise manner, some selected calculations are elaborated; however, discussions are

provided to cover the whole 19 cases based on the deterministic results. Lines numbered 105–115 in the upcoming figures represent the axial levels of the core nodalization. Moreover, the symbol COR-TCL-XXX stands for the cladding temperature in the axial level XXX.

6.4.1 Case 1: RTS, SGI, 1 EFW, 0 CVCS, 4 SIS (Sequence 2 of the event tree)

In this case, we investigate whether 1 EFW system in conjunction with all trains of SIS can lead the sequence to the success end state or not. Results show that although the affected steam generator pressure remains in vicinity of the MSSV pressure set point, operation of the EFW in the intact steam generator makes the pressure to fall slowly down after almost 5 h.

For the whole mission time (24 h), leakage will be continued at a rate of 5.5 kg/s for each side of the break. As concluded from the results, the same amount of water is compensated by the 4 trains of SIS that are in operation. Leakage is not terminated for the whole mission time with SIS injection. These forms of the plant behaviour are akin to the PF&B process because continuous water is injected to the core by SIS system and this water is discharged to the containment by safety depressurization valves (SDVs). The difference here is that the RCS water is discharged to the environment instead of containment.

In this situation, decay heat removed from the core and claddings is quenched below 500 K at the end of mission time. The cladding temperature profile is illustrated in Fig. 8a, with the peak temperature being well below the acceptance criterion of 1204 °C for the whole mission time.

Table 3 Considered sequences for SGTR analysis

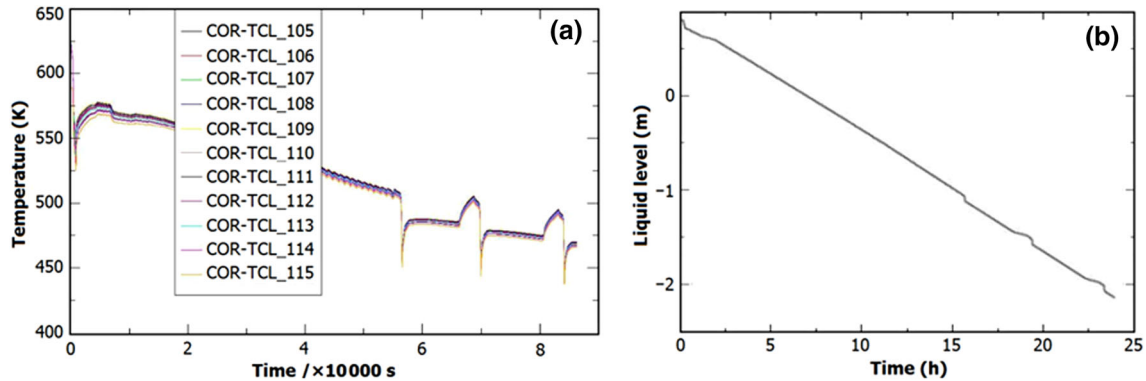| Case no.	Sequence no.	RTS	SGI	EFW SHR	SIS	CVCS	OPE	OPD	RHR	BLEED	CS
1	2	✔	✔	1	4	0	–	–	–	–	–
2	6	✔	✔	0	1	0	–	–	–	–	–
3	2	✔	✔	1	0	1	–	–	–	–	–
4	3	✔	✔	1	0	0	–	–	–	–	–
5	1	✔	✔	1	0	1	✔	–	–	–	–
6	1	✔	✔	0	0	1	✔	–	–	–	–
7	1	✔	✔	1	0	0	–	Single MSDV cooldown	–	–	–
8	4	✔	✔	0	1(F&B)	0	–	–	–	1(F&B)	1
9	7	✔	✔	0	0	0	–	–	–	–	–
10	5	✔	✔	0	1(F&B)	0	–	–	–	1(F&B)	0
11	14	✔	–	0	0	0	–	–	–	–	–
12	13	✔	–	1	0	0	–	–	–	–	–
13	12	✔	–	1	1	0	–	–	–	–	–
14	8	✔	–	1	1	0	✔	–	2	–	–
15	8	✔	–	1	1	0	✔	–	1	–	–
16	9	✔	–	1	1(F&B)	0	✔	–	0	1(F&B)	1
17	10	✔	–	1	1(F&B)	0	✔	–	0	1(F&B)	0
18	11	✔	–	0	0	0	–	–	–	–	–
19	14	✔	–	0	1(F&B)	0	–	–	–	1(F&B)	–
20	15	–	–	0	0	0	–	–	–	–	–

Fig. 8 Cladding temperature profile (**a**) and IRWST liquid level (**b**) for Case 1 of SGTR

Results show that although leakage is not terminated, even without OPE, the core damage will not occur for this sequence of the accident. We can deduce that if the water content of the in-containment refuelling water storage tank (IRWST) is enough for supplying water to the core by SIS, the sequence can be considered successful.

TH code result reveals that the liquid level of IRWST is at about half of its elevation by the end of mission time; therefore, the availability of supply water for SIS injection is guaranteed (Fig. 8b).

6.4.2 Case 2: RTS, SGI, 0 EFW, 1 SIS, 0 CVCS (sequence 6)

In this case, necessity of the EFW and the sufficiency of 1 train of SIS are studied. The results are the same as Case 1, meaning that operation of EFW system is not necessary for mitigating the accident. It confirms that even 1 train of SIS can compensate the water inventory loss from the break. Figure 9a illustrates the cladding temperature never exceeds 620 K for the 24 h analysis.
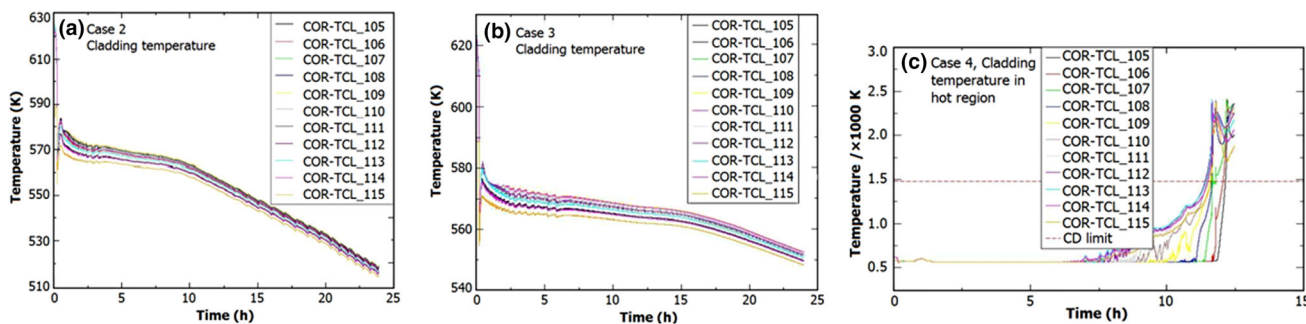
Fig. 9 Cladding temperature profiles in SGTR accident. **a** Case 2, **b** Case 3, **c** Case 4 (in hot region)

6.4.3 Case 3: RTS, SGI, EFW, 0 SIS, 1 CVCS (sequence 2)

This case is analysed to understand capability of chemical and volume control system (CVCS) for inventory control of the RCS. In other words, the purpose is to find whether CVCS can be used for the mitigation of the accident instead of SIS or not.

Results show that operation of CVCS compensates the leakage from primary to secondary side. Therefore, for inventory control, CVCS could be considered as an alternative system for SIS.

In this case, the cladding temperature falls well below the acceptance criteria, just like the previous case. Continuous discharge of RCS inventory to the secondary side in conjunction with CVCS injection to the RCS efficiently removes the decay heat of the core and reduces the cladding temperature below 560 K at the end of the mission time (Fig. 9b).

6.4.4 Case 4: RTS, SGI, 1 EFW, 0 SIS, 0 CVCS (sequence 3)

As the reference event tree of SGTR implies, in the case of SIS unavailability, the accident can be mitigated by RTS, SGI and EFW SHR (Sequence 3). In this case, the truth of this assumption will be assessed. Moreover, the necessity of inventory control function for the SGTR accident will be examined.

As shown in Fig. 9c, it is obvious that core damage is inevitable if the inventory control function fails. In this sequence, no inventory control is provided by CVCS and SIS to the core. This will result in the liquid level reduction in the core and finally to the core dry out. From Fig. 9c, the core will be damaged approximately 11 h after the SGTR initiation. Leakage from primary to secondary systems is reduced to negligible amounts; however, the steam release to the atmosphere will be continued.

Form the first four cases analysed, it can be deduced that the RCS inventory control is needed for mitigating the accident. Therefore, Sequence 3 of the event tree cannot lead to a successful end state. On the other hand, if SIS provides RCS inventory in a non-stop manner for the whole mission time, the leakage will not be terminated. For this case, the final state is ok regarding the PCT limit but the containment is bypassed. Also in this case even without EFW, CD will not happen.

6.4.5 Case 5: RTS, SGI, 1 EFW (0 EFW for Case 6), 1 CVCS, 0 SIS with OPE (sequence 1)

The obtained results show that following emergency operating procedure (EOP) by the operator, the core will be in safe and stable state. Leakage from primary to secondary system is terminated at the early stages of the accident scenario even before half an hour from the onset of the SGTR. The CVCS injection to the RCS is performed for early inventory control and is manually tripped by operator at 10000th second of the transient.

The clad temperature profile is given in Fig. 10. The secured and safe core is guaranteed by the low temperatures of 560 K that is well below the acceptance criteria. Further calculations for this sequence showed that without EFW (Case 6), the core will be damaged because the clad temperature will exceed the acceptance criteria of 1204 °C (Fig. 10b).

6.4.6 Case 7: RTS, SGI, 0 EFW, with Feed and Bleed, 1 CS/HR (sequence 4)

In this case, properties of feed and bleed process are under study (Sequences 4–7). If EFWs fail to do its function (secondary cooling is unsuccessful), the operators initiate PF&B process. Primary bleed (PBL) is initiated by operator, by opening the pressurizer safety depressurization valves (SDVs) in cooldown mode of operation in the relevant time window. After depressurization by bleeding, RCS pressure decreases to the SIS actuation set point and the "feed" process is initiated. In addition, containment spray heat removal (CS/HR) system is required for containment and IRWST cooling, hence preventing core damage.
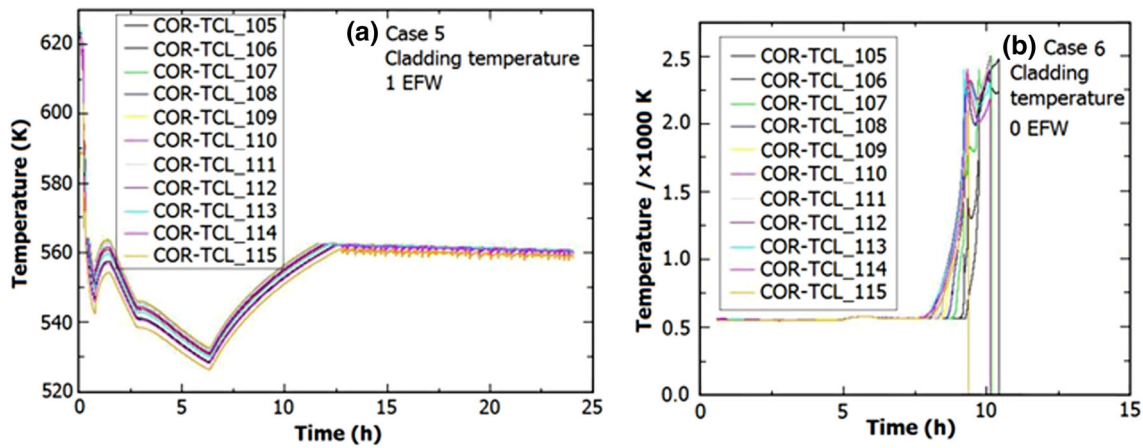
Fig. 10 Cladding temperature profiles for Case 5 (**a**) and Case 6 (**b**) of SGTR

Bleeding by operator starts at 3800th second of the calculations after unavailability of EFW. Cladding temperature as a function of time is given in Fig. 11a. The core is cooled and quenched at the end of mission time. PCT as the surrogate parameter for core damage is well below the acceptance criteria, and the sequence could be considered successful.

In the considered sequence, leakage cannot be terminated from the affected main steam line to the environment through MSSV valves. The reason is continuous injection of water by SIS and existence of pressure difference between primary side and affected steam generator.

6.4.7 Case 8: RTS, SGI, 0 EFW, 0 SIS (sequence 7)

Sequence 7 of the event tree indicates that successful steam generator isolation, failure of EFW and SIS will result in core damage. Calculations for Case 9 are performed to find out the final consequence of this configuration of the front line systems.

The result of TH calculation confirms the PSA assumptions for this scenario. As shown in Fig. 11b, about

5 h after the accident, core will be melted by exceeding the core damage limit.

6.4.8 Case 9: RTS, SGI, 0 EFW, F&B, 0 CS (sequence 5)

In this case, the necessity of the containment spray system is assessed, to study whether Sequence 5 of the event tree leads to a successful or failed end state.

By operation of the SDV, steam will flow to the containment from the pressurizer and cause a build-up of containment pressure. From all cases analysed, it is inferred that one train of containment spray suffices for meeting the acceptance criteria.

The results showed that even without containment spray system for the first 24 h of the accident, pressure of the containment is below 4.0 bar. Therefore, calculations were extended to 36 h. Case 9 resulted in failed containment at approximately 32 h after the transient initiation. Containment pressure changes are illustrated in Fig. 12.

In addition, loss of containment spray or any failure in the containment isolation may lead to vaporization of the hot inventory of IRWST, and consequently IRWST level
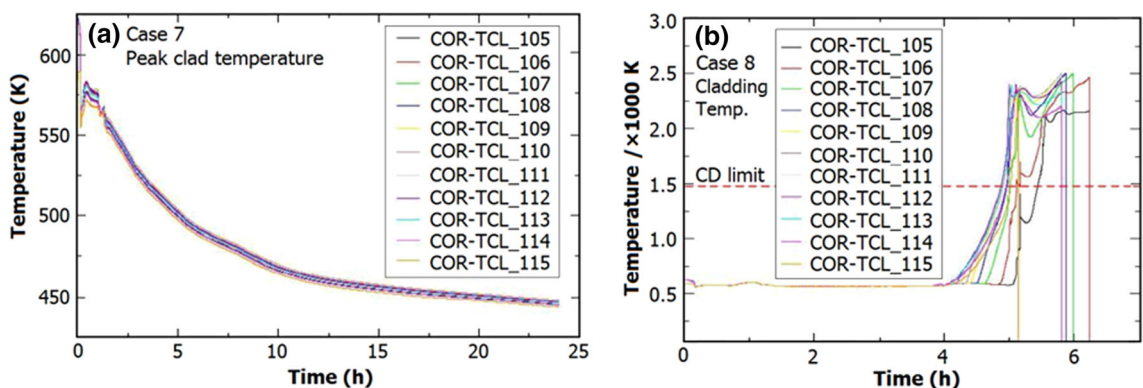

Fig. 11 PCT profile of Case 7 (**a**) and cladding temperature of Case 8 (**b**) of SGTR
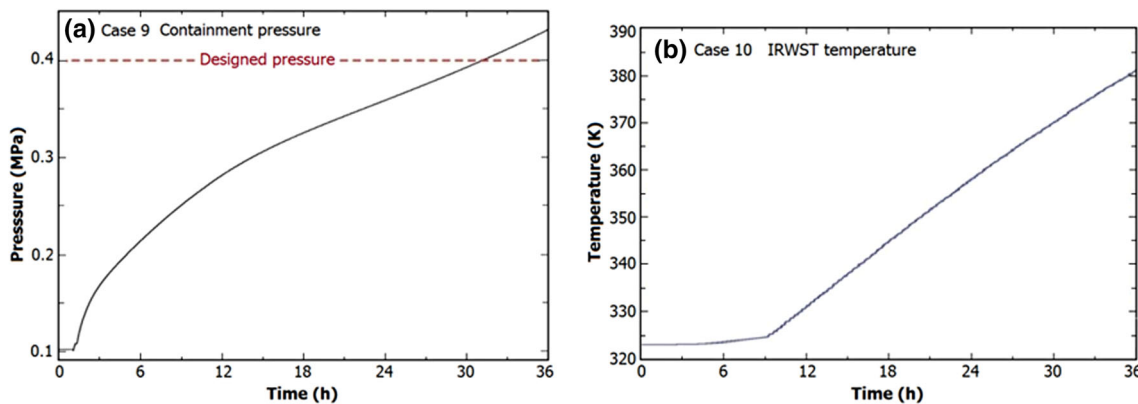
Fig. 12 Containment pressure of Case 9 (**a**) and IRWST temperature of Case 10 (**b**) for SGTR

decreases. This estimation is proven by for Case 10 as shown in Fig. 12b. The IRWST temperature rises above the boiling temperature of water in atmospheric pressure. Therefore, the final status is containment failure which can lead to core damage.

6.4.9 SGTR sequences with failure to isolate ASG (sequence 8–14)

Sequences 8–14 represent those branches of the event tree with failure to isolate the damaged steam generator. Nine more cases (Cases 11–19) are analysed for the information needed to support SGTR accident sequence modelling.

Accordingly, the worst case is selected for the failure of SGI. This is modelled by assuming that one of the MSRVs in the damaged steam generator line is stuck open. It is assumed that after the first opening of MSRV at its set point, the failure to reclose MSRV makes the affected steam generator non-isolable. For the sake of brevity, the calculations are not explained here; however, the main findings are summarized in the discussion section.

6.4.10 Case 19: RTS failure (sequence 15)

In the case of failure of RTS to trip the reactor, the sequence will lead to core damage. This is demonstrated in Fig. 13. This evidence confirms the correctness of the assumptions in Sequence 15 of the reference event tree.

7 Discussion

TH code calculation results are summarized in Table 4 for peak clad temperature, containment pressure and the state of leakage to the environment. The key findings of the code calculations are explained below:
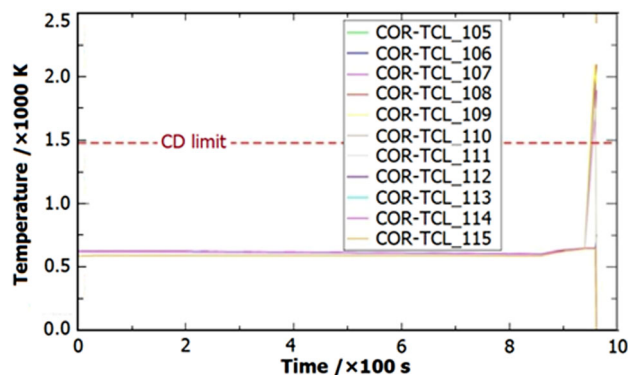

Fig. 13 PCT profile for Sequence 15 of SGTR

1. It is deduced from the first four cases that the RCS inventory control is needed for the mitigation of the accident in case of RCS depressurization through SDVs. On the other hand, if SIS provides RCS inventory continuously for the whole mission time, the leakage will not be terminated. For these cases, the end state is OK regarding the PCT limit, but the containment is bypassed. Another finding for this case is that even without EFW, CD would not happen. To summarize the insights from Cases 1–4, it is concluded that:

    –   For Sequence 3, without inventory control in the early stages, CD will come out.
    –   In Sequences 1 and 2, operation of either CVCS or SIS could avoid CD but there is still leakage from primary system (RCS) to the atmosphere through MSSV. Therefore, it is needed to include a human action for termination of SIS injection.
    –   Even without EFW, CD will not happen in case of SIS injection.

2. Case 7 reveals that one MSRV is completely capable of cooling down the reactor and there is no need for inventory control by safety injection.

Table 4 Summary of TH code calculations for SGTR

Case no.	RTS	SGI	EFW SHR	SIS	CVCS	Cooldown[a]	Depressurization[b]	RHR	Bleed	CS HR	PCT (K)	Containment pressure (bar)	Release terminated?	Consequence
1	✓	✓	1	4	0	–	–	–	–	–	623.0	N.A[c]	No (≈ 30 kg/s)[d]	OK
2	✓	✓	0	1	0	–	–	–	–	–	623.0	N.A	No (≈ 8 kg/s)[d]	OK
3	✓	✓	1	0	1	–	–	–	–	–	623.0	N.A	No (≈ 7 kg/s)[d]	OK
4	✓	✓	1	0	0	–	–	–	–	–	2358.3	N.A	No(≈ 0.6 kg/s)	CD
5	✓	✓	1	0	1	✓	✓	–	–	–	623.0	1.3	Yes	OK
6	✓	✓	0	0	1	✓	✓	–	–	–	2500.0	2.0	No	CD
7	✓	✓	1	0	0	1 MSRV	–	–	–	–	623.0	N.A	Yes	OK
8	✓	✓	0	1	0	–	–	–	–	1	623.0	2.0	No (≈ 9 kg/s)	OK
9	✓	✓	0	0	0	–	–	–	1	–	2500.0	N.A	No	CD
10	✓	✓	0	1	0	–	–	–	1	0	623.0	4.32	No	Containment damage
11	✓	–	–	–	–	–	–	–	–	–	2498.0	N.A	No	CD
12	✓	–	1	–	–	–	–	–	–	–	2497.0	N.A	No	CD
13	✓	–	1	1	–	–	–	–	–	–	623.0	N.A	No (≈ 20 kg/s)[d]	OK
14	✓	–	1	1	0	✓	✓	2	–	–	623.0	N.A	Yes	OK
15	✓	–	1	1	0	✓	✓	1	–	–	623.0	N.A	Yes	OK
16	✓	–	1	1	0	✓	✓	0	1	1	623.0	1.2	No (≈ 1 kg/s)[d]	OK
17	✓	–	1	1	–	–	–	–	–	–	623.0	N.A	No (≈ 0.5 kg/s)[d]	OK
18	✓	–	–	1	–	–	–	–	1	–	623.0	1.35	No (≈ 2.2 kg/s)[d]	OK
19	–	✓	–	–	–	–	–	–	–	–	2200.0	N.A	No	CD

[a] Cooldown = RCS cool down by operator using 1 of the intact SG MSDVs

[b] Depressurization = Manual RCS depressurization using 1 of pressurizer SDVs

[c] N. A not affected

[d] IRWST available

Table 5 Summary: SGTR top event success criteria

Event tree top event	Assumptions in success criteria analysis	Success criteria concluded from TH code results
RTS	Thermal reactor power decreases to decay heat level (automatically)	Reactor power decreases to decay heat level by pressurizer low-pressure signal
	Consequential LOOP by turbine trip	
SGI	MSIV automatic closure	PSA assumptions are confirmed
	MSSV stuck open is not considered	
	Closure of EFW and MFW isolation valves, in affected line (automatically)	
	For SGI failure, it is assumed that MSDV sticks open	
EFW SHR	For this component to deliver water to SG, 60 s delay time is assumed to consider the worst case	1/1 EFW trains actuation by low–low SG water level signal in the intact line
		At least one of the MSSVs in intact line is required
		2 EFW supply pools available -Opening the valves in connection line between two EFW supply is needed
SIS	LOOP	Automatic or manual actuation of 1/4 SIS pumps
	For SIS to deliver water to RCS, 40 s delay time is assumed	SIS stop for the leakage termination is mandatory
	SIS injection as a function of PRZ level to keep it constant	
OPE	MSDV operates in the line with intact steam generator stopping when $P_1 = P_2 <$ MSSV pressure set point	Opening of 1/2 SDVs in cooldown set points by operator
		Opening of 1/2 MSDVs in cooldown set points
		1/1 EFWS train with actuation of 1/2 pumps in intact line, main steam line isolation by MSIV, and operating 1/2 MSDVs in cooldown set point
OPD	Operator performs the primary side depressurization by actuating intact line MSDV and pressurizer SDV	Opening of 1/2 SDVs in cooldown set points by operator
	Heaters are assumed unavailable	1/1 EFWS train with actuation of 1/2 pumps in intact line, main steam line isolation by MSIV and operating 1/2 MSDVs in cooldown set
		SIS control and CVCS stop when RHR set point is reached
RHR	Actuated by operator when set points reached	1/4 CS/RHR trains
	SIS stops when RHR operates	Operator opening of RHR isolation valves to cold leg and closing of RHR isolation valves to spray lines
		Operator opening of CS isolation valves to cold leg and closing of CS isolation valves to spray lines
BLEED	Operator action	Opening of 1/2 SDVs in cooldown set point by operator
CS/HR	CS/RHR pumps actuation by high–high–high containment pressure signal (automatically)	1/4 CS/RHR trains with actuation of pumps in the related train and related heat exchanger
	LOOP condition	

3. For Sequence 4, at least one train of CS/HR system is needed to reach the safe condition.

4. From the insights of Cases 16 and 17, there is no need for containment spray system in feed and bleed process. From the results of Case 18, by failure of EFW and not isolating steam generator (i.e. Sequence 14) it is deductible that feed and bleed can mitigate the accident.

5. Continuous leakage and SIS injection resemble to PF&B process with the same outcome. This is the case for Sequences 2 and 12 of the reference event tree. Although these sequences are successful regarding PSA Level 1 criteria, their leakage to the environment is not terminated.

As the final note, top event success criteria for SGTR are summarized in Table 5.

8 Concluding remarks

A key goal of this paper is to critically review available approaches and discuss technical challenges for SCA. In fact, what has been addressed here is to provide a how-to procedure for this PSA task because the authors' driving

motivation is that a step-by-step procedure for effective success criteria analysis is missing in the literature. In this regard, we have proposed a systematic framework for effective success criteria analysis in compliance with ASME PRA standard. The proposed methodology is general and independent from the type of NPP and its associated scenario. It is implemented by accomplishment of the following tasks:

Task 1	Review of the proposed event tree and assumptions in the PSA model.
Task 2	Implementation of PSA assumption to deterministic plant model.
Task 3	TH calculations and documentation of the results.

Elements of the proposed methodology are structured on plant-specific best estimate calculations which avoid sole reliance on expert judgment, design data and DBA analysis. Moreover, it addresses some solutions for the identified limitations of this area by suggesting (1) a modification on the core damage definition by considering the containment role, (2) introducing a framework for the development of a qualified deterministic model and (3) successful application of the proposed methodology on SGTR accident in a typical PWR. The extension of the research in this area would be to extend the proposed methodology for the extraction of the operator's time window which is a key element for human reliability analysis in NPP applications and is interrelated with success criteria.

References

1. Normal Carl Rasmussen, Reactor safety study, an assessment of accident risks in US commercial nuclear power plants, NUREG 75/014 (1975)
2. W. Keller, M. Modarres, A historical overview of probabilistic risk assessment development and its uses in nuclear power industry: a tribute to the late Professor Norman Carl Rasmussen. Reliab. Eng. Syst. Saf. **89**, 271–285 (2005). doi:10.1016/j.ress.2004.08.022
3. EPRI, PRA procedures guide: a guide to the performance of probabilistic risk assessments for nuclear power plants, NUREG/CR-2300 (1983)
4. US NRC, Severe accident risks: an assessment for five US nuclear power plants (1990)
5. ASME/ANS, Standard for Level 1/large early release frequency PRA for NPP applications, Standard ASME/ANS-RA-S (2008)
6. ASME/ANS, Probabilistic risk assessment standard for advanced non-LWR nuclear power plants, Standard ASME/ANS RA-S-1.4-2013 (2013)
7. ANS/ASME, Requirements for low power and shutdown probabilistic risk assessment, Standard ANS/ASME-58.22-2014 (2014)
8. ASME/ANS, Severe accident progression and radiological release (Level 2) PRA standard for nuclear power plant applications for light water reactors (LWRs), ASME/ANS RA-S-1.2-2014 (2014)
9. M. Stamatelatos, H. Dezfuli, Probabilistic risk assessment procedures guide for NASA managers and practitioners, NASA/SP-2011-3421 (2011)
10. I.A. Papazoglou, Z. Nivolianitou, O. Anez et al., Probabilistic safety analysis in chemical installations. J. Loss Prev. Process Ind. **5**(3), 181–191 (1992). doi:10.1016/0950-4230(92)80022-Z
11. R.R. Fullwood, *Probabilistic Safety Assessment in Chemical and Nuclear Industries* (Butterworth-Heinemann, Woburn, 2000)
12. J. Tixiera, G. Dusserrea, O. Salvib, D. Gaston, Review of 62 risk analysis methodologies of industrial plants. J. Loss Prev. Process Ind. **15**(4), 291–303 (2002). doi:10.1016/S0950-4230(02)00008-6
13. G.E. Apostolakis, How useful is quantitative risk assessment? Risk Anal. **24**(3), 515–520 (2004). doi:10.1111/j.0272-4332.2004.00455.x
14. S. Schroer, M. Modarres, An event classification schema for evaluating site risk in a multi-unit nuclear power plant probabilistic risk assessment. Reliab. Eng. Syst. Saf. **117**, 40–51 (2013). doi:10.1016/j.ress.2013.03.005
15. M. Rausand, *Risk assessment: theory, methods, and applications* (Wiley, Hoboken, 2013)
16. S.M. Hoseyni, F. Yousefpour, A. Aghaei, K. Karimi, S.M. Hoseyni, Effects of soil-structure interaction on fragility and seismic risk; a case study of power plant containment. Loss Prev. Process Ind. **32**, 276–285 (2014). doi:10.1016/j.jlp.2014.09.009
17. S.M. Hoseyni, M. Pourgol-Mohammad, A.A. Tehranifard, F.A. Yousefpour, A systematic framework for effective uncertainty assessment of severe accident calculations; Hybrid qualitative and quantitative methodology. Reliab. Eng. Syst. Saf. **125**, 22–35 (2014). doi:10.1016/j.ress.2013.06.037
18. A. Prosek, M. Cepin, Success criteria time windows of operator actions using RELAP5/MOD3.3 within human reliability analysis. J. Loss Prev. Process Ind. **21**, 260–267 (2008). doi:10.1016/j.jlp.2007.06.010
19. K. Karimi, F. Yousefpour, A. Abbaspour, M. Pourgol-Mohammad, Assessment of human error importance in PWR PSA. Rom. J. Phys. **59**(7–8), 873–883 (2014)
20. R. Barati, S. Setayeshi, On the operator action analysis to reduce operational risk in research reactors. Process Saf. Environ. Prot. **92**(6), 789–795 (2014). doi:10.1016/j.psep.2014.02.006
21. USNRC, Confirmatory TH analysis to support specific success criteria in the risk models, NUREG -1953 (2011)
22. USNRC, An approach for determining the technical adequacy of probabilistic risk assessment results for risk-informed activities, Regulatory Guide 1.200 (2009)
23. M. Pourgol-Mohammad, S.M. Hosseini, Comprehensive uncertainty assessment methodology for probabilistic risk assessment, Proceedings of PSA2011 Conference, Wilmington (2011)
24. S.M. Hoseyni, M. Pourgol-Mohammad, Model uncertainty in severe accident calculations: a structural methodology with application on LOFT LP-FP-2 experiment. J. Nucl. Tech. **193**(3), 341–363 (2016). doi:10.13182/NT15-47
25. T.W. Kim, V.N. Dang, M.A. Zimmermann et al., Quantitative evaluation of change in core damage frequency by postulated power uprate: medium-break loss-of-coolant-accidents. Ann. Nucl. Energy **47**, 69–80 (2012). doi:10.1016/j.anucene.2012.04.021
26. C.J. Everline, Illustration of integrating mechanistic best-estimate analysis results in Level 1 probabilistic risk assessment. Reliab. Eng. Syst. Saf. **44**, 139–152 (1994). doi:10.1016/0951-8320(94)90006-X
27. H.F. Martz, L.L. Harem, W.H. Reed et al., Combining mechanistic best-estimate analysis and Level 1 probabilistic risk assessment. Reliab. Eng. Syst. Saf. **39**, 89–108 (1993). doi:10.1016/0951-8320(93)90151-N
28. Y.J. Cho, T.J. Kim, H.G. Lim et al., Effect of uncertainties in best-estimate thermal hydraulic analysis on core damage

frequency for PSA. Nucl. Eng. Des. **240**(12), 4021–4030 (2010). doi:10.1016/j.nucengdes.2010.01.014

29. M. Pourgol-Mohammad, "Effect of uncertainties in best-estimate thermal hydraulic analysis on core damage frequency for PSA" Y.-J. Choa, T.-J. Kima, H.-G. Limb, G.-C. Parka. Nucl. Eng. Des. **241**(9), 4060 (2011). doi:10.1016/j.nucengdes.2011.07.021

30. IAEA, Accident analysis for nuclear power plant, IAEA-SRS-No.023 (2002)

31. ASME, Standard for Level 1/large early release frequency probabilistic risk assessment for nuclear power plant applications, ASME/ANS RA-Sa-2009 (2009)

32. IAEA, Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants, IAEA TECDOC-1511 (2006)

33. BNPP, PSA Level-1 at Power for Bushehr Nuclear Power Plant (2003)