Levels of protection for nuclear energy supply and distribution and transmission grid systems

- Abstract –

Ph. Lc. Thomas Riehl, 10.10.2025

The provision of energy, particularly electricity, constitutes a multifaceted network involving generation, transformation, and conversion processes that operate in a continuous manner and are constrained solely by the available natural resources of the specific regions. In recent times, the focus of hostile actors has increasingly shifted toward central energy producers and their transport routes. These actors include lone perpetrators, terrorist groups, and states with conflicting interests. The vulnerability of sovereign states is particularly evident in current conflicts. The targeted destruction of energy facilities can be used as a means of exerting pressure on state sovereignty, the necessary economy and business, and the population. The vulnerability of nuclear power plants and their infrastructure, specifically the transmission and distribution networks, is of particular concern. These facilities, in conjunction with the distribution of electrical energy, present significant risks of failure and harbor dangers with an impact that has persisted for centuries due to their explosive power and long-term contamination. For decades, numerous governmental and non-governmental organizations have been working to develop concepts that can intelligently link central and decentralized supply structures. The objective of these efforts is to minimize failure rates in times of crisis and war. In this context, the debate frequently emerges regarding the notion that the reliable provision of energy necessitates concrete security and investment concepts. Transformer stations operated by transmission and distribution network operators in Western countries are considered a key factor in this thesis. Currently, these systems can be physically secured through the implementation of efficient military protection measures, such as the Rheinmetall C-UAS Jammer (Rheinmetall, n.d.). Concurrently, multi-layered protection mechanisms are implemented at the IT and OT levels to ensure secure software operation. (CNAS, 2025) Nevertheless, the requisite level of protection is contingent upon the type and size of the supply area, as well as the overall security of supply of a federal state and its territorial integrity.

The funding of investments in energy infrastructure must be supported by federal funds, tax revenues, commercial revenues, and private investors. The role of investors is often examined using an inductive, qualitative interpretive research approach that employs case studies and the Delphi method. (Wojciech, 2024) The objective is to obtain diversified insights into intricate interrelationships. In principle, attacks on instrumentation and control systems (I&C) in nuclear power plants result in system errors that extend beyond the permissible operating parameters. Consequently, a multi-level protection concept, known as "Defense in Depth" (DiD), must be implemented. As indicated by IAES (2021), it is imperative to consider non-computerized systems to mitigate the risk of cyberattacks. The implementation of computer security principles in I&C systems is instrumental in adhering to safety-related requirements and minimizing future retrofits, a facet that carries significant economic implications. The security DiD is divided into independent system levels with different functions to prevent the progression of failures. The objective of physical separation and independence is to avert system failures from escalating to a security concern. The field of computer security has historically centered on three fundamental tents: confidentiality, integrity, and availability. A graded security level is often implemented, with critical functions receiving higher levels of protection. The Delphi method is a structured procedure for the systematic collection and consolidation of expert opinions. This approach facilitates well-founded assessments of future developments, incorporating cost-benefit analyses, as well as uncertainties and diverse perspectives. This approach enables accurate documentation of subjective perspectives and dynamic processes within organizations. Investments in physical protective measures, such as non-governmental defense drones and missile defense systems, and preventive state-military surveillance are thus placed in the context of the operators' economic network cost analysis. This frequently manifests as a demonstrable advantage, indicating that the comprehensive protection of nuclear energy facilities and their network

operations hold greater value than investments from non-governmental and governmental entities.

In the context of IT/OT structures in comparison to INPRO (International Project on Innovative Nuclear Reactors and Fuel Cycles) planning and DCSA (Defensive Computer Security Architecture) specifications, clearly defined technical and strategic framework conditions for nuclear power plants are considered. As stated in the 2021 report by the International Atomic Energy Agency (IAEA), these measures are legally mandated with the objectives of achieving economic optimization and ecological balance. The implementation of the Delphi method in the context of power plant protection, encompassing both cyber and physical security domains, has the potential to contribute to economic optimization. The application of structured expert surveys and national guidelines, such as those promulgated by the U.S. Department of Transportation, facilitates the assessment of pertinent risks on a solid foundation and the mitigation of uncertainties. This approach enables a more targeted allocation of resources, thereby circumventing superfluous investments. This is a point of consideration for numerous operators and government budget planners. In contrast to crisis and war simulation, however, the INPRO service employs a strategic-normative approach to support national planning processes in the field of sustainable nuclear energy systems (NES). The implementation of long-term objectives and regulatory requirements is achieved through the utilization of structured process systems, thereby facilitating precise estimates of maintenance and reinvestment costs. INPRO planning necessitates a prompt response to crisis situations through preparatory structural procedures.

This analysis demonstrates that the long-term security of nuclear power plant supply, in conjunction with their grid systems, can be ensured only through meticulously planned safety concepts that involve targeted investments. Presently, there is an absence of comprehensive assurance regarding the protection of nuclear facilities and the secure transportation of electrical energy. This is a challenge that must be recognized and overcome

to protect national sovereignty and economic stability. The implementation of the security measures described herein also necessitates continuous monitoring and adaptation of the protection systems to changing threat situations. The integration of real-time data analysis and automated control mechanisms is imperative for the identification of potential risks at an early stage and the subsequent implementation of appropriate responses. The integration of stochastic methods also enables a quantitative assessment of failure probabilities, thus supporting the prioritization of investments in critical system components. A holistic approach, encompassing both physical and cybernetic protection systems, has been demonstrated to strengthen the resilience of the energy supply in the long term. This approach also ensures that the interests of owners and the requirements of stakeholders are considered in equal measure. Achieving a balance between security, economic optimization, and ecological balance in the long term necessitates systematic and precise control. Concurrently, it is neither feasible nor comprehensive to ensure uninterrupted access to the primary energy supply. This necessitates an increased emphasis on decentralized supply concepts with multi-area networks. While this conversion entails substantial expenses, it has the potential to markedly enhance supply security at the local level, particularly during crisis scenarios. In the future, a combination of different approaches will be necessary to ensure meaningful modeling.

A PSVBTR Mastercom system investment strategy can be based on the following sample calculation. According to Statista (2025), the global nuclear power generation in 2024 was approximately 377 gigawatts. When calculated using a focused economic operator model, the cost of this electricity is determined to be approximately $69 per hour per gigawatt hour, or $0.182 per gigawatt hour. A failure rate of 0.01 percent over a 360-day period can result in projected costs of approximately $6,000 per hour per gigawatt.

The annual energy consumption of an average industrial area is estimated to be approximately 1.5 terawatt hours, which corresponds to costs of approximately $287 per hour (Janson,

2025). In the event of a total failure, however, the downtime costs would amount to approximately $6,000 per hour, and the economic damage would likely be considerably higher. This is in stark contrast to the approximately $100 million investment costs, which encompass military armament and reconnaissance, protective equipment for military cyber and counterespionage, and other related expenditures, measured over a three-year period. These measures have the potential to substantially mitigate the financial repercussions of the shutdown, estimated to amount to approximately $52 million in reduced downtime costs, as well as an estimated annual economic loss of approximately $5 billion, according to the Delphi and Biba models. Consequently, an average annual profit of more than $50 million is realized through the augmentation of nuclear power plants' protection levels and the enhancement of their armaments, as well as those of their distribution and transmission grid operations.

References

Drohnenabwehr Toolbox. (n.d.). Rheinmetall. https://www.rheinmetall.com/de/produkte/flugabwehr/flugabwehrsysteme/drohnenabwehr-toolbox

Center for a New American Security (CNAS). (2025, April 7). *AI and Autonomy in Future Warfare*. CNAS. https://www.cnas.org/research/defense/the-future-of-warfare

Wadhwani, P. (2024). Marktgröße für Drohnenabwehr – nach Komponenten (Hardware, Software), nach Plattformen (bodengestützt, Handheld, UAV), nach Abwehrtyp (destruktives System, zerstörungsfreies System), nach Anwendungen (Erkennung, Störung, Unterbrechung), nach Endbenutzer und Prognose, 2024 – 2032. In *Global Market Insights Inc.* https://www.gminsights.com/de/industry-analysis/anti-drone-market

Statista. (2025, September 15). *Installierte Leistung der Kernkraftwerke weltweit bis 2024*. https://de.statista.com/statistik/daten/studie/28692/umfrage/leistung-der-atomkraftwerke-weltweit/

Janson, M. (2025, May 2). Rechenzentren überholen Heizungen bei Stromhunger. *Statista Daily Data*. https://de.statista.com/infografik/34393/prognose-zum-anstieg-des-weltweiten-strombedarfs-nach-sektoren/

Wojciech Muras, & Katarzyna Szczepańska-Woszczyna. (2024). *Shareholders, Strategy and Value Creation : The Case of the IT Sector*. Routledge.

Iaea. (2021). *Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants* (Vol. 00003). International Atomic Energy Agency.

Iaea. (2021). *Planning Enhanced Nuclear Energy Sustainability: Analysis Support for Enhanced Nuclear Energy Sustainability (ASENES) : An INPRO Service to Member States* (Vol. 00003). International Atomic Energy Agency.