This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2020-7215C

The Risk-Informed Activities in the Physical Security Pathway

F. Mitch McCrory, Douglas Osborn, Brian Cohn

Sandia National Laboratories, United States of America. E-mail: fmmccro@sandia.gov; dosborn@sandia.gov; bcohn@sandia.gov

Vaibhav Yadav, Robby Christian, Steven Prescott

Idaho National Laboratories, United States of America. E-mail: vaibhav.yadav@inl.gov ; robby.christian@inl.gov; steven.prescott@inl.gov

The U.S. Department of Energy's Light Water Reactor Sustainability Program established a Physical Security Pathway in 2019 to explore opportunities for the U.S. Nuclear Power Industry to optimize nuclear power plant's physical security while maintaining effectiveness. After September 2001, significant changes to NPPs' Design Basis Threat were implemented resulting in changes to physical security posture and increases in the number of manned posts, which were added as a conservative measure since adequate risk tools were either nonexistent or were inadequate for addressing the dynamic nature of a security threat. This has resulted in physical security being one of the largest contributors to manpower outlays at NPP sites where up to one-third of the workforce is security related. The goal of the LWRS Program PSP is to provide the technical basis necessary for stakeholders to evaluate and implement physical security changes necessary to optimize industry's physical security posture while maintaining or improving effectiveness. Risk-informing physical security is one of the key research and development (R&D) activities of the pathway. This paper focuses on: novel ways of using current risk tools; advancement of dynamic risk methods to account for the dynamic nature of a motivated adversary; R&D that creates new risk tools to help risk-inform physical security professionals and validation of these methods and tools to support implementation in a highly regulated environment.

Keywords: risk-informed, security, nuclear, LWRS, threat, plant, adversary.

1. Introduction

The U.S. Department of Energy's Light Water Reactor Sustainability (LWRS) Program established a Physical Security Pathway (PSP) in 2019 to explore opportunities for the U.S. Nuclear Power Industry to optimize nuclear power plant (NPP) physical security while maintaining necessary effectiveness. Following the events of September 2001, significant changes to NPPs' Design Basis Threat were implemented resulting in many changes to physical security posture and increases in the number of manned posts, which were added as a conservative measure since adequate risk tools either did not exist, were not applied to the security domain, or were not adequate for addressing the dynamic nature of a security threat. This resulted in physical security being one of the largest contributors to manpower outlays at United States (U.S.) NPP sites where up to one-third of the workforce is security related (Macfarlane 2016, para.16). Currently, nuclear power plant security is focused on preventing sabotage to reactor systems. Vital areas at NPPs contain critical equipment necessary to ensure adequate core cooling to the reactor core and spent fuel pool to prevent release of radionuclides. It is assumed that sabotage of a vital area results in an unacceptable release of radionuclides, However, the goal of preventing adversary sabotage of a vital area is a challenging one that NPPs have only been able to meet at great effort and expense.

This paper provides some of the work-to-date on development and application of integrated safety-security modelling through advanced risk assessment techniques that could ease the challenges faced by NPPs.

2. Risk Informed Approaches

The LWRS Program PSP has been researching ways to more accurately determine the effects of sabotage to reactor systems with the goal of providing the technical basis for risk informing nuclear security at NPPs, which could enable NPPs to better focus their security posture on

* *Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2020-XXXX*

† *Idaho National Laboratory is a multimission laboratory managed and operated by Battelle Energy Alliance, LLC, for the U.S. Department of Energy under contract DE-AC07-05ID14517.*

adversary attacks expected to cause an unacceptable release of radionuclides. In order to achieve this, the LWRS PSP has integrated security analysis, which can determine which NPP systems are sabotaged and the timelines involved and leverage dynamic probability risk assessment (DPRA) methods to determine the effects on the plant state from the loss of system(s) at specific times.

One challenge of current defensive measures is to determine their effectiveness quantitatively. To form a robust risk-informed methodology, evaluation must be more than just a pass/fail and additional statistical data needs to be collected and available for site evaluation. Current site inspections and Force on Force (FoF) evaluation methods result in limited data that can useful to the affected facility or to other facilities. Currently, facilities use advanced FoF simulation models to analyse and evaluate their protection strategies. While their ease of use makes current FoF models popular, they have several significant limitations such as being a static model that does not account for dynamic changes during an attack scenario and not modelling dynamic human actions.

Current research focuses on dynamic modelling to advance the existing capabilities to: 1) Model dynamic change during sabotage scenario in real time; 2) Account for operator actions; and 3) Integrate the existing thermo-hydraulic analysis capabilities with FoF models. This work employs the event modelling risk assessment using linked diagrams (EMRALD), a software tool developed at Idaho National Laboratory (INL), to not only obtain probabilistic results, but also model dynamic scenarios such as timing and event sequences for specified simulation results (Idaho National Labs 2019).

2.1 *EMRALD modelling tool*

A dynamic FoF model has been developed in EMRALD as part of the current research. EMRALD can couple with other simulation or physics tools to develop a modelling methodology for coupling FoF simulation with actions (operator and/or personnel), plant models, and secondary equipment such as FLEX portable equipment (Nuclear Energy Institute 2012 and 2017). EMRALD is a state diagram modelling tool based on three-phase discrete event simulation, where the next events in time are sampled. This allows for fast runtimes with either close, long, or bunched spacing of events in time. A user interface allows for quick and easy-to-understand modelling of scenarios and system, component, and operator actions. Coupling with an EMRALD model can be done through both one-way and two-way coupling (Figure 1)**.**

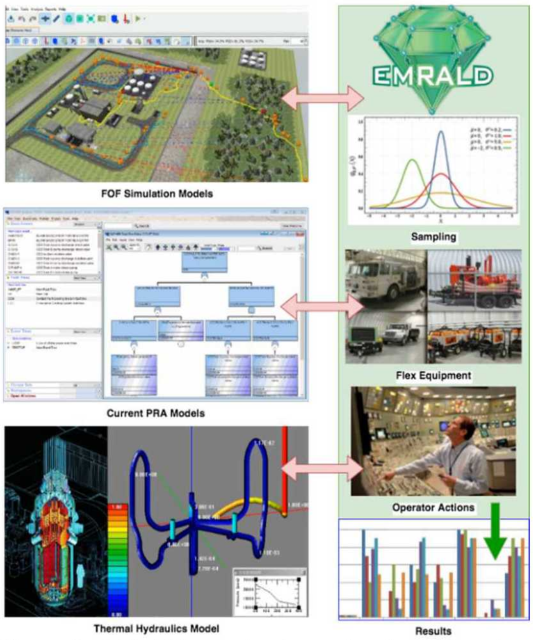


Figure 1. EMRALD as the integrating hub of various computational tools.

One-way coupling allows EMRALD to set up an external code or model given current states and values in EMRALD, model and run it, and then process the results for transitioning between states and continuing the simulation. This is the most common method as it covers the needs of most scenarios and requires no external code modifications or programming interface to be written. When feedback loops, where a second application requires evaluation of its data from the initial application before continuing, then two-way coupling is required, and an open message protocol system is available. It is anticipated that initial coupling and method development will be simple and will only require one-way coupling.

2.1.1 *EMRALD modelling example*

This section demonstrates how a Force-on-Force scenario can be modelled in a dynamic manner using the EMRALD tool. For the purpose of this illustration, a hypothetical 4-loop commercial Pressurized Water Reactor (PWR) called the Lone Pine Nuclear Power Plant (LPNPP) (Sandia National Laboratories 2017) was selected as the target facility. Figure 2 shows the layout of LPNPP facility, and lists buildings important for the plant's safety as well as structures crucial for the physical security.

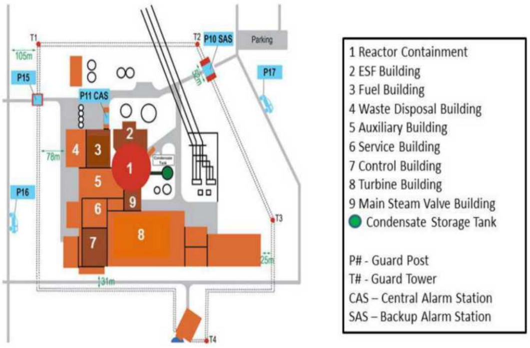


Figure 2. Lone Pine Nuclear Power Plant layout.

Based on LPNPP layout, a hypothetical attack scenario was devised and modelled to be initiated by a five-person group of adversaries with the intent of triggering a Station Blackout (SBO). The modelled attack comprises of eleven steps described in Table1.

The attack scenario is modelled in a multi-level approach in EMRALD. The first-level diagram, as shown in Figure 3, groups the scenario into an exterior and interior breach. The plant is in the key "Plant_OK" state at the start of simulation. Adversaries are defined to be successful in attack after breaching the interior building and causing explosion resulting in EDGs out of operation, marked as the "All_EDGs_Gone" event. The "Exterior_Breach" state is linked to its second level diagram by the "Adv_Commence_Attack" action.

Table 1. Description of the steps in the modelled attack scenario.

Step #	Action	Objective	Action time - seconds
1	Adv-5 places explosive charges on the legs to the main power line towers and waits for the detonation cue.	Isolate LPNPP from offsite power	200
2	Adv-1, 2, 3 and 4 sneaks on foot to the north-side of the facility.	Evade detection by tower guards	300
3	Adv-3 cuts a hole in the outer fence.	Infiltrate the protected area	20
4	Adv-3 enters PIDAS and heads to the inner fence followed by Adv-1,2, and 4.		5
5	Adv-3 cuts a hole in the inner fence.		20
6	Adv-1,2,3, and 4 enter the protected area and go towards the generator room.		10
7	Adv-3 unlocks the door to generator room.	Infiltrate the generator room	20
8	Team-1 (Adv-1 and 2) go to Emergency Diesel Generator (EDG) A and Team-2 (Adv-3 and 4) go to EDG B.	Destroy EDGs	20
9	Team-1 sets up explosives at EDG A while Team-2 sets up at EDG B.		40
10	Team-1 detonates EDG A and Team-2 detonates EDG B.		0
11	Adv-5 detonates main power line upon hearing explosions or gunfights inside LPNPP.	Create an SBO event	0

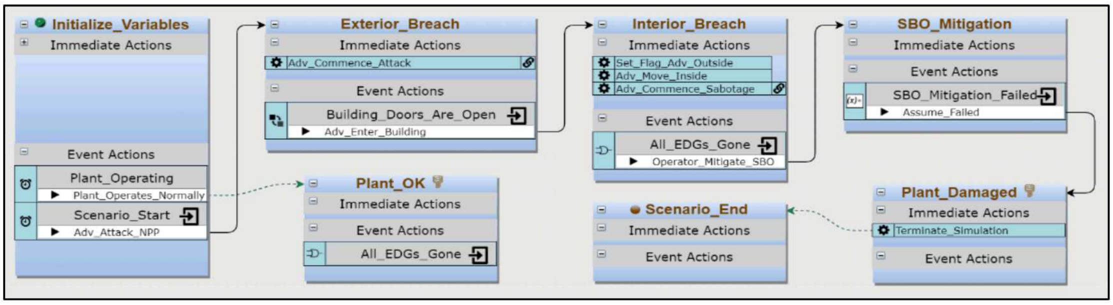


Figure 3. First-level diagram of the FoF model in EMRALD.

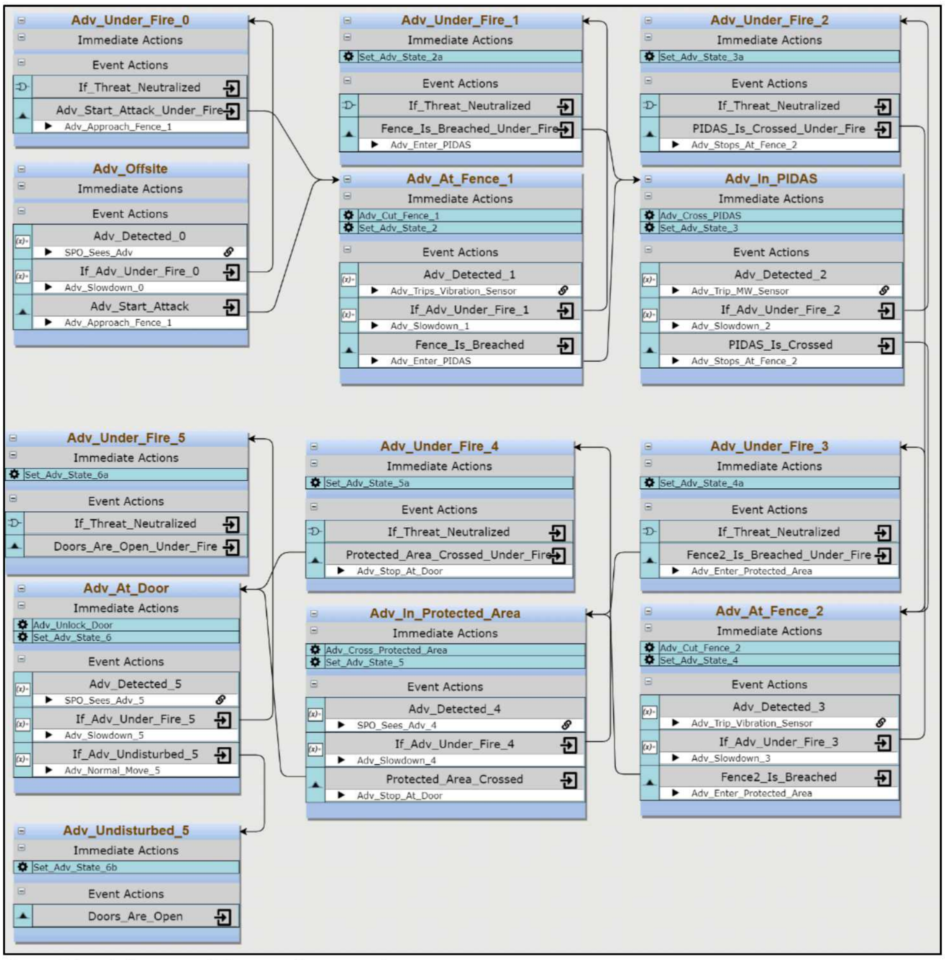
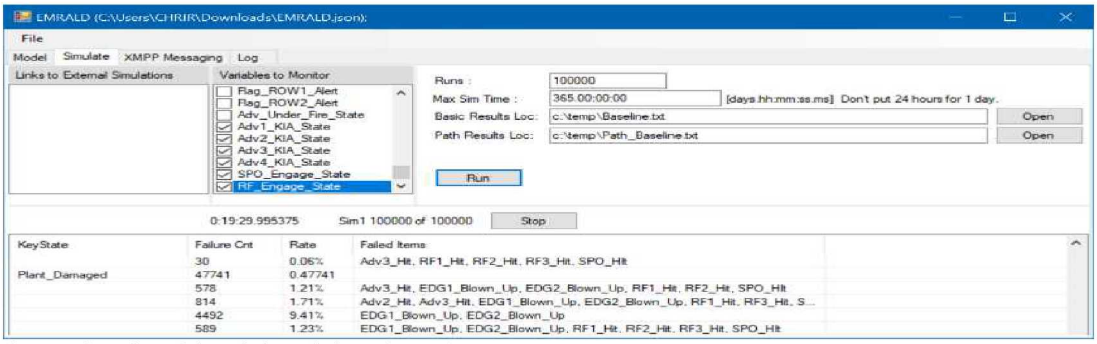


Figure 4. Second-level diagram of the Exterior_Breach state.

Figure 4 shows the second-level state transitions within the “Exterior-Breach” group. This exterior breach started from the “Adv_Offsite” state. State transitions in this “Exterior_Breach” diagram ended when adversaries unlocked the door leading to the diesel generator room. SPO engages adversaries when the simulation enters the “SPO_Engage_Adv” state. This state triggers a probabilistic transition in both the individual adversary and SPO diagrams. Figure 5 shows a snap shot of the EMRALD solutions window for the FoF model.


EMRALD (C:\Users\CHRIR\Downloads\EMRALD.json):
File
Model
Simulate
XMPP Messaging
Log
Links to External Simulations
Variables to Monitor
Open
Open
Run
Stop

□ Flag_ROW1_Alert
□ Flag_ROW2_Alert
□ Adv_Under_Fire_State
☑ Adv1_KIA_State
☑ Adv2_KIA_State
☑ Adv3_KIA_State
☑ Adv4_KIA_State
☑ SPO_Engage_State
☑ RF_Engage_State

Runs : 100000
Max Sim Time : 365.00:00:00 [days.hh:mm:ss.ms] Don't put 24 hours for 1 day.
Basic Results Loc: c:\temp\Baseline.txt
Path Results Loc: c:\temp\Path_Baseline.txt

0:19:29.995375 Sim1 100000 of 100000

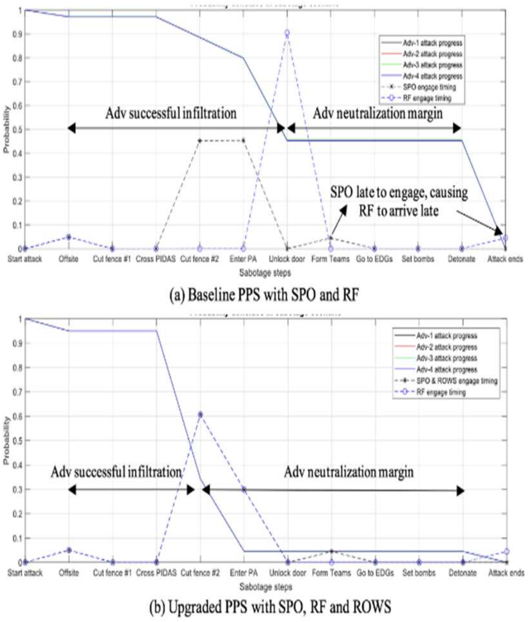
KeyState	Failure Cnt	Rate	Failed Items
	30	0.06%	Adv3_Hit, RF1_Hit, RF2_Hit, RF3_Hit, SPO_Hit
Plant_Damaged	47741	0.47741	
	578	1.21%	Adv3_Hit, EDG1_Blown_Up, EDG2_Blown_Up, RF1_Hit, RF2_Hit, SPO_Hit
	814	1.71%	Adv2_Hit, Adv3_Hit, EDG1_Blown_Up, EDG2_Blown_Up, RF1_Hit, RF3_Hit, S...
	4492	9.41%	EDG1_Blown_Up, EDG2_Blown_Up
	589	1.23%	EDG1_Blown_Up, EDG2_Blown_Up, RF1_Hit, RF2_Hit, RF3_Hit, SPO_Hit

Figure 5. Snapshot of the solution window of EMRALD FoF model listing the various scenarios and percentage of plant damage states

The EMRALD model is solved with the Monte-Carlo method using 100,000 simulation runs.

EMRALD results (Figure 6) provide a comprehensive insight into the attack scenario including the failure counts, a list of dynamic scenarios that resulted in success/failure along with the percentage and variable sensitivities.

The results from EMRALD analysis also allow to observe the evolution of probabilities as the adversarial scenario is progressing. Figure 6 shows plots of the probability values evolving over the timeline of the sabotage for two different scenarios.



(a) Baseline PPS with SPO and RF

(b) Upgraded PPS with SPO, RF and ROWS

Figure 6. EMRALD results for probability values of adversary attack progression versus responder intervention timings.

Such comparisons help in not only comparing the effectiveness of different security postures but also dig deeper into the performance at specific times during an attack.

Figure 7 presents a comparison of different probability of effectiveness obtained in EMRALD analysis for different security configurations during a reference sabotage scenario. Such comparisons provide means to optimize the security posture and select the most efficient and effective posture for a given scenario.

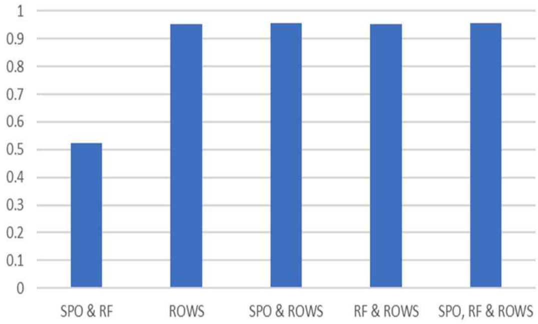


Figure 7. EMRALD results of probability of PPS effectiveness of various combinations of security response capabilities against a reference sabotage scenario.

2.2 Use of ADAPT

The LWRS PSP has integrated safety information into security analysis through the Leading Simulator/Trailing Simulator (LS/TS) method, driven by the ADAPT scheduler (Cohn, Et al, 2020). This analysis combines the LS, Scribe3D (Sandia National Laboratories 2019), which is a force-on-force simulation code designed for security analysis, with the TS, nuclear system accident response code MELCOR (Humphries, Et al, 2018), to model the response of the LPNPP to an adversary attack. LPNPP is a hypothetical 4-loop PWR regularly used for IAEA international security training course. As part of this effort, the LWRS PSP updated the LPNPP model to include a building for FLEX equipment (Nuclear Energy Institute 2012) and constructed a Scribe3D model incorporating these change (Figure 8).

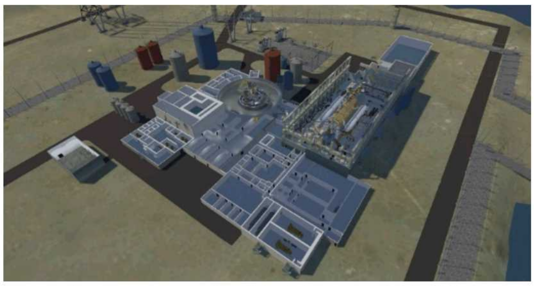


Figure 8: Lone Pine NPP shown in Scribe3D

Based on previous security analyses of LPNPP, it was assumed that the condensate storage tank (CST) is a vital area according to site's security plan. The loss of the CST is assumed to lead to the loss of the auxiliary feedwater (AFW) system and results in core damage and eventual release of radionuclides which yield an unacceptable radiological consequence. However, sabotage of the CST alone is unable to cause core damage, as water from the ultimate heat sink can also serve as a source of AFW coolant. To account for this alternate source of coolant, it was assumed that adversaries would need to sabotage both the intake and the CST to neutralize the AFW alternate intake supply sources.

2.2.1 *ADAPT example*

An adversary attack on the Lone Pine NPP site was constructed to demonstrate the safety-security integration by linking Scribe3D and MELCOR through the ADAPT DPRA scheduler. The adversary attack scenario is shown in Figure 9 following the red marked pathway. In this scenario, adversaries initially attack the intake structure, disabling it. After disabling the intake structure, the adversaries proceed to the CST in which they create a hole. After sabotaging the CST, the adversaries attempt to sabotage the FLEX building and deter operator actions throughout the facility until driven off by offsite responders.

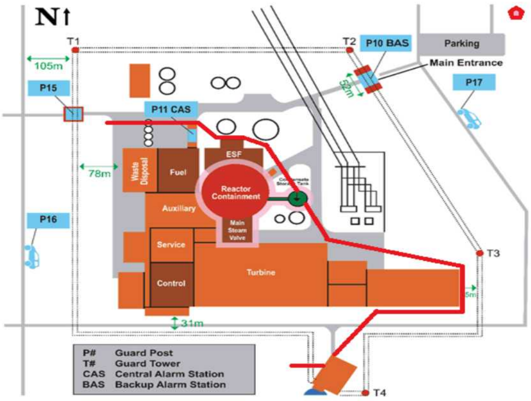


Figure 9: Lone Pine site map with adversary attack path in red

Additionally, a preliminary MELCOR simulation was performed on the LPNPP reactor to explore the dynamic nature of this sabotage. Two cases were considered: (1) sabotage of the CST leads to an immediate loss of the AFW, and (2) sabotage of the CST causes a one square meter hole in the side of the tank. In this second case, the AFW remains functional until the CST empties.

The lower plenum temperature evolutions for both cases are given in Figure 10 with each terminating once the temperature reaches 600K. When the AFW is immediately lost, the core temperature reaches 600K in ~24 minutes. However, if the AFW is instead lost only when the CST empties, the reactor takes more than three hours longer to reach the same lower plenum temperature of 600K. Because of this additional time available to operators, it may be feasible for offsite responders to retake control of the plant or other operator actions to restore adequate core cooling before the onset of core damage yielding to an unacceptable radiological consequence.

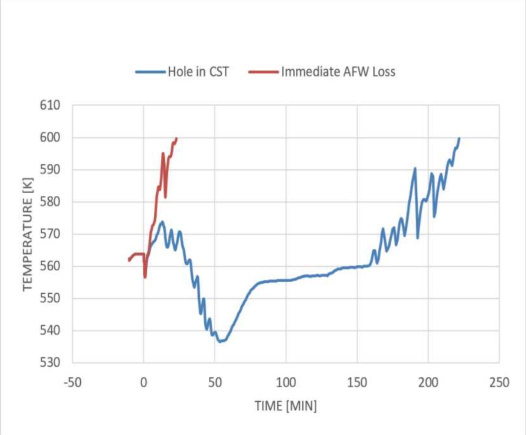


Figure 10: Lower plenum temperature following CST sabotage

3. Future Work Summary

The research presented in this report describes the development, findings, and comparative analysis of dynamic models of current and potential physical security posture at a typical US commercial nuclear power plant. These FoF models are a powerful tool for quantitative assessment of a plant's physical security performance effectiveness under an attack scenario. The models enable the analysis of current posture, perform sensitivity analysis, identify strength and weaknesses, explore different strategies and drive potential optimizations in a plant's physical security posture. The future effort towards incorporating increased realism in modelling and simulation will focus on the following:

1. Implementing EMRALD dynamic modelling capabilities for physical security posture optimization pilot: As utilities continue to make investments in advanced security technologies it is important to determine the posture that is most effective and cost-efficient. Our research team is working closely with US commercial utilities on implementing the EMRALD models on an existing physical security posture of a NPP in order to determine the optimum posture *before* making the investment.
2. Integrating the performance of FLEX portable equipment in the FoF models: Onsite FLEX includes equipment such as portable pumps, generators, batteries, compressors, and other supporting equipment and tools, all stored in a dedicated and secure building designed to withstand external hazards. In the past years, several NPPs have invested in procuring and maintaining the onsite Flex asset that stands unutilized most of the time. Integrating Flex portable equipment in FoF modeling and simulation using EMRALD will provide utilities with technical basis and quantitative results to enable taking credit of Flex in their security posture.

Both DPRA approaches have yielded initial and promising proof-of-concept results. In future work, these LWRS PSP integrated safety-security modelling approaches will be demonstrated with full adversary scenarios. These adversary scenarios will consider the interplay between the adversary, onsite guard forces, offsite response forces, and operator actions to include: (1) actions within the control room only, (2) actions within the control room and inside the plant, and (3) the application of FLEX.

Future work will also expand on preliminary work performed using Bayesian Statistics to inform adversary timeline development and other risk assessment methods used in similar non-nuclear power applications with adversary focused risk.

4. Conclusion

The goal of the LWRS Program PSP is to provide the technical basis necessary for stakeholders to evaluate and implement physical security changes necessary for the nuclear power industry to optimize its physical security posture while maintaining or improving its overall system effectiveness. Risk-informing physical security is one of the key R&D activities of the PSP. This work provides a proof-of-concept of unique and novel ways of using current risk tools, some often used in nuclear safety; advancement of dynamic risk methods to account for the dynamic nature of a motivated adversary (e.g., accounting for operator action and extending scenarios past target set loss); R&D that creates new risk tools to help risk-inform physical security professionals, and validation of these methods and tools to support implementation in a highly regulated environment.

References

Cohn, B., Noel, T., Haskin, T., Osborn, D., and Aldemir, T. (November 2020) “Quasi-Simultaneous System Modeling in ADAPT.” European Safety and Reliability Conference. Venice, Italy.

Humphries, L., Beeny, B., Gelbard, F., Louie, D., and Phillips, J., (2018) “MELCOR Computer Code Manuals Vol. 1: Primer and Users’ Guide,” SAND2018-13559 O, Sandia National Laboratories, Albuquerque, NM, USA.

Idaho National Laboratory, "EMRALD," Available: https://emrald.inl.gov/SitePages/Overview.aspx. [Accessed 1 September 2019].

Macfarlane, A. (13 April 2016) “How to protect nuclear plants from terrorists,” TheConversation.com; http://theconversation.com/how-to-protect-nuclear-plants-from-terrorists-57094.

Nuclear Energy Institute, (August 2012) “Diverse and Flexible Coping Strategies (FLEX) Implementation Guide,” NEI 12-06, https://www.nrc.gov/docs/ML1222/ML12221A205.pdf

Nuclear Energy Institute, (2017) "Guidance for Optimizing the Use of Portable Equipment (NEI 16-08)," Nuclear Energy Institute, Washington DC.

Sandia National Laboratory, (1 September 2017) "Lone Pine Nuclear Power Plant (LPNPP) hypothetical facility exercise data handbook," Available: https://share-ng.sandia.gov/itc/assets/hypo_fac_lpnpp_090117.pdf.

Sandia National Laboratory, (2019)“Scribe3D User’s Manual,” SAND2019-13848.