Czech Technical University in Prague
Faculty of Nuclear Sciences and Physical Engineering
Department of Nuclear Reactors

THESIS

Security of Small Modular Reactors

Praha 2023 Jana Vithová

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta jaderná a fyzikálně inženýrská

Břehová 7 115 19 Praha 1

Katedra jaderných reaktorů

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

Student:	**Bc. Jana Šošková**
Studijní program:	Jaderné inženýrství
Specializace:	Jaderné reaktory
Název práce česky:	**Problematika zabezpečení malých modulárních reaktorů**
Název práce anglicky:	Security of Small Modular Reactors
Jazyk práce:	angličtina

Pokyny pro vypracování:

1. Popište základní typy současných konceptů malých modulárních reaktorů (dále SMR) z hlediska konstrukce a použitého paliva. Zaměřte se na pojem „security/safety by design" a jak je řešen ve vybraných konceptech.
2. Popište současný regulatorní rámec v oblasti zabezpečení SMR z pohledu doporučení IAEA a některých vybraných zemí
3. Popište a identifikujte možné terče u vybraných konceptů SMR. Zhodnoťte možné důsledky úmyslných poškození těchto jaderných zařízení a krádeží jaderných materiálů.
4. Navrhněte, vyberte a popište hypotetické zařízení SMR. Popište proces návrhu a hodnocení systému fyzické ochrany.
5. Definujte projektovou základní hrozbu pro hypotetické zařízení. Navrhněte systém fyzické ochrany zvoleného hypotetického zařízení a zhodnoťte dostupnými matematickými modely.
6. V závěrečné části navrhněte doporučení pro analyzovaný model a shrňte výhody a nevýhody jednotlivých konceptů SMR z hlediska zabezpečení ve srovnání se současnými jaderně energetickými zdroji

Doporučená literatura:

[1] GARCIA, M. L. *The Design and Evaluation of Physical Protection Systems*. Oxford: Butterworth-Heinemann, 2008. ISBN 9780750683524

[2] IAEA. *Advances in Small Modular Reactor Technology Developments, 2020 edition*. Vienna: IAEA, 2020

[3] IAEA. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)*. Vienna: IAEA, 2011

[4] IAEA. *Identification of Vital Areas at Nuclear Facilities*. Vienna: IAEA, 2012

Jméno a pracoviště vedoucího práce: **Ing. Radovan Starý**
KJR FJFI ČVUT v Praze

Jméno a pracoviště konzultanta: **Ing. Jan Frýbort, Ph.D.**
KJR FJFI ČVUT v Praze

Jméno a pracoviště konzultanta: **Ing. Marek Ruščák**
Státní ústav radiační ochrany v.v.i.

Datum zadání diplomové práce: 14. 10. 2022
Datum odevzdání diplomové práce: 3. 5. 2023
Doba platnosti zadání je dva roky od data zadání.

V Praze dne 14. 10. 2022

prof. Ing. Tomáš Trojek, Ph.D.

Garant studijního programu

Ing. Jan Rataj, Ph.D.

Vedoucí katedry

doc. Ing. Václav Čuba, Ph.D.

Děkan

Autor:	Bc. Jana Vithová; FJFI, ČVUT, KJR
Název práce:	Problematika zabezpečení malých modulárních reaktorů
Obor:	Jaderné inženýrství
Specializace:	Jaderné reaktory
Druh práce:	Diplomová práce
Vedoucí práce:	Ing. Radovan Starý
Akademický rok:	2023/2024
Počet stran:	81
Klíčová slova:	malé modulární reaktory, SMR, jaderné zabezpečení, VEASI analýza

Author:	Bc. Jana Vithová; FJFI, ČVUT, KJR
Title:	Security of Small Modular Reactors
Field:	Nuclear engineering
Specialisation:	Nuclear reactors
Type of work:	Thesis
Supervisor:	Ing. Radovan Starý
Year:	2023/2024
Number of pages:	81
Keywords:	small modular reactors,SMR, nuclear security, VEASI analysis

Prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškerou použitou literaturu.

V Praze dne 12.1.2024 Jana Vithová

Abstrakt

Tato práce poskytuje ucelený přehled malých modulárních reaktorů (SMR) a zabývá se několika konkrétními typy. Zaměřuje se nejen na technické parametry, ale i na bezpečnostní aspekty, které jsou pro SMR typické. Zkoumá zásady zabezpečení podle návrhu a nastiňuje význam začlenění bezpečnostních opatření v počátečních fázích vývoje SMR. Druhá část práce přechází k praktickému využití a ilustruje koncepty zabezpečení prostřednictvím hypotetických scénářů na modelových lokalitách SMR. Tyto scénáře zahrnují projektovou základní hrozbu (DBT) a systém fyzické ochrany (PPS). Zkoumají se dvě různá hypotetická zařízení SMR, přičemž se zdůrazňuje přizpůsobivost bezpečnostních opatření na základě typu reaktoru a provozních charakteristik. Toto srovnání teoretických konstrukcí a praktických realizací slouží ke zdůraznění vzájemného působení mezi technologií SMR a nutností zabezpečit tato pokročilá jaderná zařízení proti potenciálním hrozbám.

Abstract

This work provides a comprehensive overview of Small Modular Reactors (SMRs), delving into several specific types. The focus extends beyond technical parameters to encompass security considerations intrinsic to SMRs. Exploring security by design principles, the narrative outlines the significance of integrating security measures during the initial phases of SMR development. The latter part of the work shifts to practical application, illustrating security concepts through hypothetical scenarios at model SMR sites. These scenarios incorporate a Design Basis Threat (DBT) and a Physical Protection System (PPS). Two distinct hypothetical SMR facilities are examined, highlighting the adaptability of security measures based on reactor type and operational characteristics. This juxtaposition of theoretical constructs and practical implementations serves to underscore the nuanced interplay between SMR technology and the imperative of securing these advanced nuclear facilities against potential threats.

Acknowledgements

I would like to thank a thousand times to the best teacher of the entire CTU, Mr. Starý, who gives me hope instead of anxiety, who is fun to be around and whose musical taste is both inspiring and fun. He was always available to me, explained everything I needed and gave me so much useful material to go over, many of which I used. Whatever happens with this paper, I am forever grateful for your mentorship. Then I would like to thank my Engineering consultant doctor Frýbort, who is always the voice of calm and reason and my SMR consultant Marek Rušák. Then I feel I really need to thank Mary Lynn Garcia for writing such a banger of a book that helped guide me through the odious process of birthing this thesis. I thank my parents for not asking me how is the thesis going, even when I was taking forever with it, and for their unwavering support in my efforts of earning the title of Nuclear Engineer. I want to thank my sister, granny, my not-so-baby any longer nephews and the rest of my family. I wholeheartedly thank to my bunny Floki, for getting me out of bed every day and reminding me that playtime before breakfast is what makes this life worth living. And last but most certainly not least I thank to my beloved husband Filip, I thank you for your endless patience, for the plethora of support you showered me with when I needed it the most, for being who you are and of course for smelling so good. You are the best person on this planet and everybody else can only strive to be the number two. I love you with all my heart. Thank you. -JV

Acronyms

3S	Safety, Security and Safeguards
4S	Super-Safe, Small and Simple
BWR	Boiling Water Reactor
CDP	Critical Detection Point
CEZ	Český Energetický Závod (Czech Energy Company)
CNSC	Canadian Nuclear Safety Commission
DBT	Design Basis Threat
DHRS	Decay Heat Removal Systém
EASI	Estimate of Adversary Sequence Interruption
EBR-II	Experimental Breeder Reactor II
ECCS	Emergency Core Cooling Systém
EPZ	Emergency Planning Zone
EW	Energy Well
FFTF	Fast Flux Test Facility
GCR	Gas Cooled Reactor
GDA	Generic Design Assessment
GNI	Global Nexus Initiative
HRC	High Radiological Consequences
HTGR	High Temperature Gas-Cooled Reactor
HTR-10	High-Temperature Gas-Cooled Test Reactor
HTR-PM	High-Temperature Gas-Cooled Reactor Pebble-bed Module
HTTR	High Temperature Engineering Test Reactor
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICS	Isolation Condenser Cooling Systém
IPyC	Inner Pyrolytic Carbon
LFTR	Lithium-Fluoride Thorium Reactor
MOX	Mixed Oxide Fuels
MSR	Molten Salt Reactor
NEA	Nuclear Energy Agency
NNS	Nuclear Security Series
NPM	Nuclear Power Module
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission

NSSS	Nuclear Steam Supply Systém
ONR	Office for Nuclear Regulation
OPyC	Onner Pyrolytic Carbon
PCV	Pressure Control Valve
PI	Probability of Interruption
PPS	Physical Protection Systems
PWR	Pressurized Water Reactors
RPV	Reactor Pressure Vessel
RTS	Regulatory Threat Statement
SeBD	Security By Design
SLM	Sabotage Logic Model
SMR	Small Modular Reactor
SyAPs	set of security assessment principles
TRISO	TRIstructural ISOtropic
URC	Unacceptable Radiological Consequences
VAI	Vital Area Identification
VDR	Vendor Design Review
VEASI	Very-Simplified Estimate of Adversary Sequence Interruption
WENRA	Western European Nuclear Regulators Association

Contents

List of Figures

List of Tables

1 Introduction

The increasing global demand for clean and sustainable energy solutions has sparked an interest in Small Modular Reactors (SMRs) as a promising avenue for nuclear power generation. These compact, versatile reactors offer the potential to revolutionize the energy landscape, providing safe and scalable nuclear energy options, even offering solutions to modern-day energy problems such as increasingly more complex load-follow needs. However, as with any advanced nuclear technology, the successful deployment of SMRs necessitates an examination of safety and security considerations. While most works on the topic done to date focus solely on safety of various SMR concepts, this work aims to provide some insight to SMR security. The first part of the thesis gives an overview of SMRs, offering classification and delving deeper into several chosen concepts. The second part concerns security, including target identification, vital area identification, the concept of DBT and Physical Protection Systems (PPS). The third part is practical and involves a look at two hypothetical SMR facilities and their security assessment using the VEASI software. Overall, this work aims to offer an initial exploration of a concern that, until now, has been largely uncharted within the SMR community.

2 Overview of Small Modular Reactors

2.1 History

The history of small nuclear power in the United States has deep roots in the successful development and deployment of small reactor systems for marine propulsion by the US Navy. It began with the launch of the USS Nautilus, the first nuclear-powered submarine, in 1954, followed by the USS Enterprise, the first nuclear-powered aircraft carrier, six years later. The Navy's Nuclear Power Program, under the guidance of Admiral Hyman Rickover, played a crucial role in the selection of light-water reactor technology as the basis for its fleet of naval vessels. Water-cooled reactors became the propulsion unit of choice due to their successful operation and safety record.

The Navy's Nuclear Power Program continues to be highly successful, with its vast experience and expertise being utilized in the development of commercial Small Modular Reactors (SMRs). Many engineers and managers involved in commercial nuclear power originally gained their experience in the nuclear Navy, and some of the current SMR vendors tap into the mature expertise of the Navy's manufacturers and component suppliers. Additionally, certain SMR designs being developed in other countries, such as Russia, have evolved directly from marine propulsion systems.

The US Air Force and US Army also embarked on nuclear power programs, exploring the use of small nuclear reactors for aircraft and long-range bombers. Although less enduring than the Navy's program, these efforts led to considerable learning and technology development relevant to commercial nuclear power, including SMRs. The Aircraft Nuclear Propulsion program explored using small reactors to power long-range bombers, while the Army Nuclear Power Program aimed to provide power to remote installations where traditional fuel resupply was challenging. The Army's program showcased the importance of designing modular plants and minimizing on-site construction, which are key features in many contemporary SMR designs.

While the military's use of nuclear power was successful in specific applications, such as powering submarines and aircraft carriers, it also led to some interesting and less practical ideas, like nuclear-powered tanks. However, the lessons learned from these military nuclear power programs continue to influence the development of modern SMRs, shaping their design, construction, and deployment for a range of commercial applications.

The commercialization of nuclear energy in the US followed the Navy's successful application of nuclear power for marine propulsion. In 1955, President Eisenhower proposed the construction of the nuclear-powered NS Savannah as a demonstration of the peaceful use of nuclear power. The Savannah, a stylish ship resembling a cruise liner, was launched in 1962 and traveled to numerous domestic and foreign ports before being retired in 1971. Several other nuclear-powered merchant ships were also constructed, including the Otto Hahn, Sevmorput, and Mutsu.

The Otto Hahn's 38MWt reactor is particularly noteworthy because it was the first commercially deployed example of an integral Pressurized Water Reactor (PWR). This integral configuration, where all primary system components are contained within a single vessel, has been widely used in many SMR designs due to its simplicity and enhanced safety.

Russia's fleet of nuclear icebreakers, while not for military or commercial use, also extends the navigable season of the Arctic Ocean and serves as a basis for some of Russia's entries into the SMR market.

The early land-based reactors for commercial power production in the late 1950s and early 1960s were essentially scaled-up versions of naval PWR plants. These early plants were designed to provide the fledgling commercial nuclear power industry with experience in construction and operation. As electricity demand grew rapidly in the US, utilities ordered larger plants exceeding 1300MWe, driven by the confidence in nuclear plant safety and the principle of "economy of scale."

The 1973 energy crisis, caused by the oil embargo, further boosted the interest in nuclear power, as crude oil and coal prices skyrocketed. This crisis led to studies exploring nuclear power for industrial heat applications rather than just electricity generation. Smaller-sized nuclear units were considered a better match for industrial energy demands, and several small reactor concepts were explored, including industrial energy PWR and Boiling Water Reactors (BWR) designs, as well as gas-cooled pebble-bed Gas Cooled Reactor (GCR) designs.

However, growing anti-nuclear sentiments in the mid-1970s cast a shadow over the nuclear industry, leading to the discontinuation of some small reactor designs. Despite the challenges, the experience gained during this period laid the groundwork for the development of modern SMRs, which are now being pursued by various countries and industries worldwide.

[1] [2]

2.2 Definition

There is not a universal definition of an SMR. Different institutions have different definitions, though many of them have common features. Some of the definitions are listed below.

IAEA [3] defines SMRs as reactors that have a power capacity of up to 300 MWe per unit, they are advanced and produce low-carbon electricity, physically small in comparison to conventional nuclear power reactor, the modularity makes it possible for the components to be made and assembled in factory and installed in location.

NRC [4] defines an SMR as a light-water reactor generating 300 MWe or less.

WENRA [5] in the Report on Applicability of the Safety Objectives to SMRs uses a following definition, labeling it as 'commonly used definition': SMRs are considered to be nuclear reactors that have several of the following features:

- a power < 300 MWe or < 1000 MWt;
- designed for commercial use i.e., electricity production, desalination, district heating, process heat (as opposed to research and test reactors);
- designed to allow addition of multiple units / modules in close proximity to the same infrastructure;
- could be built and assembled in factories to a greater extent than traditional reactors and shipped to utilities for installation as demand arises;

Furthermore WENRA notes that some SMRs use novel designs that have yet to be widely analysed or licensed by regulators.

Advantages of SMRs in comparison to regular nuclear powerplants include lower building cost and shorter building time. Furthermore, with many smaller reactors rather than a few big ones there can be a chance to load-follow, which is increasingly important since there is a phase out of coal as a source of energy and many of the renewable sources such as wind and solar cannot be controlled.

2.3 Number of concepts

In IAEA ARIS database there are currently (12.1.2024) listed 48 SMR concepts. However there are many SMRs missing from the database and are instead listed in a supplement publication Advances in Small Modular Reactor Technology Developments, commonly reffered to as the SMR Book. In the 2022 edition of the

SMR Book there are 67 concepts listed. That is the most complete database of SMR, however, there are even more concepts in the development that. The real number can be estimated at around 100 SMRs. [6]

Recently there have been multiple projects trying to connect the teams developping the SMRs, so they communicate and can cooperate and learn from each other. Those projects include Harmonise and SASPAM. [7]

HARMONISE project has set five objectives:

1. To analyse preliminary safety assessments of innovative fission and fusion installations,
2. To peruse the licensing needs for innovative nuclear installations,
3. To examine risk-informed, performance-based approaches in licensing reviews and regulatory decision-making,
4. To delimit harmonisation and standardisation on component assessments, methodologies, codes and standards,
5. To learn from earlier experience in harmonisation efforts.

This is to be achieved by semiannual workshops, organized in sequence of one virtual and one in person/hybrid.

[7]

2.4 Types

SMRs can be divided into different categories according to many parameters. They can be small or micro-sized. Micro-sized reactors are defined [8] as having maximum 20 MWt power and could work both as a part of the electric grid or independently in an own microgrid. According to NEA [9] there can be also divisions such as mobile vs stationary reactors and single module vs multi-module reactors, depending if it is designed so there are several reactors stacked together or if it is a stand-alone reactor. Another division is marine-based versus land-based reactors. Then there also is the classical division used in big nuclear reactors which is according to the type of coolant or moderator or division by neutron energy.

The IAEA SMR Book [3] uses distinction into six categories: Water cooled SMRs - land based, water cooled SMRs - marine based, high temperature gas cooled SMRs, fast neutron spectrum SMRs, molten salt reactors and micro modular reactors. This work will focus on land-based reactors, therefore only five categories out of these six are relevant. It is also possible for a reactor to fall into more of these categories. Following list gives relevant examples from each category, taking in consideration CEZ shortlist of possible SMRs built in the Czech Republic.

1. Water-cooled

   The **BWRX-300** is a small modular nuclear reactor designed by GE Hitachi Nuclear Energy, a collaboration between Japan and the U.S. It is a BWR that uses natural circulation. The BWRX-300 is designed to be more efficient, cost-effective, and flexible than traditional nuclear reactors.

   The power is 870 MWt and 270 - 290 MWe. The fuel is uranium dioxide with under 5 % enrichment in a ten-by-ten array. There are 240 fuel assemblies in the core. Refuelling cycle is planned 12 to 24 months and design life of the reactor is sixty years. Reactivity control mechanism is rods and solid burnable absorber (B_4C, Hf and Gd_2O_3).

   One of the main advantages of the BWRX-300 is its size. The total plant footprint is 9800 m^2, allowing for a wider range of locations. The plan is to have an emergency planning zone (EPZ) at the site boundary.

   The BWRX-300's main design features include the Nuclear Steam Supply System (NSSS), which consists of the Reactor Pressure Vessel (RPV) and fine motion control rod drives. The reactor core is arranged as an upright cylinder containing fuel assemblies, using GNF2 fuel with inherent reactivity control mechanisms. The Reactivity Control system relies on control rods loaded with B4C or Hf neutron absorbers and burnable neutron absorbers within fuel rods.

   Safety is a top priority, and the BWRX-300 adopts a defense-in-depth approach. Its Engineering Safety System Approach utilizes inherent margins and natural phenomena-driven safety features, minimizing the need for AC power during accidents. The Decay Heat Removal System effectively cools the reactor during shutdown, while the Emergency Core Cooling System (ICS) provides passive decay heat removal for extended periods without operator intervention.

The BWRX-300's plant layout includes the Reactor Building (RB) housing the PCV and RPV below grade. Three ICS pools sit next to the pool above the PCV, providing efficient cooling. The Turbine Building (TB) encloses the turbine, generator, and various systems, while the Control Building (CB) houses control and instrumentation equipment.

The BWRX-300 design has undergone pre-application reviews with regulatory authorities in the UK, US, and Canada, and several Licensing Topical Reports have been submitted and approved. The fuel cycle approach is similar to operating BWRs, with refueling outages lasting 10-20 days, and cycle durations ranging from 12 to 24 months.

The waste management and disposal plan follows best practices from the BWR fleet, segregating waste for optimal treatment, storage, and final disposal. The BWRX-300's comprehensive safety features, design philosophy, and adherence to regulatory guidelines make it a promising candidate for future SMR deployments.

With an expected commercial operation in 2028, the BWRX-300 is positioned to address various energy generation needs while prioritizing safety, simplicity, and cost-effectiveness. Its adaptability to load-following requirements and use in district heating, synthetic fuel production, and hydrogen production further highlights its versatility.

[10] [6]

The NuScale Power Module™ is a cutting-edge SMR developed by NuScale Power Corporation in the United States. The NuScale VOYGR™ SMR plants are designed to offer scalable and flexible electricity generation solutions. The modular approach allows customization to meet varying energy demands, with standard plant configurations such as VOYGR-4 (308 MW(e)), VOYGR-6 (462 MW(e)), and VOYGR-12 (924 MW(e)).

The NuScale VOYGR SMR is an integral PWR that utilizes light water as both coolant and moderator. The thermal capacity is 250 MWt, and the gross electrical capacity is 77 MWe. The primary circulation is driven by natural circulation, eliminating the need for reactor coolant pumps. The reactor operates at a primary operating pressure of 13.8 MPa and a core inlet/outlet coolant temperature of 249 °C/316 °C. The core comprises 37 UO2 fuel assemblies with Gd2O3 as a burnable absorber. The fuel enrichment is up to 4.95 %.

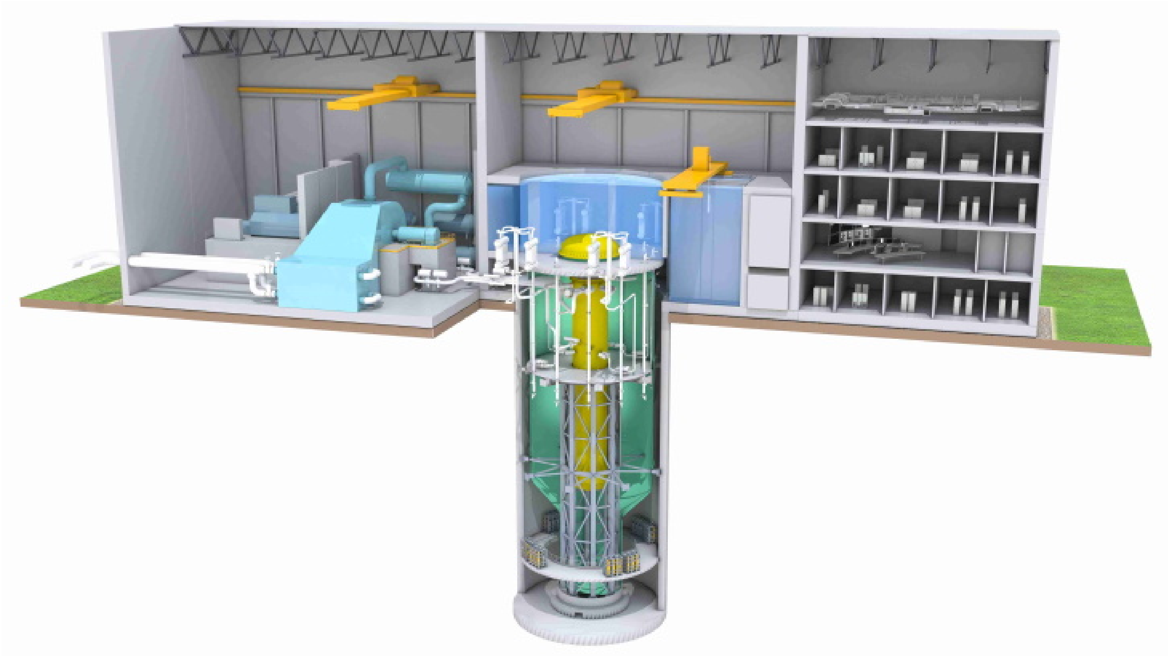

Fig. 2.1: BWRX-300 plant layout [10]

The NuScale VOYGR SMR design is founded on the principles of simplicity, proven light-water reactor technology, and passive safety systems. The innovative features include an unlimited time for core cooling without the need for AC or DC power, water addition, or operator action. The safety approach incorporates integral primary system configuration, a containment vessel, and passive heat removal systems, ensuring reliable long-term core cooling even under severe accident conditions.

The nuclear steam supply system (NSSS) includes the reactor core, helical coil steam generators, and a pressurizer within a reactor pressure vessel (RPV). The reactor coolant system operates through natural circulation, removing the requirement for reactor coolant pumps. The RPV contains the core and control rod drive mechanisms, while the containment vessel encloses the NSSS and provides heat rejection to the reactor pool.

The NuScale VOYGR SMR adopts a fully passive safety design, proven by the NuScale Triple Crown for Nuclear Plant Safety™. The engineered safety systems include the Decay Heat Removal System (DHRS) and the Emergency Core Cooling System (ECCS). The DHRS provides secondary side reactor cooling, while the ECCS utilizes reactor vent valves and recirculation valves to manage decay heat removal during loss of feedwater flow scenarios.

The plant consists of a reactor building, control building, two turbine-generator buildings, a radwaste treatment building, forced-draft cooling towers, and a dry-cast storage area for discharged fuel. Each Nuclear Power Module (NPM) operates immersed within a common reactor pool, with a dedicated concrete cover serving as a biological shield. The main control room houses all NPMs, allowing control by a single team.

The plant footprint is $140000\,\mathrm{m}^2$ which is rather large when compared to other SMR plant concepts, however this is due to the plan of having multiple reactor units stacked next to each other as well as the sheer size for achieving natural circulation in a PWR.

The journey of NuScale VOYGR SMR has seen significant milestones, starting with the initial concept in 2003 and the establishment of NuScale Power, LLC in 2007. The Design Certification Application (DCA) was submitted to the U.S. NRC in 2016, and in 2020, the NRC issued the Standard Design Approval (SDA), marking a historic achievement for SMR technology. NPM production commenced in 2022, and the first commercial VOYGR-6 plant is targeted for operation in 2029.

The NuScale VOYGR SMR employs a three-batch refueling approach on an 18-month cycle, allowing for optimization based on customer requirements. The used fuel pool provides storage for up to 10 years, with plans for on-site dry-cask storage for the plant's entire 60-year life.

Spent fuel assemblies are initially stored in the used fuel pool and later moved to on-site dry-cask storage. Final disposal is expected to be in a national fuel repository when available.

The VOYGR-12 plant requires a minimum of 3 licensed operators per shift, totaling an estimated 270 plant employees for normal operation and maintenance. The U.S. design eliminates the need for a Shift Technical Advisor.

Overall, VOYGR represents a new generation of nuclear reactors that are designed to be more efficient, cost-effective, and safe than traditional large-scale nuclear power plants. It is intended to provide a low-carbon, reliable source of energy that can be used in a wide range of applications, including remote communities, industrial facilities, and as a replacement for aging fossil fuel power plants.

[6]

Fig. 2.2: VOYGR-4 reactor hall scheme [11]

Rolls-Royce Small Modular Reactor is a cutting-edge nuclear power technology developed by Rolls-Royce SMR Ltd, based in the United Kingdom. The SMR is a 3-loop PWR utilizing light water as the coolant and moderator. It boasts a significant thermal capacity of 1 358 MW and an electrical capacity of 470 MW, making it a substantial and efficient energy generation solution.

The design philosophy of the Rolls-Royce SMR is centered around optimizing the levelized cost of electricity while keeping the capital cost low. This approach aims to maximize power output, ensuring robust economics for nuclear power plant investments. To achieve rapid, certain, and repeatable construction, the design emphasizes site layout optimization, modular build, standardization, and commoditization.

Safety is a paramount consideration in the Rolls-Royce SMR design. It employs a combined system engineering and safety assessment approach to ensure multiple layers of fault prevention and protection. The system incorporates independent and diverse active and passive safety systems, with multiple redundant trains per system. Passive safety features are designed to autonomously function for 72 hours, minimizing the need for human intervention and electrical power during critical scenarios.

The Rolls-Royce SMR features both active and passive decay heat removal systems. The Condenser Decay Heat Removal uses steam generators and a normal duty steam condenser to cool the primary plant, while Passive Decay Heat Removal relies on the steam generators and the Local Ultimate Heatsink system. The Emergency Core Cooling System provides essential decay heat removal through depressurization of the Reactor Coolant System and sustained supply of injected coolant by gravity feed.

The reactor circuit and other crucial systems are securely located within a steel containment vessel to confine the release of materials during faulted and accident conditions. In-vessel retention is also adopted to contain any postulated melt in severe accidents.

The Rolls-Royce SMR is designed for full compliance with the UK Grid Code, enabling frequent load following between 50% and 100% power, with a design target for lower power operations, such as house load operation.

The plant layout is designed to be flexible and adaptable, suitable for both coastal and inland sites with different soil and earth conditions. The compact site footprint of approximately 40,000 m^2 is achieved through seismic isolation for key safety areas, and a berm provides protection from external hazards.

The development of the Rolls-Royce SMR has seen significant progress over the years. In 2022, it entered formal design assessment by UK regulators, aiming for completion in time for construction to commence in 2026. The fuel cycle approach involves an 18-month fuel cycle with a three-batch equilibrium core.

Waste management and disposal systems are based on proven technologies and best practices, aiming to minimize active and non-active waste and discharges.

[6]

2. HTGR:

   The High-Temperature Gas-Cooled Reactor Pebble-bed Module (HTR-PM) is a nuclear power technology developed by INET, Tsinghua University, China. Its origins can be traced back to 1992 when the China Central Government approved the construction of the 10 MW(t) pebble-bed high-temperature gas-cooled test reactor (HTR-10) at Tsinghua University's Institute of Nuclear and New Energy Technology. Following the successful operation of HTR-10, the HTR-PM project was initiated in 2001.

   The HTR-PM is based on a modular pebble-bed High-Temperature Gas-Cooled Reactor (HTGR) design that utilizes helium as the coolant/moderator and graphite as the core material. The reactor has a thermal capacity of 2 x 250 MW(t) and can produce 2 x 210 MW(e) of electrical power. The primary circulation is achieved through forced circulation, and the NSSS (Nuclear Steam Supply System) operates at 7 MPa for the primary system and 13.25 MPa for the secondary system. The reactor core inlet temperature is 250°C, while the outlet coolant temperature reaches 750°C. The fuel consists of spherical elements with coated particle fuel, enriched to 8.5%, and the core discharge burnup can reach 90 GWd/ton. The reactor utilizes an on-line refueling approach for efficient operation.

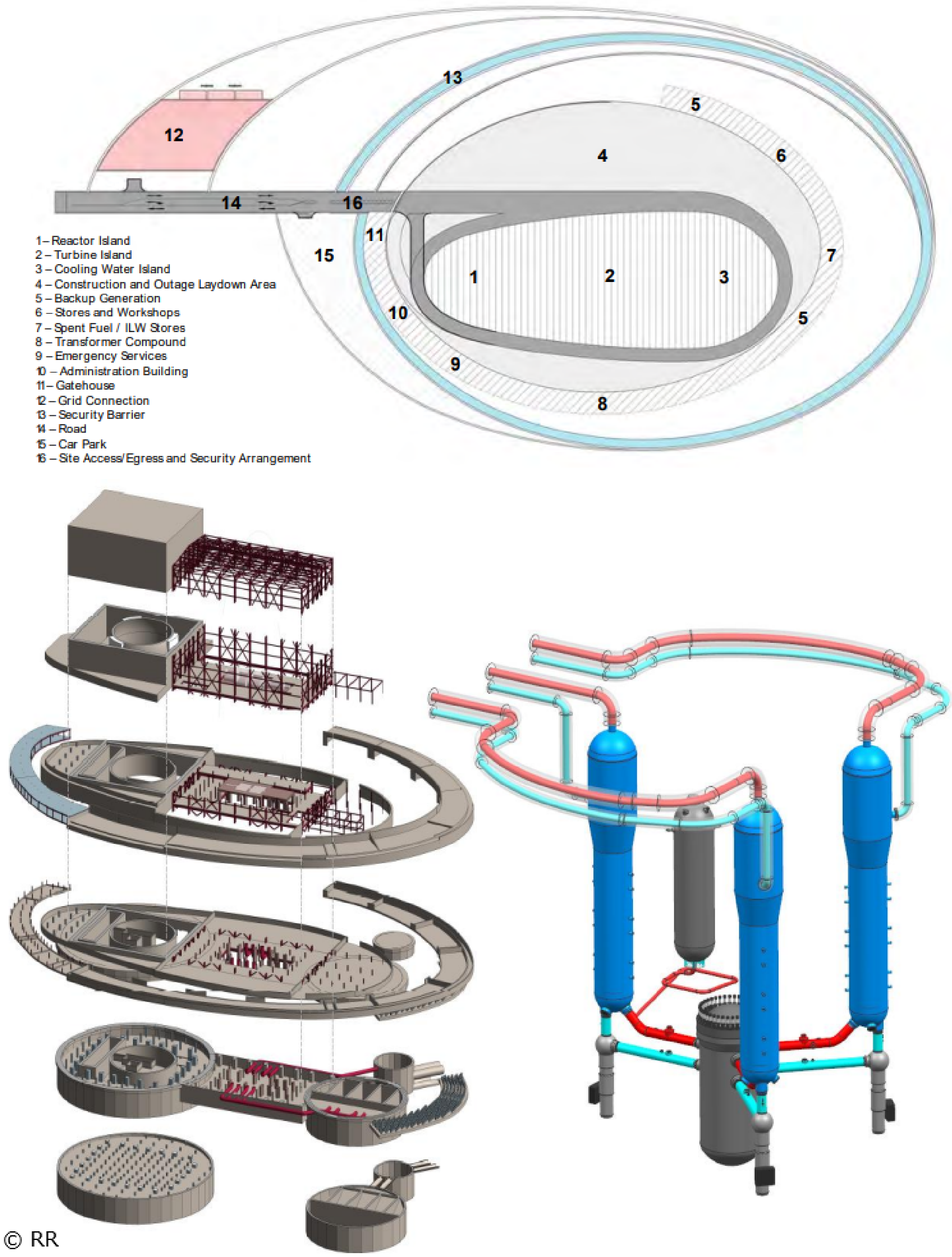

Fig. 2.3: Rolls Royce SMR plant layout and reactor loops model [12]

A notable feature of the HTR-PM is its inherent safety design, eliminating the need for offsite emergency measures. The reactor incorporates multiple safety features, including a large negative temperature coefficient, a significant temperature margin, and low excess reactivity due to on-line refueling. The control rods are employed to ensure safe operation and limit accident temperatures.

The Reactor Pressure Vessel (RPV) and internals are designed to retain radioactive materials through multiple barriers. The fuel elements, containing coated particles, serve as the first barrier, while the RPV and pressure vessels of primary components form the second barrier. The HTR-PM also features a vented low-pressure containment system to mitigate the impact of accidents.

The HTR-PM is designed in compliance with safety regulations and has undergone extensive tests and experiments to validate its safety performance. The reactor's core damage frequency from plant faults is reported to be less than 1E-07 per year of power operation, ensuring a balanced risk profile.

The primary application of the HTR-PM is electricity production as a commercial demonstration unit. It comprises two NSSS modules coupled with a 210 MW(e) steam turbine. The modular design allows for improved availability compared to power plants with periodic fuel loading.

The development milestones of the HTR-PM demonstrate significant progress, with construction starting in 2012 and various phases of testing and commissioning completed. The operation license and grid connection were achieved in 2021, with full power operation targeted for 2022.

[6]

HTR-10 is a pebble bed modular high-temperature gas-cooled test reactor developed by Tsinghua University's Institute of Nuclear and New Energy Technology (INET) in the People's Republic of China. Its construction was approved by the China Central Government in 1992, and it achieved full power operation in 2003. The primary goal of the HTR-10 project is to explore the technology and safety features of high-temperature gas-cooled reactors (HTGRs), as well as to establish an experimental base for process heat applications.

The HTR-10 has a thermal capacity of 10 MW and electrical capacity of 2.5 MW. Its reactor core, operating with helium as the coolant and graphite

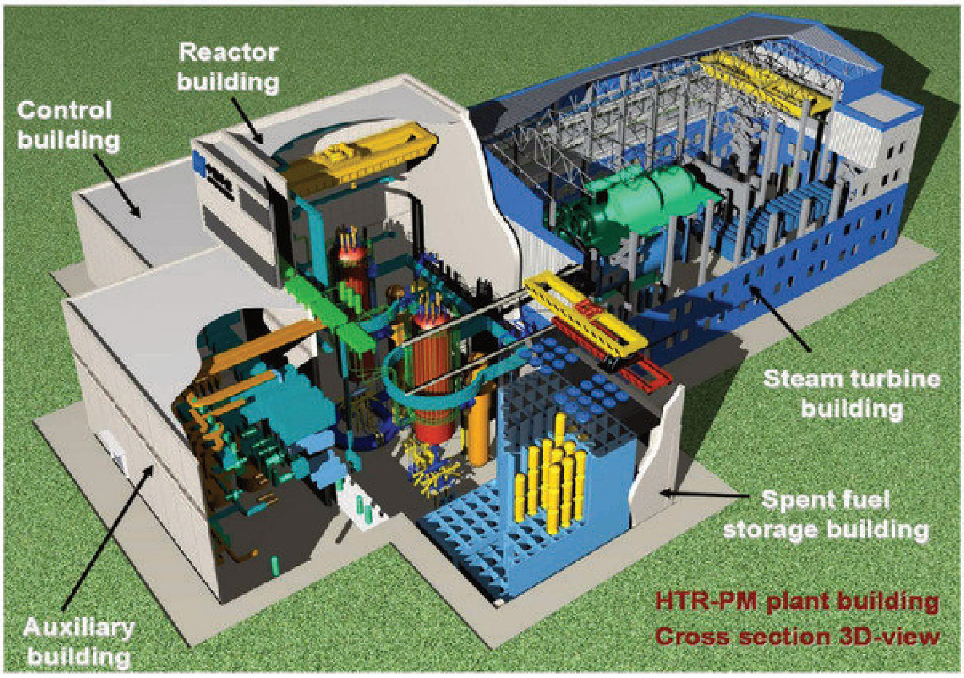

Fig. 2.4: HTR-PM plant building cross section [13]

as the moderator, consists of approximately 27 000 spherical fuel elements containing TRISO (Tristructural Isotropic) particles with UO2 (uranium dioxide) kernels. The fuel elements have an enrichment level of 17% and are designed for a mean discharge burnup of 80 000 MWd/tU.

Safety features of the HTR-10 include inherent safety characteristics that automatically shut down the reactor due to negative temperature reactivity coefficients and passive removal of decay heat from the core to the environment. The reactor's reactivity is controlled through on-line refueling, and two independent shutdown systems are available for added safety.

The reactor pressure vessel, steam generator pressure vessel, and hot gas duct pressure vessel form the primary pressure boundary of the HTR-10. Cold helium channels within the side reflector allow the helium coolant to flow upward, reversing its flow direction at the top of the reactor core before entering the pebble bed in a downward flow pattern.

The HTR-10 is equipped with a fuel handling system designed to handle the spherical fuel elements used in the reactor. The control system of the HTR-10 utilizes a distribution control system with full digitalization.

The plant layout arrangement of the HTR-10 includes the reactor building, turbine/generator building, two cooling towers, and a ventilation center with a stack, all situated on an area of 100 x 130 square meters. The design philosophy of the HTR-10 emphasizes a modular approach with components arranged to facilitate maintenance and mitigate accidents, such as water ingress into the core.

As of its current status, the HTR-10 is operational, and plans for the extension of its operating license are underway. The reactor follows a once-through fuel cycle, and its waste management and disposal plan will be included in the national plan for test facilities.

Throughout its development, the HTR-10 has served as an essential test platform for exploring high-temperature gas-cooled reactor technologies and demonstrating inherent safety features critical for the advancement of modular HTGRs.

[6]

The High Temperature Engineering Test Reactor (HTTR) is Japan's first High Temperature Gas-cooled Reactor (HTGR), located at the Oarai Research and Development Institute of the Japan Atomic Energy Agency (JAEA). The HTTR has been designed with superior safety features, utilizing coated fuel-particles, a graphite moderator, and helium gas coolant. Its ability to provide high-temperature heat above 900°C makes it suitable for power generation and various industrial applications. JAEA conducted several tests and operational achievements to demonstrate its safety and viability.

The HTTR's objectives include establishing and upgrading the technological basis for advanced HTGR, conducting innovative basic research in high temperature engineering, and demonstrating high-temperature heat applications and utilization achieved from nuclear heat.

The reactor building is designed with five levels of three underground floors and two upper ground floors, with the containment steel vessel housing the reactor pressure vessel, intermediate heat exchanger, and other heat exchangers in the cooling system. The core design incorporates specific safety features to ensure safe operations as a test reactor.

Main Design Features:

- Reactor Core: The reactor core consists of graphite and metallic core support structures accommodating prismatic fuel blocks. It includes 30 fuel columns and 7 control rod guide columns in the active core region, surrounded by a permanent graphite reflector.
- Fuel: The HTTR uses TRISO-coated fuel particles with UO2 fuel kernels, encapsulated by layers of PyC and SiC. Approximately 13,000 CFPs are fabricated in a graphite matrix of fuel compacts, forming 150 fuel assemblies with 31 or 33 fuel rods each.
- Reactivity Control System: The HTTR features a control rod system with 16 pairs of control rods made of B4C and a reserve shutdown system (RSS) using B4C/C pellets. Both systems ensure stable and safe reactor shutdown.

Safety Features:

- Chemically Stable Coolant: Helium coolant is chemically stable, preventing hydrogen gas production in accidents.
- TRISO-Coated Fuel Particles: TRISO-coated fuel particles offer excellent heat resistance, maintaining fuel temperature below 1600°C to prevent fuel damage.
- Graphite-Moderated Core: The graphite core provides a negative reactivity coefficient and high thermal conductivity, ensuring inherent removal of residual heat without excess emergency safety systems.

Various operational tests have been conducted to confirm plant safety and operational stability. These tests include pre-operational tests, start-up physics tests, rise to power tests, and safety demonstration tests, which successfully demonstrated the HTTR's inherent safety.

The HTTR's instrumentation and control systems consist of various sensors, operation mode selector, reactor power control system, and safety protection systems to ensure proper monitoring, operation, and reactor protection.

The plant area covers 200 m × 300 m and includes the reactor building, cooling towers, exhaust stack, laboratory building, and auxiliary facilities.

The HTTR construction started in 1991, with first criticality achieved in 1998. It received permission to restart operations in July 2021.

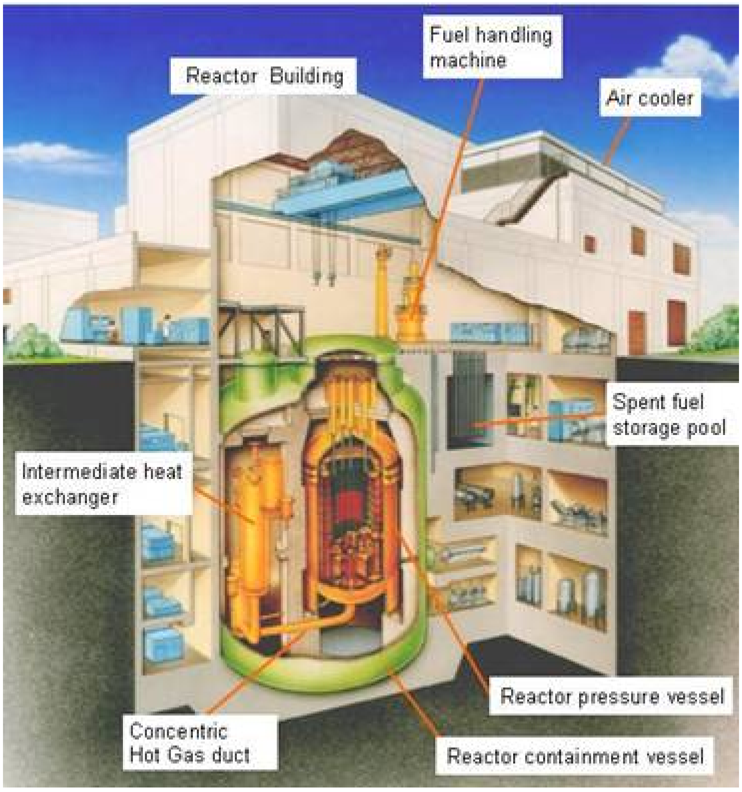

Fig. 2.5: HTTR power plant layout cross section [14]

Future plans for the HTTR include safety demonstration tests, international cooperation projects, and hydrogen production utilizing high-temperature heat from the reactor.

Overall, the HTTR stands as a pioneering HTGR in Japan, showcasing advanced safety features and potential applications for high-temperature heat utilization

[6]

3. Fast:

The **4S** (super-safe, small and simple) is an innovative small sodium-cooled pool-type fast reactor with metal fuel, developed by Toshiba Energy Systems & Solutions Corporation in Japan. It offers two power output options: 30 MW(t) or 10 MW(e), and 135 MW(t) or 50 MW(e), depending on demand analysis. Designed for multi-purpose applications, the 4S reactor serves as a distributed energy source, catering to remote areas, mining sites, and non-electric applications.

Using metal fuel (U-Zr alloy) with an enrichment of less than 20%, the 4S reactor has a core lifetime of around 30 years for the 10 MW(e) core. The reactor core is unique in that it eliminates the need for refueling during its lifetime. It achieves negative reactivity temperature coefficients, ensuring passive safety features and simplifying reactor operation. The primary shutdown system involves dropping reflector sectors, while the back-up shutdown system inserts the ultimate shutdown rod from the core center.

Decay heat removal is handled by a water/steam system during normal shutdowns. For accidents where the water/steam system is unavailable, two passive systems, the Reactor Vessel Auxiliary Cooling System and the Intermediate Reactor Auxiliary Cooling System, provide independent decay heat removal. Spent fuel cooling is managed without the need for a spent fuel pool. The containment system consists of a cylindrical/spherical design, with nitrogen gas provided inside the top dome to mitigate sodium fire.

The 4S reactor prioritizes simplicity and inherent safety features, aligning with the defense in depth strategy. It operates without active involvement from plant operators due to features like automatic burn-up reactivity compensation and the absence of fuel reloading during its core lifetime. The instrumentation and control system includes safety-related and non-safety related systems, ensuring reliable plant operation.

The plant layout is optimized for functional needs, safety, and construction considerations. The reactor building is embedded underground to enhance security and protection against external events. The balance of plant, including the steam turbine system, is situated at ground level. Testing for design verification and validation has been performed, demonstrating the reliability and performance of the 4S design.

Licensing activities with the U.S. NRC have been initiated, and Toshiba Energy Systems & Solutions continues to work on the detailed design and safety analysis for design approval. The 4S reactor can be applied to either once-through or closed fuel cycle schemes, depending on the user country's fuel cycle policy.

[6]

4. MSR:

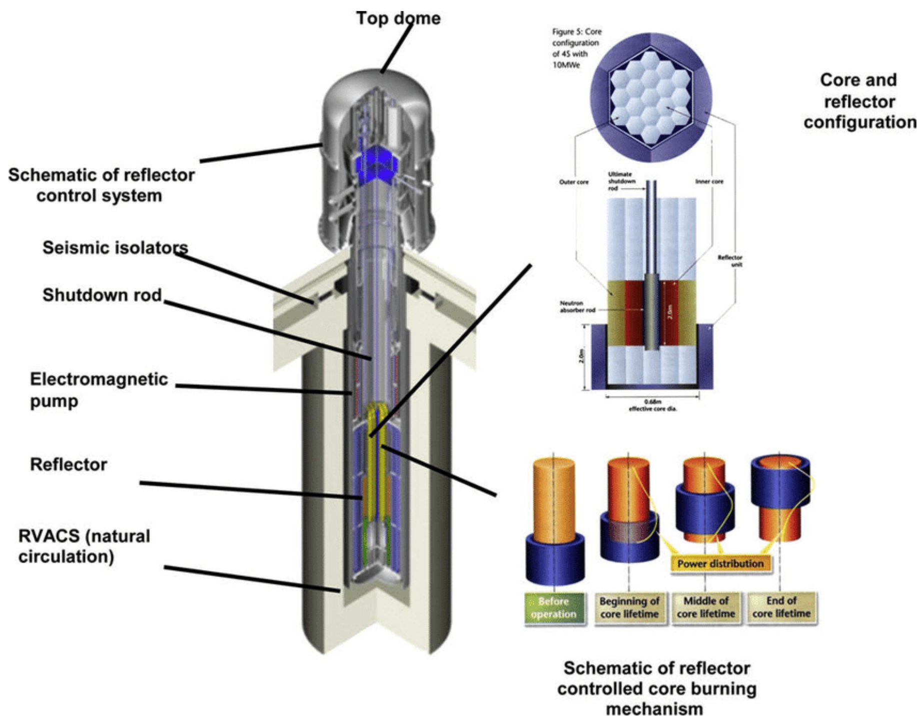

Fig. 2.6: 4S reactor scheme [15]

The **lithium-fluoride thorium reactor** (LFTR) is an advanced nuclear reactor design developed by Flibe Energy, Inc. in the United States of America. It operates as a graphite-moderated, thermal-spectrum reactor that utilizes a unique combination of liquid fluoride salts containing both fissile and fertile materials. The primary goal of the LFTR is to produce electricity at a low cost by efficiently utilizing thorium as a fuel source.

LFTR employs a liquid fluoride salt mixture consisting of LiF-BeF2-UF4 fuel salt and graphite as the moderator. The fuel enrichment is not applicable, as it utilizes 233U derived from thorium as its primary fissile material. This is achieved through a continuous refueling cycle, where 233U is produced in the blanket region of the reactor by neutron capture and beta decay of 232Th.

One of the key features of LFTR is the use of mixtures of fluoride salts, which become liquid at high temperatures, creating an optimal environment for nuclear fission reactions. These fluoride salts have an inherent ionic bond structure that prevents radiation damage and enables the reactor to operate at high temperatures while maintaining essentially ambient pressure.

The LFTR's high operational temperatures (ranging from 500 to 700 degrees Celsius) make it ideal for coupling with a closed-cycle gas turbine power conversion system. The reactor can achieve high energy conversion efficiencies, reaching approximately 45%, using a supercritical carbon dioxide gas turbine employing the recompression cycle.

The core design of LFTR consists of two regions: the feed region and the breed region. It operates on a closed fuel cycle based on thorium. Within the reactor vessel, two plena are incorporated—one for the active core region and the other for the outer blanket area—both filled with fluoride salt. The blanket region facilitates the conversion of thorium (232Th) to uranium-233 (233U) through neutron capture and beta decay. These fissile materials are then separated and reintroduced into the fuel salt mixture for fission. The LFTR's design ensures that almost all the energy content of thorium is extracted, making it an almost unlimited and cost-effective resource.

Safety is a paramount concern in the LFTR design. It incorporates a passive shutdown and heat removal system, which automatically activates in case of reactor overheating or coolant flow loss. The freeze valve within the primary loop fails open when necessary, allowing the fuel salt to drain into a separate fuel salt drain tank with a cooling system, preventing any criticality issues.

The fluoride salts used in LFTR have exceptional chemical stability, but they require specific alloys to avoid corrosion. Graphite, which serves as the moderator, is not wet by the fluoride salts and does not require cladding. The LFTR's design accounts for potential dimensional distortion of graphite over time and compensates for it accordingly.

At present, the LFTR design is in an early stage of development, and licensing activities have not yet commenced. Nevertheless, LFTR technology shows great promise for achieving efficient, sustainable, and low-cost electricity generation by harnessing the abundant thorium resources and reducing waste production compared to traditional nuclear reactors. As it progresses, LFTR has the potential to revolutionize the future of nuclear power and contribute significantly to clean and sustainable energy solutions.

[6]

5. micro:

Energy Well (EW) is a Fluoride High-temperature Micro Reactor project currently being developed in the Czech Republic by Centrum výzkumu Řež. The primary objective of this project is to create an advanced, inherently safe, low-power high-temperature reactor. The main application of EW is to provide a stable and clean energy source for both remote and populated areas, with a focus on electricity, heat, and hydrogen production for energy storage. The reactor is designed to be transportable and capable of operating in synergy with large-scale nuclear power reactors, heating plants, and renewable energy sources.

The EW reactor is designed with a focus on passive safety and simplicity. It adopts a 7-year fuel cycle, low power density, and high use of passive safety systems. The modular design approach minimizes on-site welding operations, enhancing ease of construction and maintenance.

The EW reactor features a thermal capacity of 20 MW(t) and an electrical capacity of 8 MW(e). The primary circulation utilizes forced circulation, while the coolant/moderator employed is molten salt FLiBe. The reactor core consists of 25 hexagonal fuel assemblies, 6 central graphite blocks, and an external graphite reflector, with precise control enabled by 19 control rods. The fuel characteristics include the use of TRISO (Tristructural Isotropic) spherical fuel particles enriched to 15% uranium. The refueling cycle is set at 7 years. The reactor coolant system utilizes molten fluoride salt (FLiBe) containing lithium and beryllium as the primary coolant, while the secondary circuit effectively separates the primary and tertiary circuits, using either NaBF4 or other salts.

EW implements passive safety systems and relies on inherent features for reactor shutdown and heat removal. The primary circuit operates at atmospheric pressure, and the reactor core is situated underground. In case of loss of flow, passive residual heat removal takes place through the reactor vessel. The fuel assemblies, as well as reactor and containment vessels, act as barriers to prevent the spread of fission products in the event of any accidents.

The power plant employs three cooling circuits: liquid fluoride salts (FLiBe, NaBF4) in the primary and secondary circuits and supercritical carbon dioxide (sCO2) in the tertiary circuit. The tertiary circuit utilizes the sCO2 in an Ericsson–Brayton-based cycle to transform the heat into electric power, resulting in high thermodynamic efficiency.

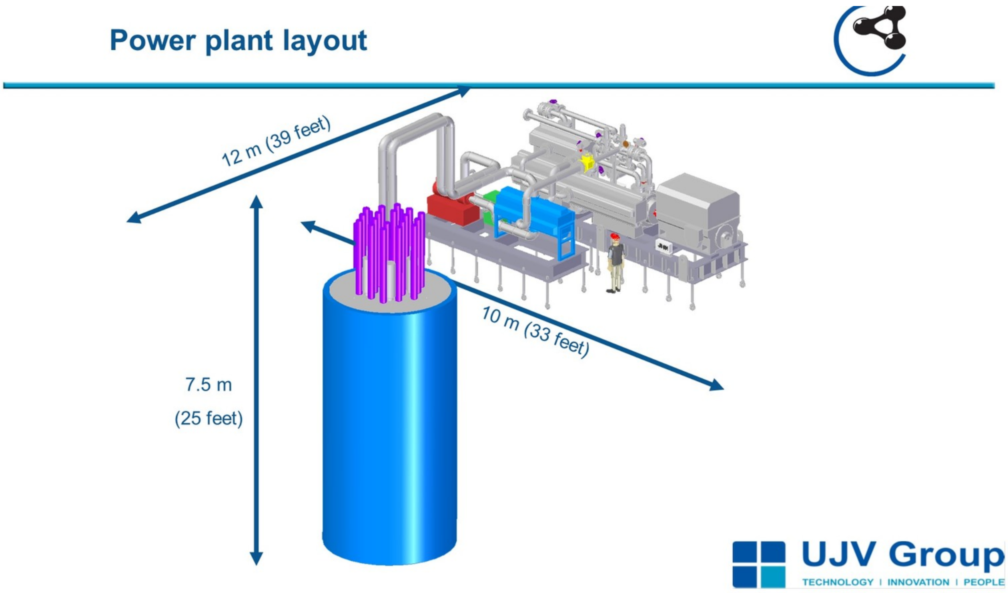

Fig. 2.7: EW power plant layout [16]

The development of EW is ongoing, and the project is in the process of further refinement and verification through experiments and design work.

[6]

2.5 Safety, Security and Safeguards

For the past two decades or more, "Safety by Design" and "Safeguards by Design" have been integrated into the design process of conventional reactors. A more recent approach, "Security by Design," takes this concept further, involving the analysis and incorporation of nuclear Safety, Security, and Safeguards (3S) provisions and features right from the initial stages of nuclear reactor design and construction. Since many SMRs are still in the conceptual or design phase, designers now have a unique opportunity to proactively include various safeguards and security features in their designs. The "Security by Design" analysis can be achieved using fault tree approaches, similar to probabilistic safety analysis, and/or consequence-based graded approaches to security. Early considerations can be factored into design elements, such as fuel element size, core lifetime and burnup, and excess reactivity, ensuring enhanced safety and security measures from the very beginning. [17]

Examples of the passive safety systems for different reactor types can include following:

Advanced BWR:

- ECCS: Utilizes gravity-driven systems and accumulators to provide water injection into the reactor core in case of accidents, ensuring cooling without active pumping.
- Passive Containment Cooling System: Employs natural circulation and condensation processes to remove heat from the containment structure during accidents.

High-Temperature Gas-Cooled Reactor (HTGR):

- Helium-Cooled Reactor Design: Uses helium as a coolant, which is inherently stable and does not react with air or water, providing passive safety against coolant-related accidents.
- Triso Fuel Particles: Incorporates TRISO fuel particles with multiple layers of containment, reducing the risk of radioactive release during accidents.

Molten Salt Reactor:

- Freeze Plug: Utilizes a freeze plug mechanism that, in case of power loss or overheating, allows the fuel salt to solidify and drain into a safe containment, preventing core damage.
- Passive Decay Heat Removal: Relies on natural convection and heat transfer to remove decay heat from the reactor core, eliminating the need for active cooling systems.

Liquid Metal-cooled Fast Reactor:

- Passive Shutdown Systems: Employs materials with strong negative reactivity feedback to ensure automatic shutdown in case of temperature increase or power excursion.
- Natural Circulation: Utilizes natural circulation of the liquid metal coolant to remove heat during normal operation and accidents without the need for pumps.

Fluoride High-Temperature Reactor:

- Atmospheric Pressure Primary and Secondary Circuits: Operating at atmospheric pressure reduces the risk of pressure-related accidents and simplifies safety measures.

- Passive Residual Heat Removal: Employs passive mechanisms to remove decay heat from the primary circuit in case of flow loss or accident conditions

In the realm of SMRs, challenges concerning 3S have been a focal point of discussion and analysis in the published literature. The most extensive examination has been devoted to safety considerations, particularly the concept of "inherent safety" or "passive safety systems" inherent in SMR designs. Unlike traditional light water reactors, which rely on active safety systems requiring external mechanical or electrical input, nearly all SMRs incorporate inherent and passive safety features. These systems operate independently of emergency power and eliminate the need for auxiliary feedwater subsystems, contributing to enhanced reliability. Examples of passive safety systems in SMRs include passive condensers, gravity-driven injection, and heat removal via natural convection through the containment liner.

Safeguards for SMRs present another challenge, with the literature acknowledging the impact of SMR characteristics on the traditional International Atomic Energy Agency (IAEA) comprehensive safeguards agreement-based regime. Low thermal signatures, extended reactor core life, and infrequent refueling rates are among the unique aspects of SMRs that challenge the current safeguards paradigm. Proposed solutions often center around the concept of "safeguards-by-design," incorporating technical and procedural elements to increase diversion difficulty of nuclear materials in basic engineering steps for facility operations. However, implementing safeguards at SMR facilities requires further exploration and adaptation of existing guidance.

[18]

Security by Design (SeBD) is a comprehensive concept that incorporates security principles and measures into all phases of facility design, construction, operation, and decommissioning. It aims to create a robust and effective physical security infrastructure to protect against potential malicious acts and evolving threats, particularly in the context of nuclear facilities and SMRs. SeBD involves a proactive and integrated approach that involves various disciplines, including engineering, safety specialists, security professionals, and operators, working together to optimize security features.

Key principles of Security by Design include:

1. Integrated approach: SeBD promotes collaboration between engineering and safety specialists to achieve integrated security systems. This involves integrating the expertise of various professionals, such as physical and cyber

security specialists, during the design process to create a holistic and effective security solution.

2. Inherently secure: The concept of inherent security advocates for incorporating security considerations into the core design elements of plants, facilities, buildings, and systems from the very beginning. Instead of adding security measures as an afterthought, SeBD ensures that security features are an integral part of the design, making the facility inherently secure.

3. Passive security: SeBD emphasizes reducing reliance on active security measures and human interventions to counter security events. Passive security measures are designed to operate automatically or passively, minimizing the need for constant human intervention and reducing the risk of human error.

4. Evolving response: Security by Design recognizes the importance of designing security systems that can adapt and respond flexibly to changing threat levels and evolving security challenges. This adaptive approach ensures that security measures remain effective and relevant over time, even as the threat landscape evolves.

The implementation of SeBD requires an understanding of the facility's characteristics, size, and types of nuclear material involved. Conducting a security risk assessment is essential to identify credible threats and establish security priorities. Sharing threat information with approved designers ensures that mitigating measures are effectively implemented during the design phase.

SeBD is relevant to planned future SMRs. By incorporating security measures early in the design process, SMRs can be designed to reduce intrinsic vulnerabilities and minimize costs and disruptions to operations. Moreover, SeBD aims to prevent conflicts between safety and security requirements, emphasizing the importance of integrating nuclear safety and security, along with safeguards.

[19]

2.5.1 Safety and security challenges

SMRs exhibit distinct features compared to large nuclear power plants (NPPs) due to their smaller size, enabling modularization, assembly line fabrication, reduced financial risk, and flexible deployment, including off-grid applications. While these attributes have garnered significant attention in the published literature, they also present challenges in safeguarding SMR facilities against illicit proliferation, necessitating the development of appropriate safeguards and non-proliferation standards. [17]

In 2018, GNI (Global Nexus Initiative) presented four key challenges related to nuclear security and advanced reactors. These challenges are as follows:

- Physical Protection: Ensuring the physical security of nuclear facilities and materials to prevent unauthorized access, theft, or sabotage.

- Facility Sabotage and Nuclear Terrorism: Addressing the risks of deliberate acts of sabotage or nuclear terrorism targeting nuclear facilities.

- Cyber and Emerging Technologies: Addressing the security implications of cyber threats and the use of emerging technologies, such as Artificial Intelligence and blockchain, in the context of nuclear security.

- Reactor Siting: Considering the security aspects associated with the location and siting of nuclear reactors, including the vulnerability of remote locations.

During the preliminary security assessment, GNI experts evaluated different types of advanced reactors and their vulnerabilities. They found that Molten Salt and TRISO-Based reactors appeared to have low vulnerability to theft of nuclear material and dispersal of radioactivity. However, Fast Spectrum reactors, particularly those containing plutonium in fresh fuel or separated from spent fuel, presented a Category I risk (see Fig. 4.1). Below ground placement of reactors was identified as a potential measure to lower security risks. However, further analysis is required for remote locations to better understand their security challenges. The assessment also highlighted the potential role of emerging technologies like Artificial Intelligence and blockchain in addressing some security concerns.

[20]

One of the significant challenges lies in SMRs designed for remote regions, where they are fabricated, fueled, and securely sealed in a factory before being transported to their respective sites for power generation. This sealed transport approach minimizes the risks of technology misuse and material diversion. SMRs deployed in off-grid scenarios find ideal applications in catering to small remote northern communities and mining sites. Their isolated locations and limited accessibility naturally reduce the likelihood of physical attacks, especially from external adversaries. However, economic considerations may make it challenging to fully staff these SMRs with adequate manpower for complete protection against sabotage attacks. A notable subset of SMR designs proposes deploying the core module underground, introducing additional difficulties, costs, and technical challenges for facility access, necessitating robust physical protection and combat plans.

Another critical challenge pertains to cyber security. As SMRs embrace digitalization, increased automation, remote supervisory control, and maintenance, a strong cyber security program becomes essential from the outset to prevent unauthorized modifications and eliminate vulnerabilities. Establishing a well-defined cyber security classification scheme for Instrumentation and Control (I&C) architecture lays the groundwork for regulatory assessment, enabling optimal allocation of limited resources based on the relative value or significance of systems and assets throughout their lifespan. This approach becomes particularly critical when designing a licensable I&C architecture, including its concept of operations. While certain SMR designs might boast inherent walk-away safety, security requirements are more likely to be driven by the business case, focusing on reliability and availability needs, rather than solely by regulators. Neglecting to prepare for cyber security incidents can incur significantly higher costs than investing in robust cyber security measures from the outset.

SMR designs often aim to extend the operating lifetime of the reactor core, securely sealing it to facilitate safe transport and modular core replacements. By adopting a sealed core approach, access to the core, particularly at the SMR site, is restricted, thereby reducing the potential consequences of any core-related attack. However, it becomes imperative to uphold stringent security measures throughout the extended core lifespan. Reliable monitoring methods for nuclear material within sealed cores become necessary to address the absence of core access for verification purposes.

The distributed operation of SMRs, producing power directly at the point of consumption, presents both strengths and weaknesses. As the number of SMR sites increases, so does the potential target for security breaches. However, this setup allows for the establishment of a substantial security task force that can cater to a significant network of SMR sites through strategically located dispatch centers. These centers ensure a timely and efficient response in case of emergencies, justifying the larger security force by the broader coverage it provides.

SMRs' smaller fissile inventory effectively minimizes the amount of nuclear source material susceptible to theft, sabotage, or unauthorized access, thereby mitigating the potential consequences of a successful attack. However, when aiming to scale down the security infrastructure of an SMR facility in proportion to the reduced fissile inventory relative to a standard nuclear power plant, it is crucial to adopt a graded approach based on meticulous security risk analysis. Such an approach tailors security measures to the specific risk profile of each SMR facility, ensuring that the level of protection remains commensurate with the potential threats and vulnerabilities.

Analyzing advanced fuel cycles is crucial to determining the most efficient and effective security measures. Some smaller SMR designs incorporate advanced safety features, including passive safety mechanisms, which can significantly enhance safety levels. Since many radiological consequences resulting from safety accidents and security breaches are interconnected, these advanced safety features can potentially mitigate the extent of required security controls and measures. A comprehensive assessment of the security implications of various enrichment levels and fuel choices is essential to develop tailored security strategies for each SMR design.

Moreover, challenges posed by transportation to remote locations with limited access must be addressed, necessitating robust plans to handle such scenarios. Transporting a sealed and fully-loaded reactor core requires careful adherence to packaging and transport regulations for nuclear substances and dangerous goods in all countries along the transportation route. Ensuring adequate protection and maintaining a sub-critical arrangement during transport are paramount concerns.

The fuel cycle plays a crucial role in determining how used nuclear fuel is handled, safeguarded, and stored in the short term and long term. Collaboration among organizations such as the IAEA, national regulators, operators, and nuclear waste management entities becomes essential, especially for SMR designs using MOX fuels and higher enrichment levels. Adequate planning and coordination should occur before the deployment of SMRs to ensure that the spent fuel can be safely and effectively managed throughout the entire fuel cycle. By taking these proactive steps, the deployment of SMRs can be carried out in a manner that ensures the safe and responsible management of spent nuclear fuel.

[17]

3 Current regulatory framework for SMR Security

3.1 UK

Security by Design (SeBD) in the UK is a significant aspect of the regulatory framework for new nuclear power station designs. The Office for Nuclear Regulation (ONR) plays a central role in assessing and ensuring the adequacy of security measures in these designs.

The ONR has established a set of security assessment principles (SyAPs) along with supporting Technical Assessment Guides. These SyAPs outline specific security outcomes that licensees must demonstrate compliance with. SeBD is an approach that seeks to reduce vulnerabilities in the design phase rather than attempting to secure or mitigate them post-design. It aims to mitigate specific threats by employing tailored approaches, designs, or arrangements to address potential malicious acts.

In the Generic Design Assessment (GDA) process, which is essential for obtaining Design Acceptance Confirmation and Statement of Design Acceptability in the UK, security forms a major part. Design companies seeking approval for their reactor designs must submit Conceptual Security Arrangements as part of the GDA process. These arrangements should contain sufficient information for the ONR to evaluate the adequacy of the security aspects of the proposed design.

The Conceptual Security Arrangements eventually serve as the basis for a Nuclear Site Security Plan for any licensed site that adopts the approved design. This ensures that the security measures implemented at the site align with the security features specified in the generic design, maintaining consistency and effectiveness across various sites.

ONR security inspectors work collaboratively with the wider regulatory team during the GDA process to assess security aspects comprehensively. This includes evaluating physical protection, cyber and information security, and personnel security measures. The aim is to incorporate security by design throughout the entire spectrum of protective security measures, right from the early stages of the design process.

By integrating security considerations into the design process, potential vulnerabilities and threats can be effectively addressed. This proactive approach helps to create a more robust and secure nuclear facility design, minimizing risks and enhancing overall safety and security. Ultimately, the commitment to SeBD ensures that new nuclear power station designs in the UK prioritize both nuclear safety and security objectives from the very beginning. [19]

3.2 USA

In the USA, the concept of Security by Design (SeBD) is gaining prominence in the nuclear regulatory framework, particularly concerning SMRs and advanced reactor designs. The NRC is actively engaged in pre-application activities with SMR designers and is working to develop a regulatory approach that addresses the unique security challenges posed by these advanced technologies.

The NRC recognizes the importance of integrating security considerations into the design phase of nuclear facilities to reduce vulnerabilities and enhance protection against potential threats. The NRC's approach to SeBD involves working closely with industry stakeholders, including designers and licensees, to ensure that security is fully integrated into the design process from the very beginning.

To achieve this, the NRC has developed GDA processes that allow for the separate evaluation of safety, security, and environmental implications of new reactor designs. This approach enables the NRC to assess the security aspects of new designs independently of specific site applications, ensuring a comprehensive and standardized evaluation of security measures.

In its assessments, the NRC considers a variety of security challenges, including physical protection, facility sabotage, nuclear terrorism, cyber threats, and reactor siting. The focus is on reducing vulnerabilities and mitigating potential consequences of malicious acts through an integrated and risk-informed approach to security.

One of the key objectives of SeBD in the USA is to reduce reliance on traditional security measures, such as onsite armed response forces, by incorporating engineered physical security systems and features into the facilities. The goal is to tailor security arrangements to address specific threats and to implement measures that reduce or eliminate vulnerabilities during the design phase itself.

Recognizing that SMRs and advanced reactor designs may have different risk profiles compared to traditional nuclear power plants, the NRC is also exploring options to develop more flexible regulations and security requirements. This involves a shift away from prescriptive regulations to performance-based approaches that allow applicants to demonstrate their safety case and technical basis for security measures. [19]

3.3 Canada

In Canada, the Canadian Nuclear Safety Commission (CNSC) plays a crucial role in regulating nuclear activities and ensuring the safety and security of nuclear facilities, including SMRs. The CNSC has developed regulatory documents and processes to address security concerns and integrate Security by Design (SeBD) principles into the design and operation of nuclear facilities.

One of the important regulatory documents is REGDOC-2.5.2, titled "Design of Reactor Facilities: Nuclear Power Plants." This document highlights the significance of integrating 3S in the design of nuclear power plants. It emphasizes that safety measures, nuclear security measures, and nuclear material accounting and control systems must be designed and implemented in an integrated manner, ensuring they do not compromise one another.

To adapt to an evolving security environment and address evolving threats, the CNSC is moving towards a more performance-based approach with less prescriptive requirements. This approach allows for flexibility and adaptation in security measures based on risk-informed considerations. The goal is to develop a regulatory framework that considers radiological consequences and public health impacts in the event of a release, while also establishing security levels through a graded approach.

The CNSC has also engaged in discussions with industry representatives to find risk-informed criteria for nuclear security that can assist in applying a graded approach for SMRs. To support this approach, the CNSC has developed technology-neutral requirements and a risk-informed graded approach specific to SMRs and advanced reactors. The security requirements are established for all stages of the nuclear facility lifecycle, with a particular focus on the conceptual design phase. This allows for the optimization of security measures, integration of safety and security interfaces, and reduction of retrofit costs.

The graded approach considers the category of nuclear material and potential radiological consequences in the case of sabotage. Security objectives and requirements are established for each category of nuclear material and for preventing different levels of potential radiological consequences at nuclear facilities. SMR proponents are required to demonstrate their plans for preventing acts of sabotage, protecting vital areas, and incorporating SeBD principles to mitigate radiological consequences in case of sabotage.

To further support SeBD and the integration of security measures, the CNSC has developed a Pre-Licensing Vendor Design Review (VDR) as an optional service for SMR developers. This review allows CNSC staff to provide feedback early in the design process based on a vendor's reactor technology. The VDR includes an assessment of SeBD and the interfaces with safety, ensuring the robustness of structures, systems, and containment, as well as safeguards for nuclear material accounting and control. The review also assesses physical and cyber security systems in a more holistic approach to counter blended attacks.

Furthermore, CNSC is exploring the possibility of sharing relevant nuclear-sensitive information from the national DBT with SMR designers. Access to this information can help designers consider credible and future threats in their design and enable the integration of SeBD effectively. However, challenges exist in sharing classified information with foreign vendors and designers due to security clearance requirements and potential risks of unauthorized dissemination.

Overall, the CNSC's approach emphasizes a risk-informed and flexible regulatory framework that considers security by design principles to ensure the effective protection of nuclear facilities while accommodating the unique characteristics and risk profiles of SMRs. By engaging in dialogue with industry stakeholders and incorporating SeBD into the early stages of design, Canada aims to maintain a secure and robust nuclear industry in the face of evolving security challenges. [19]

4 Target identification

Target characterization is a crucial step in the development of an effective PPS for any nuclear facility, including SMRs. It involves the identification and understanding of specific targets that require protection from potential adversary attacks or security breaches. The characteristics of these targets are assessed to determine the appropriate security measures needed to safeguard them.

In an NPP, potential targets for security protection can be categorized into two main types: materials and the facility itself. Each type of target requires specific security measures to prevent unauthorized access, theft, or sabotage.

For SMRs, target characterization may differ from traditional NPPs due to various factors:

- Decreased Complexity of Safety Systems: SMRs are designed to have simplified and modular safety systems, which may result in a reduced number of targets associated with safety systems. These changes in safety system design should be taken into account while characterizing targets for protection.

- Unique Theft Threats: SMRs may have different theft threats compared to traditional NPPs. For example, due to the high burnup designed for some SMRs, the spent fuel from these reactors could contain Category-I quantities of nuclear material. This spent SMR fuel could be considered a theft target, and as a result, sites may need to implement a higher level of protection for such fuel.

- Self-Protecting Spent Fuel: In contrast to spent fuel from NPPs, which is generally considered self-protecting and may have lower protection levels, spent fuel from SMRs may need to be treated differently, especially if it contains significant quantities of nuclear material.

4.1 SMR fuels

The types of SMR fuels are varied to serve each kind of reactor design and operational requirements. Different SMR concepts utilize specific fuel types tailored to their unique characteristics and intended performance. From the aforementioned types, the less usual kinds of fuels include TRISO and metal fuel used in HTGRs (and some molten salt concepts) and SFRs, respectively.

4.1.1 TRISO

TRISO (Tri-structural Isotropic) fuel is a type of nuclear fuel known for its exceptional safety features, making it an attractive choice for advanced nuclear reactor designs. These safety features are achieved through the unique structure and materials used in TRISO fuel. Here's a detailed explanation of TRISO fuel and its safety features:

- TRISO Particle Structure: TRISO fuel consists of a small spherical kernel of fissile material, such as uranium or plutonium, surrounded by three layers of coatings, forming a robust "pebble" or "ball" of fuel. Each layer serves a specific safety function.

  First Layer: The innermost layer is the fuel kernel itself, containing the fissile material. The kernel is typically made of uranium dioxide (UO2) or mixed oxides, encapsulating the radioactive material.

  Second Layer: The first coating, known as the buffer layer, is made of materials like pyrolytic carbon. It acts as a buffer between the fuel kernel and the subsequent layers, providing thermal stability and preventing chemical interactions.

  Third Layer: The second coating is the innermost protective layer, called the inner pyrolytic carbon (IPyC) layer. It shields the fuel kernel from fission products and other impurities, preventing the release of radioactive materials even under extreme conditions.

  Fourth Layer: Following the IPyC layer is the silicon carbide layer. This layer is designed to retain fission products and act as a barrier against the release of radioactive materials during reactor operation.

  Fifth Layer: The outermost layer is composed of Pyrolytic Carbon, referred to as the OPyC layer. It provides a final protective barrier for the TRISO fuel particle.

Safety Features:

- High Temperature Tolerance: TRISO fuel can withstand high temperatures, making it highly resistant to fuel failures or cladding breaches. Even under extreme conditions, the SiC layer retains its integrity and prevents the release of radioactive materials.

- Inherent Radiation Containment: The multiple layers of coatings in TRISO fuel act as successive containment barriers for radioactive products. This inherent containment ensures that fission products are trapped within the fuel particles, reducing the risk of radioactive release into the coolant or environment.

- Negative Temperature Coefficient: TRISO fuel exhibits a negative temperature coefficient of reactivity, meaning that as the fuel temperature increases, the reactivity decreases. This natural feedback mechanism helps stabilize reactor operation and reduces the risk of temperature-induced power excursions.

- Passive Safety: The robust and self-contained nature of TRISO fuel provides passive safety features. The fuel particles can withstand high temperatures and pressure without external cooling systems, making them resilient to accidents and reactor transients.

- Reduced Risk of Core Meltdown: Due to the multiple layers of containment, TRISO fuel has a low probability of core meltdown. Even if the reactor experiences a loss of coolant or cooling system failure, the fuel particles remain intact, preventing fuel melting and significant radiological releases.

[6] [21]

4.1.2 Metal fuel

The 4S reactor utilizes a U-10Zr metallic fuel design, which has undergone extensive evaluation and pre-licensing activities by Toshiba Corporation. The metallic fuel is a key component in the reactor's operation and safety. It is based on uranium and zirconium, with extended irradiation data gathered from previous reactors such as EBR-II and FFTF, along with a database of out-pile experiments.

The metallic fuel exhibits several safety features that make it well-suited for the 4S reactor's long-life operation. One notable characteristic is its strong negative temperature coefficient, which means that as the fuel temperature increases, the neutron energy also increases, resulting in a reduction of fission reactions and power output. This inherent safety feature allows the core to stabilize even under adverse conditions, preventing catastrophic failures or radiation releases.

The design of the 4S metallic fuel includes considerations for fuel swelling and fission gas release, fuel constituent migration, and fuel-cladding chemical interactions. Additionally, the reactor employs automatically deployed reactivity controls and inlet and outlet shutoff valves to ensure continued safety in case of helium pressure or flow loss. The fuel pins in the 4S reactor are wider and longer compared to EBR-II and FFTF fuel pins, allowing for enhanced performance and stability.

The use of the LIFE-METAL fuel performance code has provided further validation and confidence in the 4S fuel design. The analysis using this code confirms that the 4S fuel meets conservative pre-specified fuel integrity design criteria, even under conditions more severe than expected in the reactor. This quantitative evaluation assures that the 4S metallic fuel is expected to perform adequately and safely during its intended 30-year lifetime.

[6] [22]

The enrichment of SMR fuels varies depending on the specific reactor type and design. In general, SMR fuels tend to have higher enrichments compared to traditional PWRs to achieve higher power densities and longer refueling cycles.

1. LWRs: Many SMRs, such as NuScale Power's SMR, utilize light water reactor technology, similar to conventional PWRs. The enrichment of uranium in these reactors typically ranges from 3% to 5% U-235.

2. HTGRs: HTGRs, like the pebble bed design used in the HTR-PM in China, often employ TRISO fuel particles. The enrichment of uranium in TRISO fuel for HTGRs can be higher, typically ranging from 8% to 20% U-235.

3. SFRs: Some SMRs, like the 4S reactor, are sodium-cooled fast reactors. The enrichment of uranium in SFRs can vary, but it is generally higher than LWRs, ranging from 15% to 20% U-235.

4. MSRs: MSRs, such as the design proposed by TerraPower, use thorium or enriched uranium dissolved in a molten fluoride salt. The enrichment level in MSRs can be tailored to the specific design requirements, with enriched uranium ranging from 5% to 20% U-235 or higher.

It is important to note that the enrichment levels in SMRs are subject to specific safety, operational, and economic considerations. The higher enrichments in certain SMR designs allow for improved reactor performance, increased fuel utilization, and longer refueling intervals. However, with higher enrichments, additional safety and security measures must be implemented to ensure the safe and secure operation of these advanced reactor designs.

Some of the afforementioned concepts were put into categories dependent on the used nuclear material in accordance with Fig. 4.1. Concepts such as BWRX-300, NuScale, Rolls-Royce, HTR-PM and HTTR fit the third category, while concepts such as HTR-10, 4S and EW have parameters suited for II. category.

Material	Form	Category I	Category II	Category III[c]
1. Plutonium [a]	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235 (^{235}U)	Unirradiated[b]			
	– Uranium enriched to 20% ^{235}U or more	5 kg or more	Less than 5 kg but more than 1 kg	1 kg or less but more than 15 g
	– Uranium enriched to 10% ^{235}U but less than 20% ^{235}U		10 kg or more	Less than 10kg but more than 1 kg
	– Uranium enriched above natural, but less than 10% ^{235}U			10 kg or more
3. Uranium-233 (^{233}U)	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated fuel (The categorization of irradiated fuel in the table is based on international *transport* considerations. The State may assign a different category for domestic use, storage and *transport* taking all relevant factors into account.)			Depleted or natural uranium, thorium or low enriched fuel (less than 10% fissile content)[d, e]	

[a] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

[b] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h. (100 rad/h) at 1 m unshielded.

[c] Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.

[d] Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

[e] Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/h (100 rad/h) at one metre unshielded.

Fig. 4.1: Categorisation of nuclear materials. Table taken and edited from NNS 13. [23]

4.2 Vital Area Identification

Vital Area Identification (VAI) is the process of identifying the areas of a nuclear facility that must be protected to prevent malicious acts that could directly or indirectly endanger the public health and safety by exposure to radiation.

[24]

If the aforementioned areas are adequately protected, high radiological consequences (HRC) or unacceptable radiological consequence (URC) will be prevented. The threshhold between the URC and HRC is determined by each state, not universal.

[25]

PPS uses graded approach. There are different kinds of URC or HRC thresholds. They can be quantitative, such as safety criteria or qualitative, like relative risk. Then there are release-based or dose-based criteria, including maximum allowable release or dose, which usually use existing safety limits. The design limit threshold specifies an unacceptable plant state, such as core damage, and is generally more conservative.

[26]

The process to identify vital areas goes as followes:

1. Identify Radioactive Material Inventories: The first step is to identify and compile a comprehensive list of all radioactive materials present within the facility. These materials may include nuclear fuel, radioactive waste, and other nuclear materials that could pose radiological hazards if tampered with.

2. Assess Direct Dispersal Possibility: For each identified radioactive material inventory, an assessment is made to determine whether direct dispersal of these materials is possible in the event of sabotage. This step involves evaluating potential scenarios where radioactive material could be released or dispersed.

3. Identify Initiating Events: Initiating events are events or conditions that, when combined with malicious acts, could lead to sabotage of the identified radioactive material inventories. These events could be natural disasters, equipment failures, or intentional malicious actions.

4. Develop the Sabotage Logic Model (SLM): The Sabotage Logic Model is a logical representation of various combinations of events that could lead to

indirect sabotage of the identified radioactive material inventories. The SLM helps analyze the potential pathways for sabotage and their consequences.

5. Eliminate Events Beyond DBT: The DBT represents the specific threat scenarios that a nuclear facility must be protected against. Events in the Sabotage Logic Model that exceed the specified DBT are eliminated from consideration.

6. Identify Areas Corresponding to Events in SLM: Specific areas within the facility that are associated with the events in the Sabotage Logic Model are identified. These areas are potential targets for sabotage and require protection.

7. Replace Events with Associated Areas: Events from the Sabotage Logic Model, such as direct dispersals, initiating events, and mitigation system disablement events, are replaced with their associated areas within the facility. This step helps to focus on the physical locations that need protection.

8. Identify Target Sets: Target sets are combinations of areas that an adversary must access to cause radiological sabotage. These target sets are essential for understanding the critical areas requiring enhanced security measures.

9. Select Vital Areas for Protection: Based on the identified target sets and associated areas, the vital areas that must be protected to prevent radiological sabotage are prioritized. These vital areas represent the key focus of the security measures and safeguards implemented at the facility.

[25] [24]

SLM can be a statement, an algebraic expression or a graphical representation, such as a fault tree or an event tree. A logic model is solved by application of Boolean algebra. An example of such logic model is shown in NSS 16.

Take a fictional facility with following characteristics:

1. There are two initiating events (IEs) identified for this facility, IE1 and IE2, that if unmitigated will result in releases that exceed the HRC limits established by the competent authority.

2. Safety system S1 is designed to mitigate IE1 and system S2 is designed to mitigate IE2.

3. System S1 has two trains of equipment, T1 and T2. If either of these trains functions properly, S1 can successfully mitigate IE1 (that is, both trains must fail for S1 to fail).

4. System S2 has three trains, T3, T4, and T5. Either T3 or both T4 and T5 must function in order for S2 to successfully mitigate IE2 (that is, S2 will fail to mitigate IE2 if either T3 and T4 fail or T3 and T5 fail).

5. The trains in the systems have components (designated by C below) that must operate for the trains to function.

   - T1 fails if either of two components (C1 or C2) fails.
   - T2 fails if either C3 or C4 fails.
   - T3 fails if either C5 or C6 fails.
   - T4 fails if either C7 or C8 fails.
   - T5 fails if either C9 or C10 fails.

6. In order to cause the IEs and disable the various components a saboteur would have to gain access to different plant locations, designated with L labels below.

Event	Location
Disable C1	L1
Disable C2	L2
Disable C3	L2
Disable C4	L2
Disable C5	L3
Disable C6	L3
Disable C7	L5
Disable C8	L6
Disable C9	L6
Disable C10	L6
Cause IE1	L8
Cause IE2	L9

These statements constitute a form of a sabotage logic model of the facility. An analysis of the statements leads to combinations of locations that a saboteur

Tab. 4.2: Boolean algebra

Logic symbols		
Symbol	Operation	Definition
$\vee$	OR	Either of two events occurs.
$\wedge$	AND	Both of two events occur.
$\neg$	NOT	Negation.
Boolean algebra rules		
$A \vee A = A$	$A \vee A \wedge B = A$	$\neg (A \vee B) = \neg A \wedge \neg B$
$A \wedge A = A$	$A \wedge (B \vee C) = A \wedge B \vee A \wedge C$	$\neg (A \wedge B) = \neg A \vee \neg B$

(a) OR (b) AND

Fig. 4.2: Logic gates

must enter in order to cause the IEs and component failures that would lead to HRCs. In a simple facility, the analysis can be done by simply inspecting the statements. For more complex facilites a better approach is to use Boolean logic. Tab. 4.2 summarises relevant logic symbols.

For diagrams there are also logic gates, following images dislplayed on Fig. 4.2 show AND gate and OR gate.

Using aforementioned symbols and logic operators, Boolean logic can be applied to the fictional facility problem, as follows:

$$HRC = IE1 \land S1 \lor IE2 \land S2 \tag{4.1}$$
$$S1 = T1 \land T2 \tag{4.2}$$
$$S2 = T3 \land T4 \lor T3 \land T5 \tag{4.3}$$
$$T1 = C1 \lor C2 \tag{4.4}$$
$$T2 = C3 \lor C4 \tag{4.5}$$
$$T3 = C5 \lor C6 \tag{4.6}$$
$$T4 = C7 \lor C8 \tag{4.7}$$
$$T5 = C9 \lor C10 \tag{4.8}$$

In the equations 4.1-4.8 S1 means safety system 1 was disabled and so on. If events are replaced with locations where they can be disabled, the problem leads to the following set of equations:

$$T1 = L1 \lor L2 \tag{4.9}$$
$$T2 = L2 \lor L2 = L2 \tag{4.10}$$
$$T3 = L3 \lor L3 = L3 \tag{4.11}$$
$$T4 = L5 \lor L6 \tag{4.12}$$
$$T5 = L6 \lor L6 = L6 \tag{4.13}$$
$$S1 = (L1 \lor L2) \land L2 = L2 \tag{4.14}$$
$$S2 = L3 \land (L5 \lor L6) \lor L3 \land L6 = L3 \land L5 \lor L3 \land L6 \tag{4.15}$$
$$HRC = L8 \land L2 \lor L9 \land (L3 \land L5 \lor L3 \land L6) \tag{4.16}$$

Adjusting the equation 4.16 in accordance with allowed Boolean logic operations leads to the final equation $HRC = (L8 \land L2) \lor (L9 \land L3 \land L5) \lor (L9 \land L3 \land L6)$ which shows that there are three combinations of locations where a saboteur can cause HRCs. Each of these combinations is called a set of the sabotage location equation. VAI's goal is to discover a minimum set of such areas to be defended against sabotage and thus preventing all scenarios leading to HRCs.

Diagram on Fig. 4.3 shows the fault three with the solution.

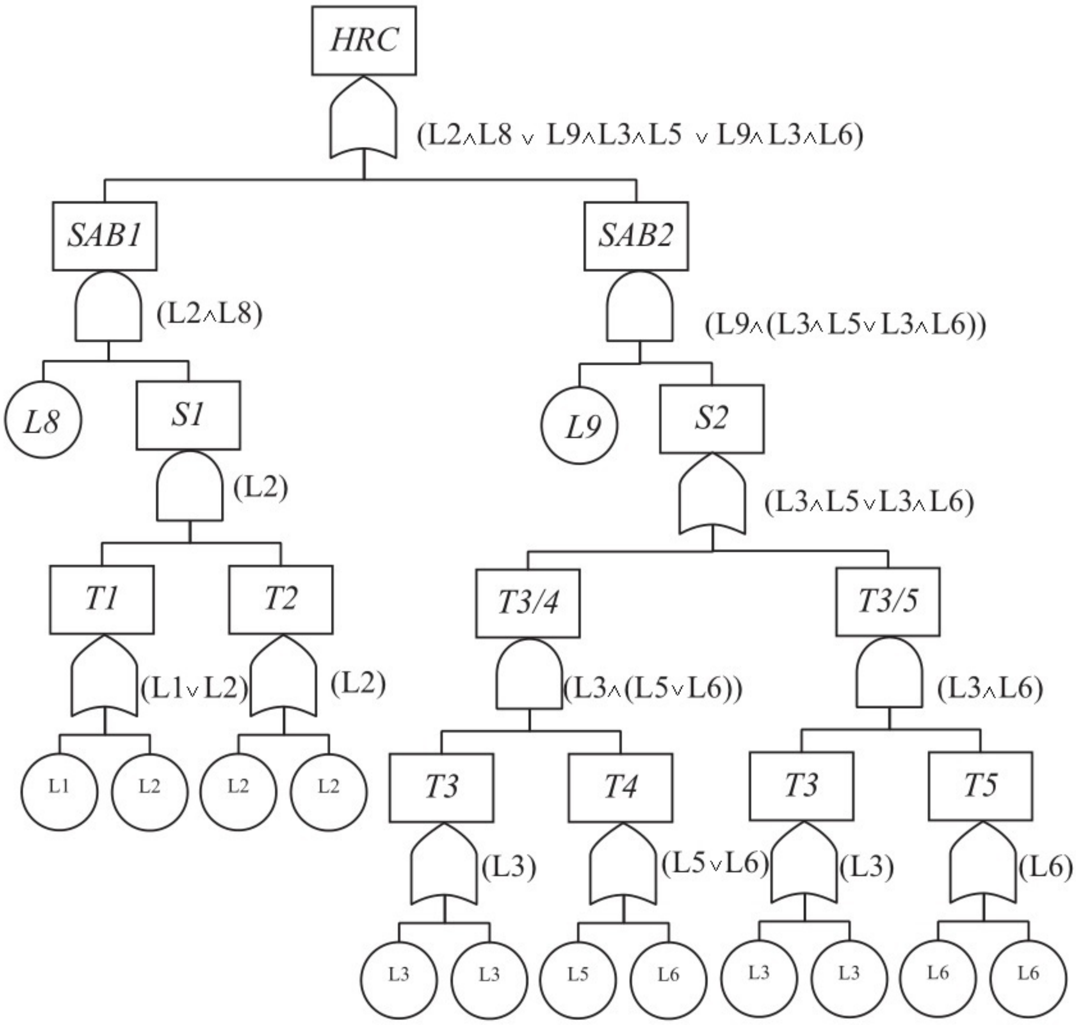

Fig. 4.3: Solved fault tree for the fictional facility. Picture taken and adjusted from [27]

5 Design Basis Threat

Threat characterization is a crucial aspect of designing a PPS for nuclear facilities, including SMRs. Modern nuclear facilities face complex threats from a diverse range of actors. The threat landscape is continuously evolving, and nuclear facilities must be prepared to defend against a wide range of adversaries and potential threats.

IAEA Nuclear Security Series (NSS) defines the following terms:

- Threat - A person or group of persons with motivation, intention and capability to commit a malicious act [23]

- Threat Assessment - An evaluation of the threats – based on available intelligence, law enforcement, & open source information – that describes the motivations, intentions, and capabilities of these threats [23]

- Design Basis Threat - Attributes and characteristics of

  - Potential insider and/or external adversaries deemed to have the intent and capabilities to commit a malicious act . . . , against which a PPS is designed and evaluated [28]

  - Threats for which the State organizations and operators have protection responsibilities and accountability [28]

For SMRs, the threat environment may differ from traditional NPPs due to their potential deployment in various settings, including urban or rural environments. This variability in deployment locations can impact the types of adversaries considered in the DBT or Regulatory Threat Statement (RTS). Adversaries could range from terrorist groups to environmental activists to common criminals, and the potential threats they pose need to be thoroughly assessed.

The threat characterization process is typically conducted by the State, which defines the DBT or RTS that will be shared with the licensees. The State may take different approaches to design the protection system:

- Providing the Threat and Guidance: The competent authority shares the DBT or threat with the licensee and offers guidance on the effectiveness of the PPS to protect against it.

- Establishing Performance Requirements: The regulator formulates performance requirements based on the DBT or threat statement and then provides these requirements to the licensee.

- Defining Prescriptive Requirements: The regulator outlines prescriptive requirements based on the DBT or threat statement and provides them to the licensee.

[25]

The motivation for using DBT stems from the security design problem, where an event of a high consequence can have low probability, therefore it can be complicated to establish the right amount of security. Security design needs a stable, detailed defensible design criteria to support efficient allocation of resources, delegation of physical protection responsibilities, performance baseline for evaluations, more objective and less arbitrary design. DBT establishes threat-based criteria for design, evaluation, operator accountability and national risk strategy.

DBT attributes need to be reasonable, based on best available threat information and considering state-specific policies. They also need to be defendable, providing technical basis for defining performance requirements, cost-effective and need to help provide assurance that level of protection is adequate.

Security designs for the following should be influenced by DBT:

- Protection of PPS computers and networks
- Vehicle barrier design and location
- Intrusion detection
- Personnel access control
- Vital area delay capabilities
- Airborne threat protection measures
- Material transport system protection measures

Credible scenarios based on the DBT are first defined, then used to test the PPS to ensure it meets the objective.

Potential threat can involve outsiders, insiders or a combination of both. Outsider or insider can be defined as any individual or group of individuals deemed to have the intent and/or capabilities to commit a malicious act. [28]

According to NSS 13 [23] an insider is one or more individuals with authoriyed access to nuclear facilities or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so.

The involvement of an insider can be either active or passive. The active insider can be violent or nonviolent (unwilling to use force against personnel; aborts if detected or confronted). The active insider may act alone or in collusion with an outsider. The passive insider restricts actions to providing information and usually acts in collusion with an outsider. [28]

For threat assessment a Probability-Impact table (P-I) can be used to estimate a relative importance of risk. Matrix diagram of risk can be used to separate high-impact risk from low-impact risk. This risk assessment method is here used to categorise potential threats, which will be divided into four categories: kittens, puppies, alligators and tigers. Kittens and puppies pose a relatively small threat as they cannot do a lot of damage, while tigers and alligators can cause a lot of damage.

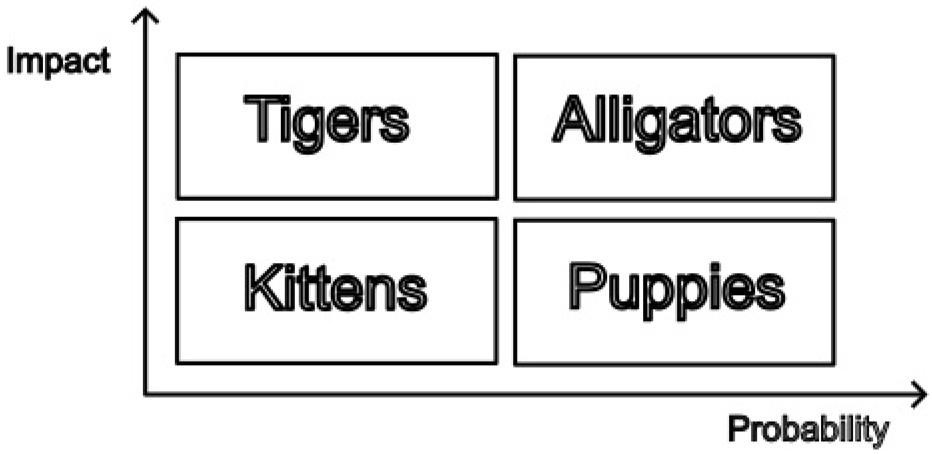

Fig. 5.1: Probability-Impact chart

An example of kittens might be a local environmentalist group with very small budget and shallow understanding of the problematic. Puppies could be a group of protesters, specifically targeting nuclear power stations, they are loud in their disagreements but they still pose a relatively low threat. Tigers could be experienced thieves, possessing knowledge of how to effectively overcome a variety of security measures. Though a nuclear power station could be too risky target for them, if they choose to strike, they could potentially cause some damage. And alligators can be a well-organised terrorist group working with a large budget that has a man on the inside, ready to sabotage the plant.

Once the threat assessment is done, there can be a DBT development, following the phases displayed on Fig. 5.2.

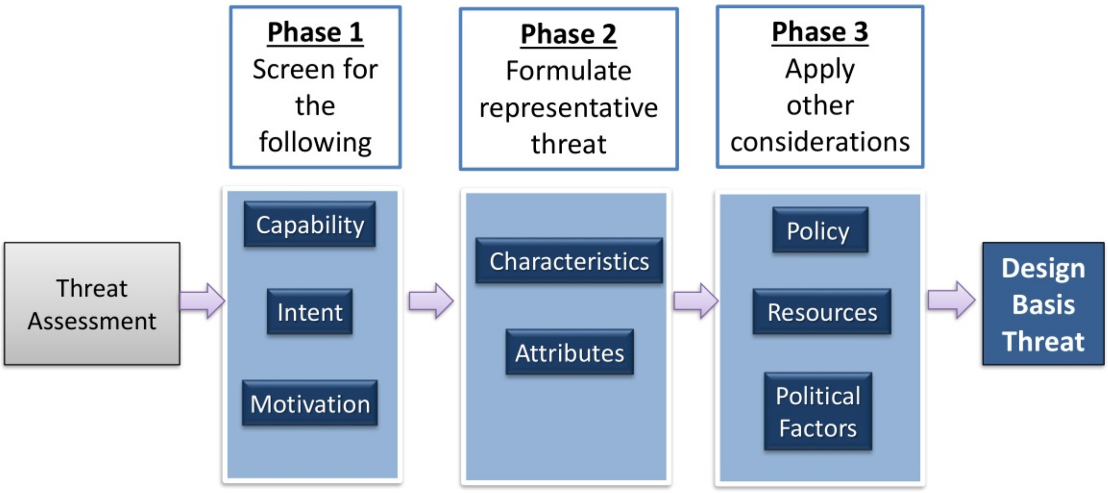

Fig. 5.2: DBT development process overview. Picture taken from [28]

It is important to note that threat characterization is an ongoing process. As new information about potential threats becomes available or new capabilities are realized, the threat assessment should be revisited to ensure that the PPS remains effective against emerging threats.

6 Design and evaluation of physical protection systems

The NSS 40-T [29] provides the following definition of a PPS:

A PPS is an integrated system of detection, delay and response measures, and should be effective against both unauthorized removal and sabotage. It should comprise people, procedures and equipment to provide defence in depth, with a graded approach, to address the range of threats identified in the applicable threat statement and to protect against both unauthorized removal and sabotage.

The key functions of a PPS include deterrence, detection, delay and response.

Deterrence aims to prevent or discourage adversaries from taking certain actions by convincing them that the costs or risks outweigh the potential benefits. The idea behind deterrence is that if a potential aggressor believes that an undesirable outcome or punishment will follow their actions, they are less likely to engage in those actions.

There are two primary types of deterrence. Deterrence by Threat of Retaliation involves convincing potential adversaries that if they take a particular action, they will face severe and unacceptable consequences. This can involve military retaliation, economic sanctions, or other punitive measures. The goal is to create a credible threat that dissuades the adversary from taking the undesired action. Deterrence by Denial focuses on preventing an adversary from achieving its objectives rather than punishing them after the fact. This can involve building defenses, creating a robust security infrastructure, or implementing policies that make it difficult for an adversary to succeed in their actions. The idea is to deter by making the potential aggressor believe that their efforts will be futile.

Detection is the process of identifying and uncovering adversary actions or potential threats. The goal of detection is to identify security incidents promptly, allowing for a timely response to mitigate potential damage.

Delay refers to the measures and mechanisms put in place to slow down or impede an adversary's progress during an attempted security breach. The objective is to create obstacles that increase the time it takes for an adversary to reach a critical or protected area, providing security personnel with more time. Common examples of delay components in PPS include physical barriers such as fences and walls, access control points, perimeter intrusion detection systems, surveillance cameras, lighting systems, vehicle barriers, locks and access controls.

Response refers to the actions taken by security personnel or automated systems when a security threat or breach is detected. It aims to minimize the impact of a security incident, protect assets, and ensure the safety of people within a facility.

Path analysis serves to compare adversary timeline with the timeline of the response force, as is shown in Fig. 6.1. It is crucial that the response time is sufficient to apprehend the adversary when designing a PPS. One of aforementioned key features of a power plant with an SMR is overall smaller size of the plant than a regular one, which begs the question of the complexity of security measures necessary to compensate for the reduced adversary task time by the small scale.

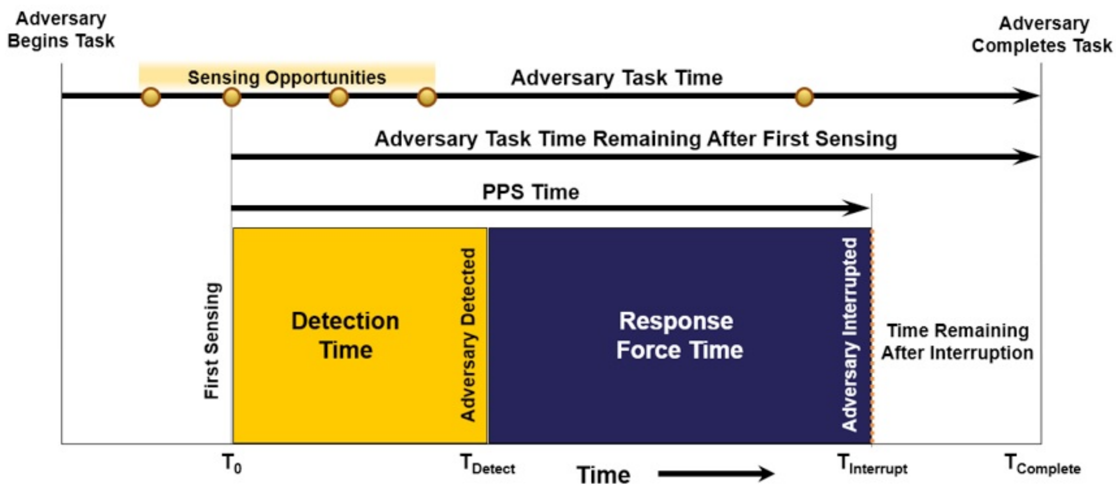

Fig. 6.1: Comparison of physical protection timelines [25]

The Cumulative Probability of Detection describes the likelihood of detecting a threat over multiple stages or layers of a security system. It represents the overall effectiveness of a security system in detecting and preventing adversarial actions as they progress through different phases of an attack. Security systems consist of multiple layers or stages, each contributing to the overall detection capability. These layers could include surveillance, access controls, alarm systems, response forces, etc. At each stage of the security process, there is a probability of detecting and responding to an adversarial action. This could be influenced by factors such as the quality of surveillance equipment, the effectiveness of access controls, or the response time of security personnel. Cumulative probability of detection is a measure that considers the combined effect of these individual probabilities across all stages. It takes into account the likelihood of an adversary being detected at each layer and calculates the overall probability of successful detection before a threat reaches its intended target.

Critical Detection Point (CDP) is a concept used to identify the specific stage or moment in an adversarial sequence where the detection of a threat becomes crucial for preventing potential harm or damage. It represents a strategic point in the security process where timely and accurate detection is essential to disrupt or mitigate an unfolding threat.

For evaluating effectiveness of a PPS, there are various different models, one of such is a quantitative analytic tool EASI, which stands for Estimate of Adversary Sequence Interruption. EASI is used to evaluate performance of a PPS along one path, computing probability of interruption from an analysis of the interaction of detection, delay, response and communication values. Other more complex analysis tools are based on EASI.

As an input EASI uses Probability of detection P_D for each sensor in adversary's path, where P_D is a product of P_S, P_T and P_A. P_S represents the probability that the detector will sense the behaviour that is abnormal or unauthorized, P_T is the probability than an alarm indication will be transmitted and P_A is the probability of accurate assessment. P_C represents the communication of an alarm to the response force. The output is then the P_I, which is the probability of interruption. Minimal acceptable value is 85 %. [30] If the path only consists of one sensor, the resulting probability would be a product of P_D and P_C. P_I represents the likelihood that security measures will successfully interrupt or thwart an adversary's attempt at theft, sabotage, or any other malicious activity.

[31]

The Very Simplified Estimate of Adversary Sequence Interruption (VEASI) model is a user-friendly computational tool designed for estimating the P_I in the context of physical protection systems. Primarily focusing on a single, specific path, VEASI employs detection, delay, and response time values as inputs to calculate PI. Despite its simplicity, VEASI offers the capability to conduct sensitivity analyses and explore interactions and time trade-offs within the physical protection system along the specified path. The required inputs encompass detection probabilities, mean times for delay elements, the temporal relationship between detection and delay, and the Response Force Time from security response plans. The model outputs the probability of intercepting an adversary before any theft or sabotage occurs. VEASI allows users to dynamically alter input parameters to observe their impact on the output.

[32]

7 Hypothetical SMR facility

To simply demonstrate the vast variety of options when it comes to SMRs, two hypothetical SMR facilities will be described, one with a BWR reactor, where overall low security necessity is expected (HYPO-BWR) and another facility with a fast reactor, where the fuel categorisation may present some need for additional security measures (HYPO-fast).

Facility Name:	HYPO-BWR
SMR Type:	BWR
Power Output:	200 MW
Emergency Planning Zone:	1 km from the boundary of the site
Plant Configuration:	The majority of the facility is contained within one building with a footprint of 8800 square meters.
Proximity to City:	Nearest city is located 500 meters from the boundary of the site. It is called Nuclear City with population 150 000 people. The plant supplies it with electricity.
Operational Staff:	The facility is operated by a staff of 70 people during normal operation.
Most likely target:	Fuel in the reactor hall, III. category, enriched uranium, low enrichment
On-site response team:	None. Instead the response is conducted by Nuclear City Police Department.
Response time:	300 s

Security Implications:

- Critical Infrastructure: Given its role in supplying electricity to a nearby city, HYPO-BWR is classified as critical infrastructure
- City Proximity: The proximity of the city introduces challenges in balancing accessibility for electricity supply and ensuring the safety of the population as well as sufficient security.
- Integrated Security Measures: Security measures should be integrated into the design and operation of HYPO-BWR, encompassing physical protection, cybersecurity, and personnel security.

- Target: Though the fuel may not seem like a likely target at first glance, the reason for it being likely targeted is further explored in the DBT section.

Fig. 7.1 shows the layout of the protected area of the facility.

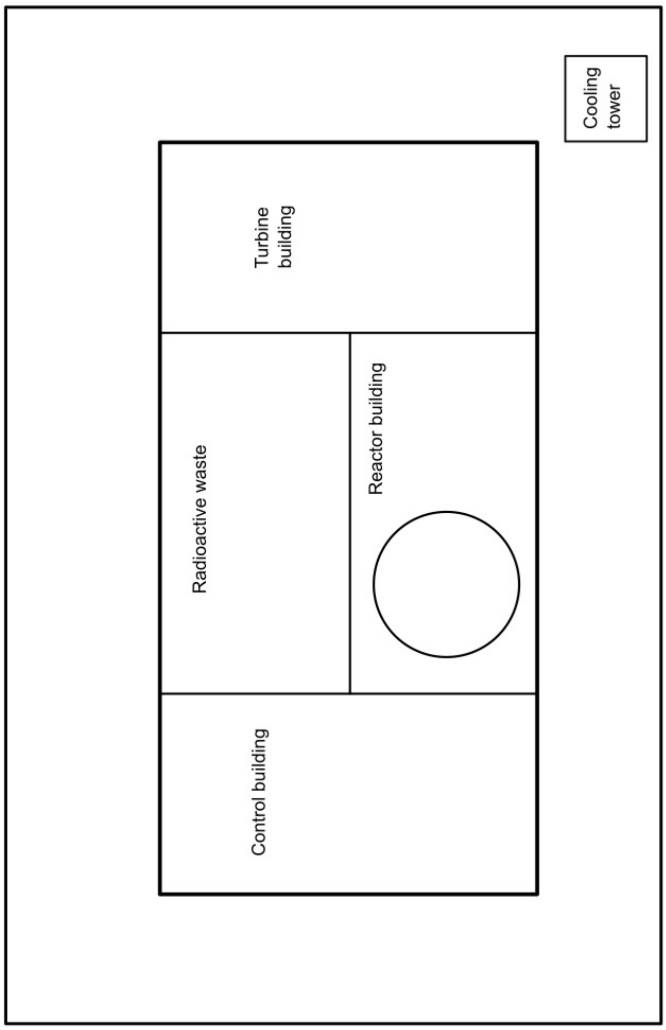

Fig. 7.1: Layout of the protected area of HYPO-BWR.

Facility name:	HYPO-FAST
Type:	Fast reactor with liquid metal cooling (sodium)
Enrichment:	Less than twenty percent
Size:	Facility dimensions are 400 by 400 meters

Capacity:	10 MWe
Operational Staff:	10 people during normal operation
Emergency Planning Zone:	3 km from the site border
Most likely target:	Sabotage of the primary pumps
On-site response team:	Yes. Four people on site at all times.
Response time:	120 s

- Location and Surroundings: The nearest establishment is a mining site. EPZ distance 3 km provides a buffer zone, however, apart from the mining site there is only wilderness around. Nearest town is 25 km far.

- Critical Infrastructure: The facility serves as an electricity supplier for a mining site.

- Security Considerations: Liquid metal cooling requires specialized safety measures due to the use of sodium. Enrichment Level under twenty percent reduces certain proliferation risks, however, the amount of fuel necessary puts the fuel into II. category according to Fig. 4.1. The lack of nearby residential areas could simplify security zoning, however could also affect response times.

- Personnel: A smaller staff (10 people) compared to larger facilities.

- Emergency Planning: Considerations for power supply continuity to the mining site.

- Emergency Response: Coordination with the mining site for integrated emergency plans.

- Public Perception: Clear communication strategies due to the isolated nature of the facility.

Fig. 7.2 shows the layout of the protected area of the HYPO-fast facility.

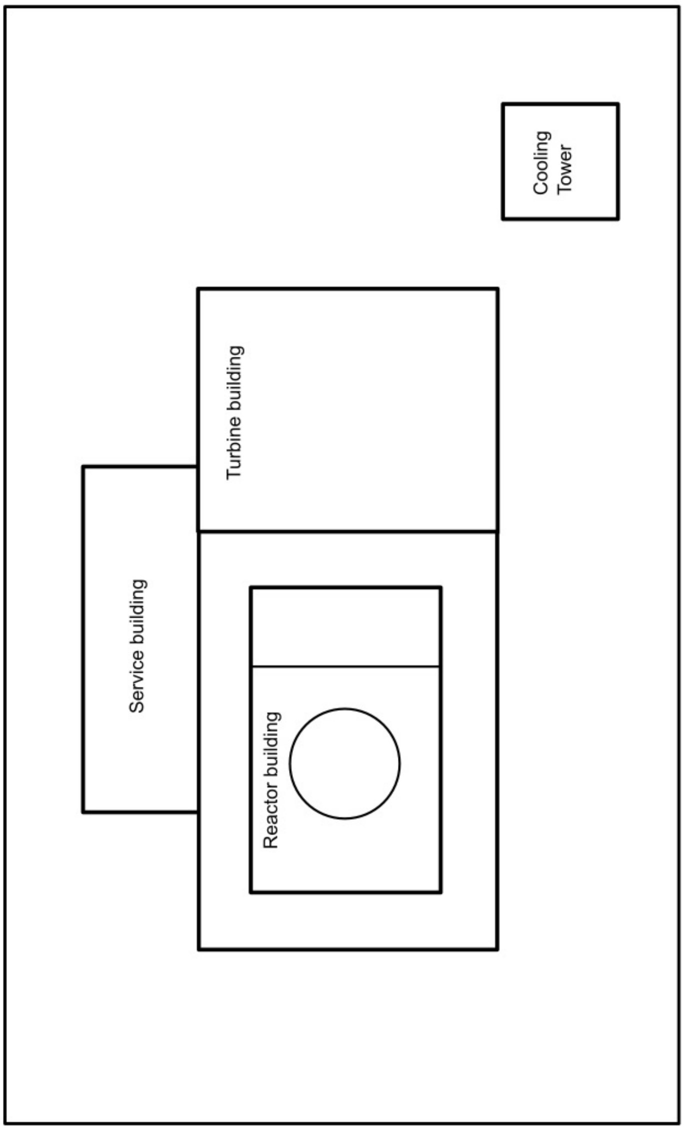

Fig. 7.2: Layout of the protected area of HYPO-fast.

7.1 Design basis threat

To form a DBT for the HYPO facilities, as is displayed in Fig. 5.2, there needs to be screening for capability, motivation an intent, as phase one of DBT analysis.

HYPO-BWR is very close to a large city (population 150 000 people), thus Kittens and Puppies are to be expected as potential adversaries, such as drunken disturbance of the perimeter, or a random attempt at breaking and entering followed by theft. Though the majority of 65 % citizens of Nuclear City is proudly pro-nuclear, the city is also the base of "Water is for Soup" activist organisation, vehemently protesting any kinds of BWRs. Their concerns are that BWRs are not safe and as an example they name the Fukushima Daiichi accident. The Nuclear Country, in which Nuclear City is located, has very low tectonic activity and is an inland country. However, the Water is for Soup organisation stays adamant despite the extensive pro-nuclear PR campaign by the operator of the HYPO-BWR. Water is for Soup focuses mostly on recruitment, protests and collecting signatures for open letters to select political parties, however, their numbers have remained steady for over a decade and they could potentially attempt a break-in and sabotage of HYPO-BWR.

HYPO-fast on the other hand is not very likely targeted by Kittens at all, due to the remote location, at the far end of Nuclear Country. The main concern may be a Tiger attack, aimed at compromising electricity supply to the mine. As such, Tigers may attempt a break-in and sabotage the vital area.

Phase two involves formulating a representative threat, including characteristics and attributes. For HYPO-BWR that can be a Water is for Soup break-in, with an assistance of an insider, who is one of them, working covertly on site for the last five years as one of the cleaning staff.

For HYPO-fast, two saboteurs break into the plant in an attempt to force shutdown and stop production.

Phase three looks at other factors: policy, resources and political factors. Nuclear Country is proud for the public support and acceptance of nuclear power. Most major political parties are onboard and as for international politics, due to the export of electricity from Nuclear Country it tends to not be influenced by potential international disagreements about nuclear energy.

Final stage is forming a DBT. For HYPO-BWR that would be an attempted theft by a group of Water is for Soup protesters, trying to get into the reactor building and stealing some fresh fuel in an attempt to discredit the power station in the public eye and forcing a permanent shutdown. A group of four adversaries is considered. They do not have access to any explosives and are equipped with lockpicks, crowbars, pipe wrenches and other hand tools. For HYPO-fast a pair of determined outsiders attempt to break the primary pump. They have access to explosives, which lowers the time delay at doors.

7.2 System of physical protection

In both HYPO facilities, there are layers that an adversary has to surpass in order to reach its target or the vital area. Following table Tab. 7.3 surmises the areas as well as the barriers between them. An adversary needs to get pass these layers in order to conduct a sabotage or theft.

Tab. 7.3: SECURITY LAYERS FOR HYPO-BWR AND HYPO-FAST

HYPO-BWR	**HYPO-Fast**
OFFSITE	OFFSITE
Fence, Gate	Fence, Gate
LIMITED AREA	LIMITED AREA
Surface, window, personal gate, vehicle gate	Surface, window, personal gate, vehicle gate
PROTECTED AREA	PROTECTED AREA 1 - Main Building
Vessel surface, vessel cover	Surface, personal gate, manipulation gate
VITAL AREA / TARGET	PROTECTED AREA 2 - Reactor room
	Surface, Lid
	VITAL AREA / TARGET

The suggested security measures for HYPO-BWR are following:

1. Outer fence: A fence 2.5 m tall, topped with barbed wire and also equipped with shaker sensor system, adding to the probability of an early detection. Expected delay 20 s. Low probability of detection.

2. Gate: An access point through the outer fence, higher probability of detection. Expected delay 15 s.

3. Wall: 30 cm thick reinforced concrete walls. No need for blast resistance due to the low probability of that type of attack on this specific facility. It would be necessary for an adversary to be equipped with a concrete saw or a more powerful tool to breach it, making it a noisy affair, thus heightening the probability of detection.

4. Window: Transparent plastic window with a security bar. Expected hand-tool penetration 120 s.

5. Personal gate: High-security, attack-resistant door with strengthened frames and hinges, equipped with entry control system. Expected penetration 600 s, probability of detection 0.6.

6. Vehicle gate: A pair of interlocked gates where one needs to be closed for the other to open, ensuring high probability of detection.

7. Vessel surface: Metal-concrete fuel vessel, very hard to penetrate, estimated time 1200 s.

8. Vessel cover: The cover of the vessel can be opened using hand tools, however estimated time is at least 600 seconds without use of explosives.

Assessing the scenario of the fuel theft by a group of Kittens, without the insider help can be seen in Fig. 7.3. Multi-Path VEASI software was used for this assessment. [33] The time estimates for barrier penetration were based on information found in [34] and examples from [31]. The adversary data are filled out in accordance with Tab. 7.3 and the times and probabilities according to the suggested security measures above. The response time and strategy is entered. Numbers of response people and adversaries must be filled out, which are then used to obtain the P(N) value, giving the probability of the response forces overpowering the adversaries (probability of neutralization). Then the analysis is conducted and the product of P_I and P(N) gives the P(E) value, which is the probability of system effectiveness.

Fig. 7.4 shows that even if one of the adversaries is an insider, helping with significantly shortening the delay time and the lowering probability of detection at PERSONAL GATE, CDP remains at the same point. The probability of interruption is effected by the insider, however, not to detrimental effect as 87 % is still considered sufficient and the system effectiveness is down at 85 % from 92 %, but again, sufficient. Another example in Fig. ... and ... shows the difference of stopping a Kitten attack, in case the PPS response time was 600 s (ten minutes) in one case, or 900 s (fifteen minutes) in the other. In this case the change is detrimental and while ten minutes is sufficient response time, fifteen minutes is not, showing that in HYPO-BWR either the response force needs to be nearby. Otherwise the delay after detection needs to be significantly enhanced.

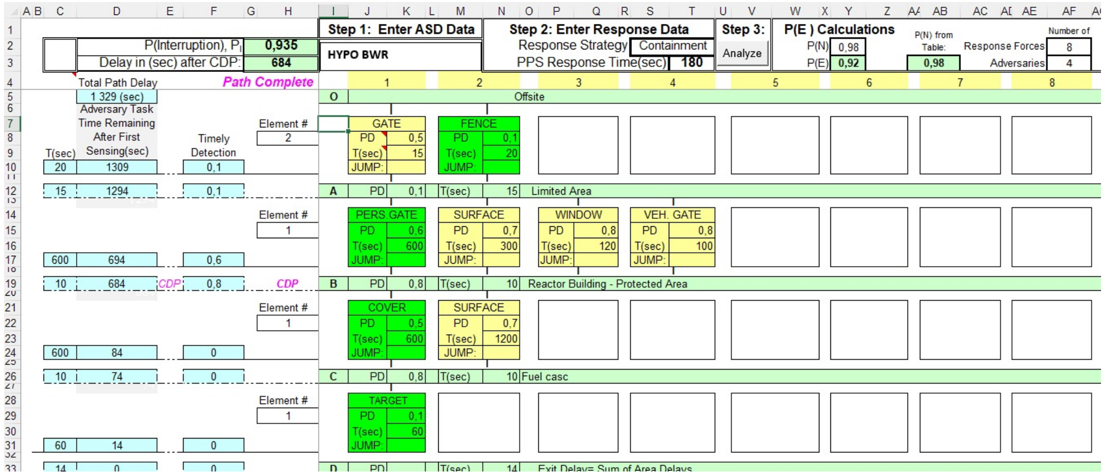

Fig. 7.3: VEASI analysis on HYPO-BWR, 4 Kitten adversaries with no insider help.

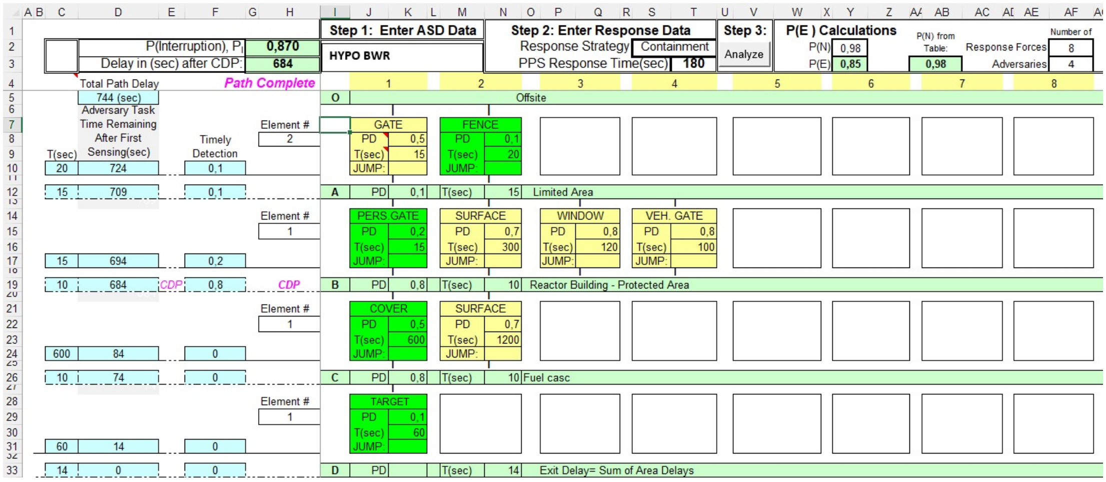

Fig. 7.4: VEASI analysis on HYPO-BWR, 4 adversaries, one of them insider, aiding in bypassing PERSONAL GATE.

HYPO-Fast on the other hand needs to be prepared for adversaries equipped with explosives, so suggested security measures need to reflect such.

1. Due to being so remote it is imperative that HYPO-fast has its own response force on site.

2. Outer fence: a double fence 2.5 m tall outer and 3.5 m tall inner, topped with barbed wire, between them barbed tape rolls. The inner fence also equipped with shaker sensor system. Expected delay 50 s.

3. Gate: CCTV surveillance going directly to the on-site response team, that needs to approve of any comings and goings, paired with shake detectors, granting high probability of detection.

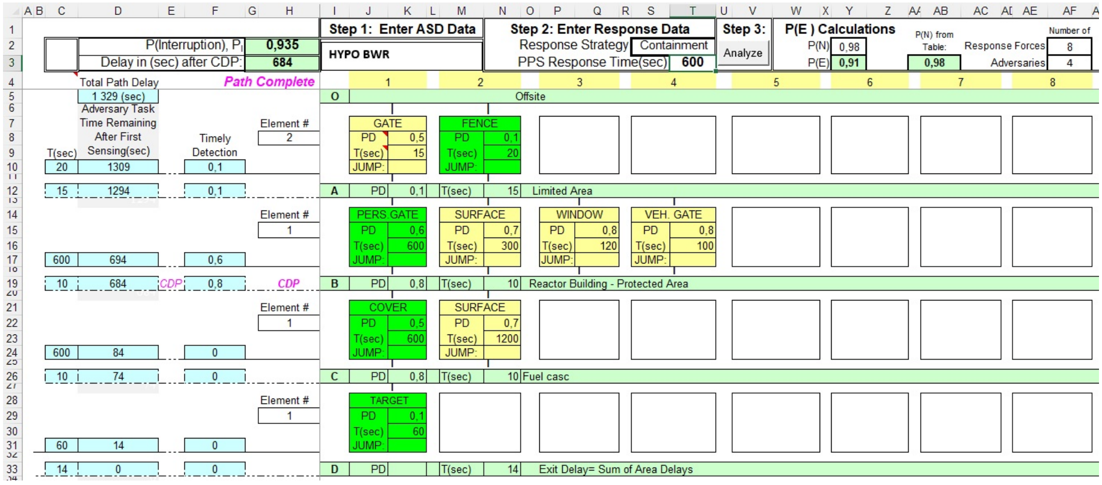

Fig. 7.5: VEASI analysis on HYPO-BWR, 4 Kitten adversaries, PPS Response time 600 s.

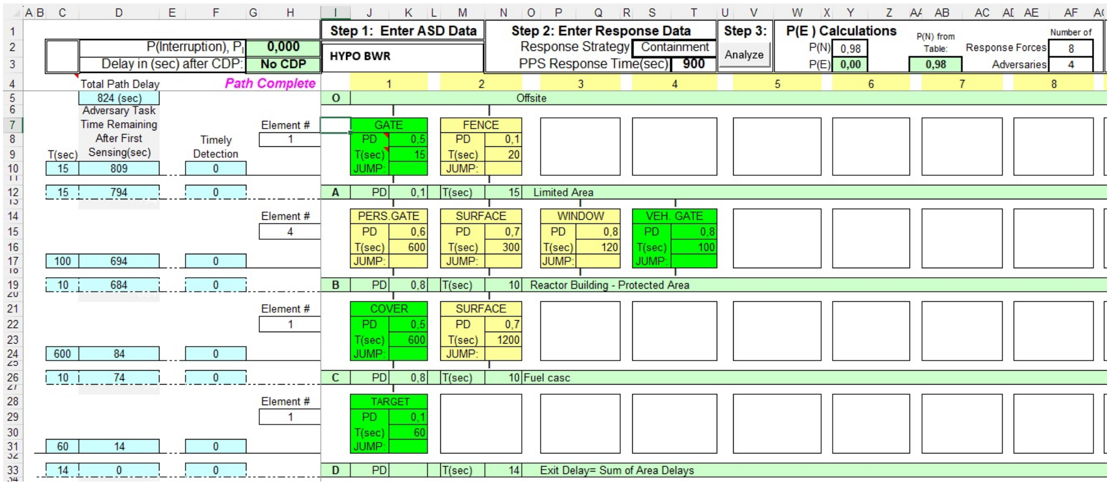

Fig. 7.6: VEASI analysis on HYPO-BWR, 4 Kitten adversaries, PPS Response time 900 s.

4. Wall: Walls need to provide sufficient delay when adversaries use explosives, therefore higher thickness of the reinforced concrete wall is necessary, resulting in both longer delay (unlike mere seconds with ordinary concrete wall and an explosive) and a need for a significantly larger amount of explosives. The blast significantly raises the probability of detection. Even higher thickness on the reactor building walls is considered.

5. Window: Security windows made of laminated glass, with bars. Sensors on all windows ensuring high detection probability. Estimated time of delay 20 s, considering the use of explosives.

6. Personal gate: Personal gates designed to withstand blasts. Entry control systems employed.

7. Vehicle gate: As in the previous case, a pair of interlocked gates where one needs to be closed for the other to open, ensuring high probability of detection.

8. The reactor itself together with the primary pump is installed below ground level and covered by a lid which needs to be raised in case of maintenance.

9. Surface: Very thick concrete floor.

10. Lid: Sturdy metal cover, fastened by large screws, normally opened by machinery.

Applying these criteria to the VEASI software, we get the following model for an attack by two Tigers equipped with explosives for the walls and mats to climb over the fences, whose goal is to sabotage the primary pump. The results are shown in Fig. 7.7.

For comparison, VEASI analysis of a scenario where goal is the same as in DBT, but the attack is conducted by Puppies instead was calculated, as shown in Fig. 7.8. As can be seen, even with no explosives the CDP does not change and the probability of interruption remains sufficient.

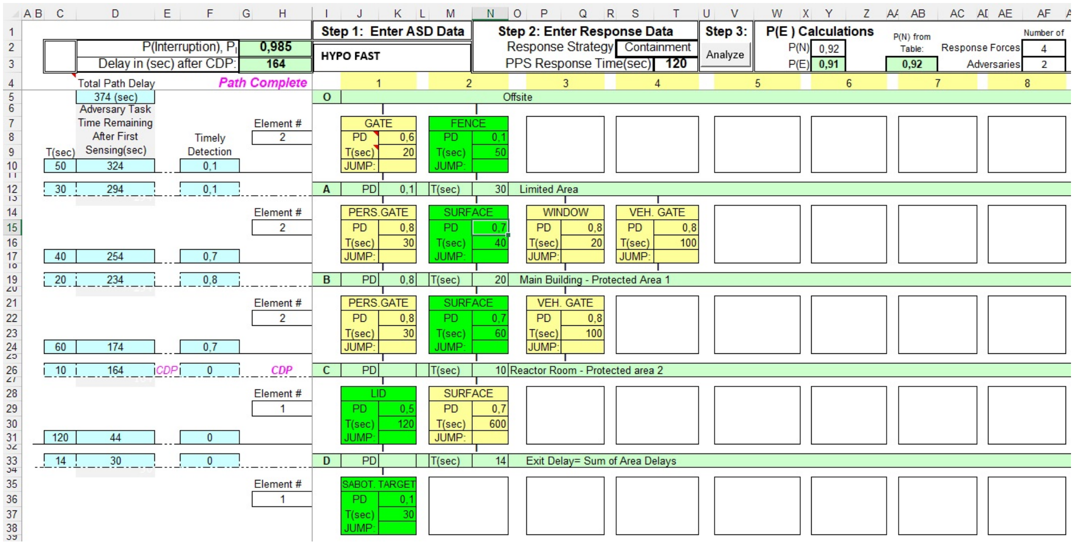

Fig. 7.7: VEASI analysis of a DBT on HYPO-fast

While a few concepts of SMRs intended for remote locations insist that their facilities are to be completely self-sufficient for years and operated remotely, with no on-site employees, this idea is not likely to work due to security reasons, as demonstrated on the example of HYPO-Fast in Fig. 7.9. If there was no response

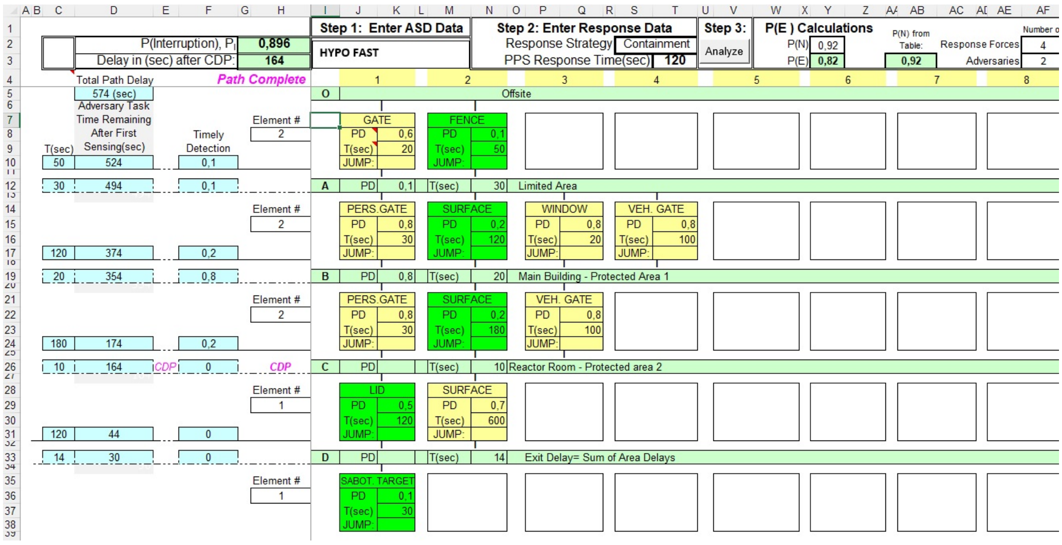

Fig. 7.8: VEASI analysis of a Puppy attack scenario on HYPO-fast

team on site or near the site and security was manned by a helicopter team from the nearest city, that would mean the response time of 30 minutes (1 800 s), with flight speed 300 km/h. Even a single adversary from the Puppy category would not be stopped in time, the probability of interruption being zero, despite all the reinforced walls and blast-resistant windows.

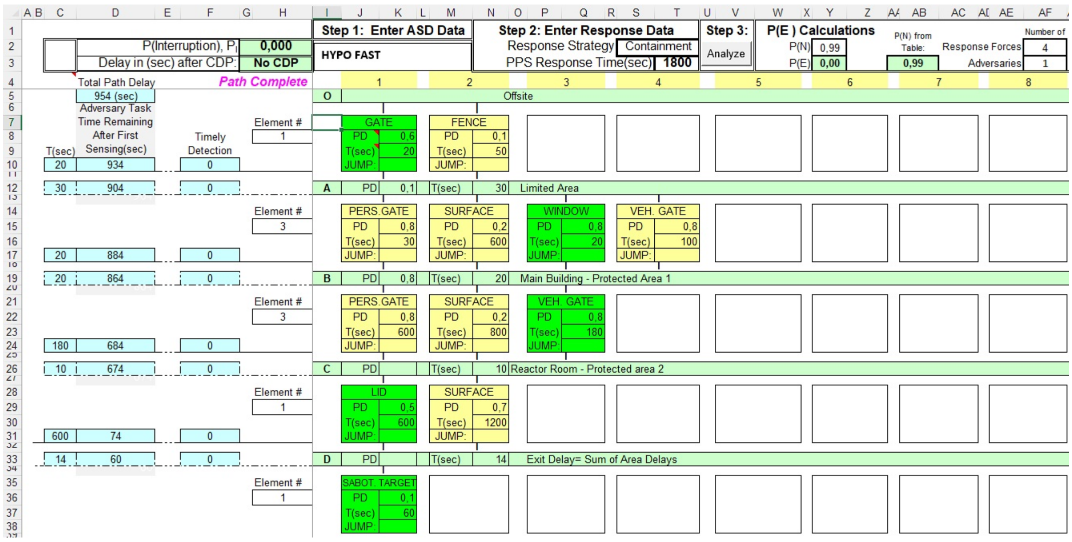

Fig. 7.9: VEASI analysis of a remote security case.

8 Comparison with current nuclear facilities

One distinctive feature that sets Small Modular Reactors (SMRs) apart from traditional Generation II PWR facilities lies in their inherent safety-in-depth design. Many SMR concepts incorporate advanced safety features that inherently mitigate the consequences of various adverse events, including potential sabotage. The modular nature of SMRs allows for more effective containment and isolation of radioactive materials, minimizing the potential impact of deliberate malicious acts. Advanced passive safety systems, such as natural circulation and passive cooling mechanisms, contribute to the resilience of SMRs against external threats.

In contrast, Generation II pressurized water reactor facilities often rely on active safety systems, and their larger scale and older designs may pose greater challenges in terms of complete containment. The robustness of SMR designs, often characterized by advanced materials and innovative cooling mechanisms, provides an additional layer of defense against the consequences of intentional acts of sabotage.

SMRs present a unique advantage in terms of security costs due to their smaller footprint. The reduced size of these reactors inherently limits the area that needs to be secured, resulting in more cost-effective security measures. The economies of scale in security are evident, as securing a smaller facility requires fewer resources compared to a larger, traditional nuclear power station. This characteristic makes SMRs particularly appealing for deployment in various locations, including remote sites or regions with less established infrastructure.

The cost-effectiveness of security measures in SMRs is further enhanced by advancements in technology, such as integrated security systems and remote monitoring capabilities. These innovations not only bolster security but also contribute to operational efficiency and cost savings. The scale and adaptability of SMRs make them well-suited for distributed energy generation, where security considerations are tailored to the specific characteristics of each site.

Innovations in SMR design extend to the conceptualization of facilities without traditional vital areas. Some SMR concepts, specifically from the PWR and BWR category, but also special cases from others, leveraging advancements in passive safety features and distributed layout, challenge the conventional notion of a central vital area. Instead, safety is integrated throughout the reactor, making the entire facility less susceptible to targeted attacks. This departure from the traditional vital area paradigm not only simplifies security considerations but also aligns with the principles of Security by Design (SeBD), emphasizing holistic safety integration into the core of the reactor design.

9 Conclusion

This work has undertaken a comprehensive exploration SMRs, shedding light on various facets of their design and security considerations. The initial sections provide an overview of the diverse landscape of current SMR concepts, emphasizing the significance of 3S risk analysis and the integration of security by design principles into their development. The exploration also offers a look into the regulatory frameworks for SMRs in the UK, USA, and Canada.

A pivotal aspect of the investigation revolves around target identification and the potential consequences of sabotage or theft, with a specific focus on TRISO and metal fuel. Enrichment levels are scrutinized to assess their vulnerability, offering valuable insights into the development of a robust vital area identification process. The examination extends to the formulation of a DBT and the intricate process of designing and evaluating physical protection systems for SMRs.

The practical application of these theoretical frameworks comes to fruition through the introduction of two hypothetical SMR facilities: one situated near an urban center featuring a BWR, called HYPO-BWR, and another in a remote location housing a fast reactor, called HYPO-Fast. The analysis of their respective DBTs and the proposed systems of physical protection sets the stage for an examination using the MP VEASI software. This computational tool allows for the quantitative assessment of the probability of interruption under various adversary scenarios, providing a metric to gauge the efficacy of the suggested security measures. HYPO-Fast analyses specifically shows that SeBD with the reactor placed underground, which is a feature considered by multiple SMR concepts, helps greatly with delay after detection. HYPO-BWR shows that thanks to safety by design and subsequent small EPZ, a need for a dedicated on-site response unit can be avoided, if the proximity of the city police is sufficient.

In a broader context, a comparative analysis between the security paradigms of SMRs and second-generation PWR facilities is conducted. Notably, it is observed that the inherent safety features embedded in many SMR designs may alleviate the necessity for security measures to be as robust as those employed in traditional reactor facilities. Additionally, the smaller footprint of SMRs contributes to potentially more cost-effective security solutions, further solidifying their appeal as a promising alternative in the realm of nuclear power generation.

In essence, this work serves as a pioneering exploration into the intricate intersection of design and security considerations for SMRs. By delving into the nuances of target identification, DBT development, and physical protection system design, it lays the groundwork for future research and practical implementations, fostering a deeper understanding of the evolving landscape of small modular reactors in the pursuit of clean and sustainable energy solutions.

Literature

1. Davis, W. *SMR's, Ships, and History* https://www.ans.org/news/article-2173/smrs-ships-and-history/.
2. Ingersoll, D. T. in *Small Modular Reactors* (ed Ingersoll, D. T.) 21–38 (Woodhead Publishing, Boston, 2016). ISBN: 978-0-08-100252-0. https://www.sciencedirect.com/science/article/pii/B9780081002520000021.
3. Liou, J. *What are Small Modular Reactors (SMRs)?* https://www.iaea.org/newscenter/news/what-are-small-modular-reactors-smrs.
4. *Small Modular Reactors (LWR designs)* U.S. Nuclear Regulatory Commission. https://www.nrc.gov/about-nrc/contactus.html (2024).
5. *Applicability of the Safety Objectives to SMRs* report (Western European Nuclear Regulators Association, 2021). https://www.wenra.eu/sites/default/files/publications/WENRA_RHWG_Report_on_applicability_of_safety_objectivers_to_SMR.PDF.
6. *Advances in Small Modular Reactor Technology Developments* 2022. https://aris.iaea.org/Publications/SMR_booklet_2022.pdf.
7. Ferretto, D. *Harmonise, SASPAM, ...* Consult. 9:30 2022-11-16. 2022.
8. *Microreactors* https://www.nrc.gov/about-nrc/contactus.html.
9. *The NEA Small Modular Reactor (SMR) Strategy* https://www.oecd-nea.org/jcms/pl_26297/the-nea-small-modular-reactor-smr-strategy.
10. *BWRX-300* status report (GE Hitachi and Hitachi GE Nuclear Energy, 2019).
11. *VOYGR* NuScale Power Corporation. https://www.nuscalepower.com/-/media/nuscale/images/products/voygr/voygr-4.jpg?h=1080&iar=0&w=1080&hash=5CCE13939CBE27FA43CDDE9A18B69EDB (2024).
12. *Rolls-Royce Small Modular Reactor* https://www.kernvisie.com/innovatie/innovatieve-kernreactorontwikkeling/rolls-royce-smr.html.
13. Chen, H., Li, C., Xing, H. & Fang, C. The R&D of HTR-STAC Program Package: Source Term Analysis Codes for Pebble-Bed High-Temperature Gas-Cooled Reactor. *Science and Technology of Nuclear Installations* **2018,** 1–9 (Dec. 2018).

14. *Outline of High Temperature Engineering Test Reactor* Japan Atomic Energy Agency. https://www.jaea.go.jp/04/o-arai/nhc/en/faq/httr.html (2024).

15. Ingersoll, D. Deliberately small reactors and the second nuclear era. *Progress in Nuclear Energy* **51,** 589–603 (May 2009).

16. *ENERGY WELL* press release (UJV Group, 2018).

17. Bentoumi, G., Chaudhuri, A., van der Ende, B. & Bhaskar, S. Safety and Security for small modular nuclear reactors (SMRs). *IAEA Conference* **278/560** (Feb. 2020).

18. Williams, A. D., Osborn, D. & Cohn, B. Security Safety and Safeguards (3S) Risk Analysis for Small Modular Reactors. https://www.osti.gov/biblio/1640767 (June 2019).

19. Duguay, R. Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to Protect Against Malicious Acts and Evolving Threats. *International Journal of Nuclear Security* **7** (Dec. 2020).

20. Nilsson, A., Jorant, R. & Luongo, K. GNI Advanced Reactors Security Analysis & Findings. https://globalnexusinitiative.org/wp-content/uploads/2018/12/GNI-Security-Nov.-15-FINAL-11.13.18.pptx (2018).

21. Šošková, J. *Stanovení zbytkového tepelného výkonu paliva* 2019.

22. Yacout, A. M. *Long-life Metallic Fuel For the Super Safe,Small and Simple (4S) Reactor* report AFT-2008-000056 (2008).

23. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* INFCIRC/225/Revision 5. International Atomic Energy Agency (2011).

24. Varnado, G. B. & Whitehead, D. W. *Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants* report SAND2008-5644 (2008).

25. Evans, A., Byrum, C., Stanford, D. & Sandt Emily nad Goolsby, T. *Physical Protection Recommendations for Small Modular Reactor Facilities* report SAND2021-15712 (2021).

26. Starý, R. *Vital Area, Physical Protection, Security* consult. 9:00 2022-10-18. 2022.

27. *Identification of Vital Areas at Nuclear Facilities* International Atomic Energy Agency (2012).

28. *National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements* Revision 1. International Atomic Energy Agency (2021).

29. *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities* International Atomic Energy Agency (2021).

30. Starý, R. *Minimal Acceptable Value* consult. 10:00 2024-01-11. 2024.

31. Garcia, M. Design and evaluation of physical protection systems: Second edition. *Design and Evaluation of Physical Protection Systems: Second Edition,* 1–351 (2008).

32. *The Twentieth International Training Course* report SAND2007-6467P (2007), 17-1 - 24S–8.

33. *Multipath Very-Simplified Estimate of Adversary Sequence Interruption (MP VEASI)* Copyright 2017 National Technology & Engineering Solutions of Sandia, LLC (NTESS). Under the terms of Contract DE-NA0003525 with NTESS licensed by CTU, license n. 11755. 2017.

34. *ČSN EN 1627 - Dvěře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace* technical norm (Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2021).