Journal of Energy

ISSN 1849–0751 (On-line)
ISSN 0013–7448 (Print)
UDK 621.31

https://doi.org/10.37798/EN2023721

ENERGIJA

VOLUME 72 Number 1 | 2023

Journal of Energy

Scientific Professional Journal Of Energy, Electricity, Power Systems
Online ISSN 1849–0751, Print ISSN 0013–7448, VOL 72
https://doi.org/10.37798/EN2023721

Published by
HEP d.d., Ulica grada Vukovara 37, HR–10000 Zagreb
HRO CIGRÉ, Berislavićeva 6, HR–10000 Zagreb

EDITORIAL

The first paper is “Integral Approach for Overvoltage Management Based on FieldData and Modelling”. This paper presents an integral approach for managing power transformer overvoltages, combining field measurements and advanced electromagnetic transients (EMT) modeling. The approach involves detailed simulations, including high-frequency transformer models, and continuous monitoring of overvoltage events in the network. By implementing this framework, power utilities can gain insights into overvoltages, implement mitigation measures, and improve long-term planning and equipment maintenance. This approach enhances economic planning, fleet management, equipment reliability, and reduces downtime, contributing to overall network reliability. The work also explores the statistical analysis of network transients for system operators, enabling better insulation coordination across geographically diverse power network regions.

The second paper is “Assessing the Scale of the Radioactive Waste Management Problem: A Review of European Union and International Reporting”. This paper reviews the latest reports from the IAEA and EC, focusing on RW inventory and disposal status. The findings provide comparable information on RW policies, frameworks, and programs, with emphasis on inventories, practices, and technologies. The paper presents findings on the overall situation in the European Union (EU), comparing inventories between EU Member States and global reporting from the IAEA. It normalizes the presentation of inventories per person and land area to improve understanding of the scale of the RW management problem. The analysis reveals a relatively small amount of RW, with the majority being low or very low level and a significant portion already disposed of. Hazardous waste inventories are also compared, demonstrating the manageable nature of RW.

The third paper is “Application of fully automated centralized voltage regulation in transmission system operation management This work focuses on implementing an advanced VVC system for real-time control of reactive power, both in partially automatic and fully automatic modes, using the optimal power flow algorithm. HOPS is among the first transmission system operators to implement closed-loop reactive power regulation. The VVC system can also be operated in semi-automatic or manual modes, with safety algorithms in place to prevent voltage breakdown and equipment overloading. Although the closed-loop approach is rarely used, HOPS has successfully implemented it. However, it is crucial for transmission system operators to be aware of potential risks and exercise caution. HOPS initially prioritized the safer semi-automatic mode, which remains under the control of the dispatcher or operator.

The fourth paper is “Graphical Visualisation of the MCNP Mesh Tally File”. This paper introduces an updated version of the MTV3D program, designed for visualizing mesh tally files generated by the MCNP code. The improvements include enhanced figure export functionality, the ability to switch between linear and logarithmic value axes, dynamic figure scaling, and the inversion of relative errors. MCNP is a widely used Monte Carlo computer code for simulating neutron, photon, and electron transport in three-dimensional configurations. The graphical display provided by MCNP aids in model setup error-checking and the visualization of results from mesh tally files. The updated MTV3D program is showcased using hybrid-shielding problems involving the ADVANTG3.0.3 and MCNP6.1.1b codes. Key features of MTV3D include 3D visualization of mesh-based results, cut-plane results with surface plots, and curve plots for independent axes. The program was developed using the MS Windows SDK 8.1, supporting Windows 7 to 10, and employs Win32 interface and Windows Controls library procedures for application controls.

The last paper is “Cybersecurity of the Power Production and Distribution of Critical Infrastructure”. The paper presents a comprehensive approach to managing the cyber security of critical electricity national infrastructure in power production and distribution. The author, responsible for protecting and ensuring the resilience of the national electric power infrastructure against cyber threats, discusses an effective and universally applicable methodology. The management of cyber security is based on a complete and comprehensive Program that adheres to current legislation and established standards. The paper highlights the complementary activities of risk assessment and Business Impact Analysis (BIA) to ensure the continuity of industrial processes in critical electric infrastructure. However, there is a need to address vulnerabilities and associated risks that may impact the continuity and integrity of electricity production and distribution processes. Incorporating and addressing these emerging vulnerabilities within the Program framework outlined in the paper is an important future consideration.

Igor Kuzle
Editor–in–Chief

Journal of Energy

VOLUME 72 Number 1 | 2023

journal homepage: http://journalofenergy.com/

Integral Approach for Overvoltage Management Based on Field Data and Modelling

Bruno Jurišić, Tomislav Župan, Božidar Filipović-Grčić and Goran Levačić

***Summary* — The requirements for the power network to be flexible and to be able to transmit more power are becoming more important as a consequence of high share of the renewables. Therefore, to maintain the level of reliability of the power network, it is necessary to monitor more and more data as well as to better understand the phenomena that might exist in the power system, such as transients. One of the points that are of interest are interaction between power transformer and the other components in the network. A failure of such component may lead to power network unavailability and high economic cost. According to the CIGRE WG A2.37, high portion of the transformer failure may have been caused by the overvoltage. Therefore, it is important to handle overvoltage in the power network with high care. In this paper, an integral approach for power transformer overvoltages management based on field measurements and advanced electromagnetic transients (EMT) modelling is presented. It consists of simulating overvoltages using detailed power network models, including the high frequency transformer models and continuous monitoring of overvoltage events at the places of interest in the power network. This work gives a framework for dealing with overvoltages in the power network that could be implemented by power utilities.**

***Keywords* — Power transformer, overvoltages, high frequency, EMTP, modelling, asset management, field measurements**

I. Introduction

Modern power systems with high share of renewable energy sources (RES) and implementation of power electronic devices, such as DC lines, are more prone to transient events. Overvoltages can occur in the power network due to switching operations or can be caused by lightning activities. These overvoltages may cause failure of the components in the network, even though good practices of the insulation coordination were followed.

One of the critical system components is a power transformer. In the case of a power transformer failure, economic consequences can be several times higher than the cost of the transformer itself. Therefore, it is necessary to establish asset management system for such components. A crucial part of this system is to mitigate overvoltages as much as possible. Therefore, it is necessary to know the real types and severity of overvoltage events for a specific device, and to understand its response to them. In general, two approaches to evaluate the overvoltages that may exist at transformer terminals are possible.

The first one is to run simulations in EMTP-type software with detailed wideband transformer models [1]. Based on the results of simulations, one can determine the waveshapes of possible overvoltages. These waveshapes can be useful information for the transformer manufacturer, in order to produce the transformer that will not contain natural winding frequencies which are likely to be triggered by the overvoltages. In the case when natural frequency of the transformer winding is close to the main overvoltage frequency, internal insulation breakdown may occur due to the phenomenon called resonance. Moreover, these simulations can help to better design and dimension the equipment in the transformer bay. The problem with this approach is lack of transformer data, especially during the procurement process. For the transformers that are already in operation, transmission system operators can build its own transformer model based on measurements, also known as black box model.

Another approach is to continuously monitor overvoltages at the transformer terminals in the substation. This can be done by using the transformer monitoring system equipped with devices for monitoring of transients. Overvoltage monitoring can help in extending the knowledge of transients that occur in power networks, as these can significantly differ from the standard test impulses [2]. Such data can be used either in system planning phase or in defining the protection specification. By more thoroughly specifying the power transformer, it can be able to withstand possible nonstandard overvoltage waveforms that may occur at the particular position in the power network. On the other hand, adopting or installing better specified protection devices can help in eliminating potential equipment failures.

Both approaches lead to gathering more knowledge on overvoltages. This knowledge can be used in proper dimensioning of both the transformer and its protection devices, which can lead to better economic decisions and general increase in reliability. To maximize the level of knowledge on interactions between power transformer and the power networks, the best practice would be to use both of the presented approaches, EMTP simulations and transient monitoring.

One of the main goals of the currently active CIGRE WG A2.63 is to analyze whether the standard test impulse waveforms are enough to describe all the potential overvoltages that can occur in the power network. The paper is in line with the mentioned

(Corresponding author: Bruno Jurišić)
Bruno Jurišić and Tomislav Župan are with the Končar – Electrical Engineering Institute Ltd., Zagreb, Croatia
(e-mails: bjurisic@koncar-institut.hr, tzupan@koncar-institut.hr)
Božidar Filipović-Grčić is with the Univesrity of Zagreb Faculty of Electrical Engineering and Computing, Zagreb, Croatia
(e-mail: bozidar.filipovic-grcic@fer.hr)
Goran Levačić is with the Croatian Transmission System Operator Plc. (HOPS) (e-mail: goran.levacic@hops.hr)

CIGRE WG, as it analyses the overvoltages measured at 220/110 kV substation through extended time period. Statistical analysis is done based on grouping of measured data, in order to compare the measured overvoltages with the standard ones. Genetic algorithm and energy equivalent method is used to find double exponential expressions that fits measured overvoltages. In that way, overvoltage waveform parameters, such as rise and tail time, can be more precisely compared with the standard ones.

The aim of this work is to explore the possible applicability of new insights that the statistical analysis of network transients can give the system operators, and how it can affect the insulation coordination at geographically different power network regions. In this paper, first the examples of high frequency transformer modelling, which is used to evaluate overvoltages using EMT simulations, is presented. Then, a monitoring of transient events in vicinity of a power transformer, installed in the network with high share of RES is presented. The results of long term overvoltage monitoring are analysed using statistics. As these two approaches are necessary inputs for successful power transformer asset management, directions for implementation of framework for overvoltage management based on field data and modelling are given in forth section. Fifth section gives the conclusions of this approach and work.

II. Emtp Simulation Inlcuding High Frequency Transformer Modelling

In this section, a detailed EMTP modelling of the power network including high frequency transformer modelling is presented. The aim of this section is to provide an insight for a power utility on how to deal with simulation of fast overvoltages that includes detailed transformer models.

In general, to simulate fast and very fast transients in the power system, high frequency transformer models are needed [3]. High frequency components of such overvoltages are causing resonant behavior inside the transformer. As a consequence of this resonance, electromagnetic behavior of a transformer becomes complex and traditional transformer models are not suitable for its representation.

Wide-band transformer models are classified in four different categories, in accordance with the data they require for their construction and application: simplified models, Black Box models, White Box models and Grey Box models [4]. From the perspective of power utility, the only model, besides simplified ones, which can be used straightforwardly is the Black Box model. They are based only on the measurements that can be conducted at transformer terminals, using standard SFRA or VNA equipment [5], [6]. Measurements can be done both in the HV laboratory or on field. Only condition that has to be satisfied is to have a proper grounding which is satisfied both in the HV laboratory and in the substation.

Measuring on field requires more preparation as power transformer has to be deenergized and disconnected from the power network, which can be seen in Figure 1.

Fig. 1. On field measurements of power transformer admittance matrix.

The admittance matrix for the particular 150 MVA 220/110 kV autotransformer unit has been measured on field and EMTP model is established based on the measurement results and fitting, which can be seen from Figure 2 [7], [8].

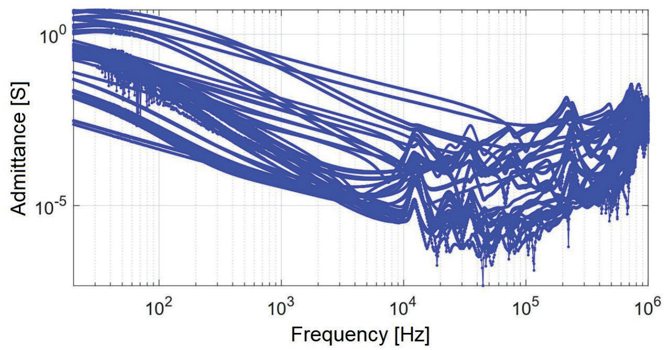

Fig. 2. Frequency dependent admittance matrix coefficient for a 150 MVA transformer unit [9]

Once the model is established, it can be used in EMTP to simulate overvoltages [10]. An example of EMTP simulation of a lightning strike to a 220 kV overhead line tower, which led to flashover in phase B, following by the flashover in phase A, is given below. Observed transformer unit is located in the area with significant lightning activity and high soil resistivity due to the rocky mountain terrain [11]. Seven 110 kV and two double-circuit 220 kV overhead lines are connected to the substation with three autotransformer 220 kV/110 kV working in parallel.

Particular lightning strike was detected by the lightning location system, while SCADA detected double phase to ground short circuits, in phases A and B. Measured overvoltage amplitude, obtained from the installed transient recorder was approximately 320 kV, as can be seen from Figure 3. Waveshape of the overvoltages suggest that the fault, following the lighting strike, was double phase to ground fault in phases A and B.

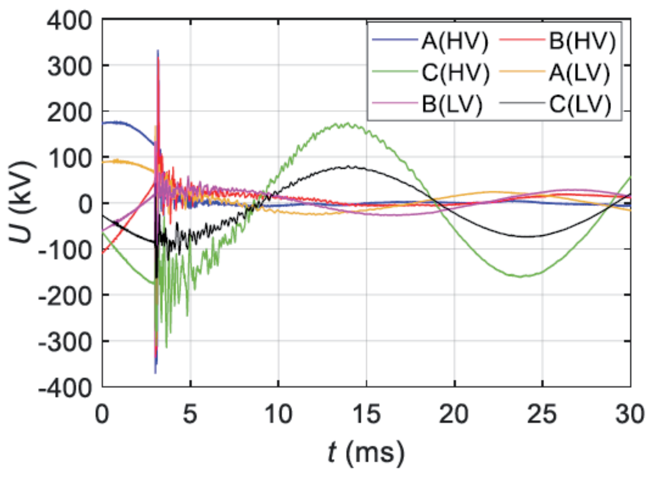

Fig. 3. Measured overvoltages, by transient recorder, in the case of double phase to ground short circuit

In EMTP simulation, overvoltage is simulated as a lightning strike to the tower of the 220 kV overhead line. The overvoltage propagated to the 220 kV part of the substation, through the transformer to the 110 kV side as can be seen from Figure 4. Modelling includes detailed EMTP model of the substation as well as the overhead lines connected to the substation. Overhead lines, busbars and connections inside substation are modelled using frequency dependent line models [12]. Surge arresters are installed in every transformer bay (surge arresters with rated voltage U_r=198 kV are installed at 220 kV level and with U_r=108 kV at 110 kV level) [11]

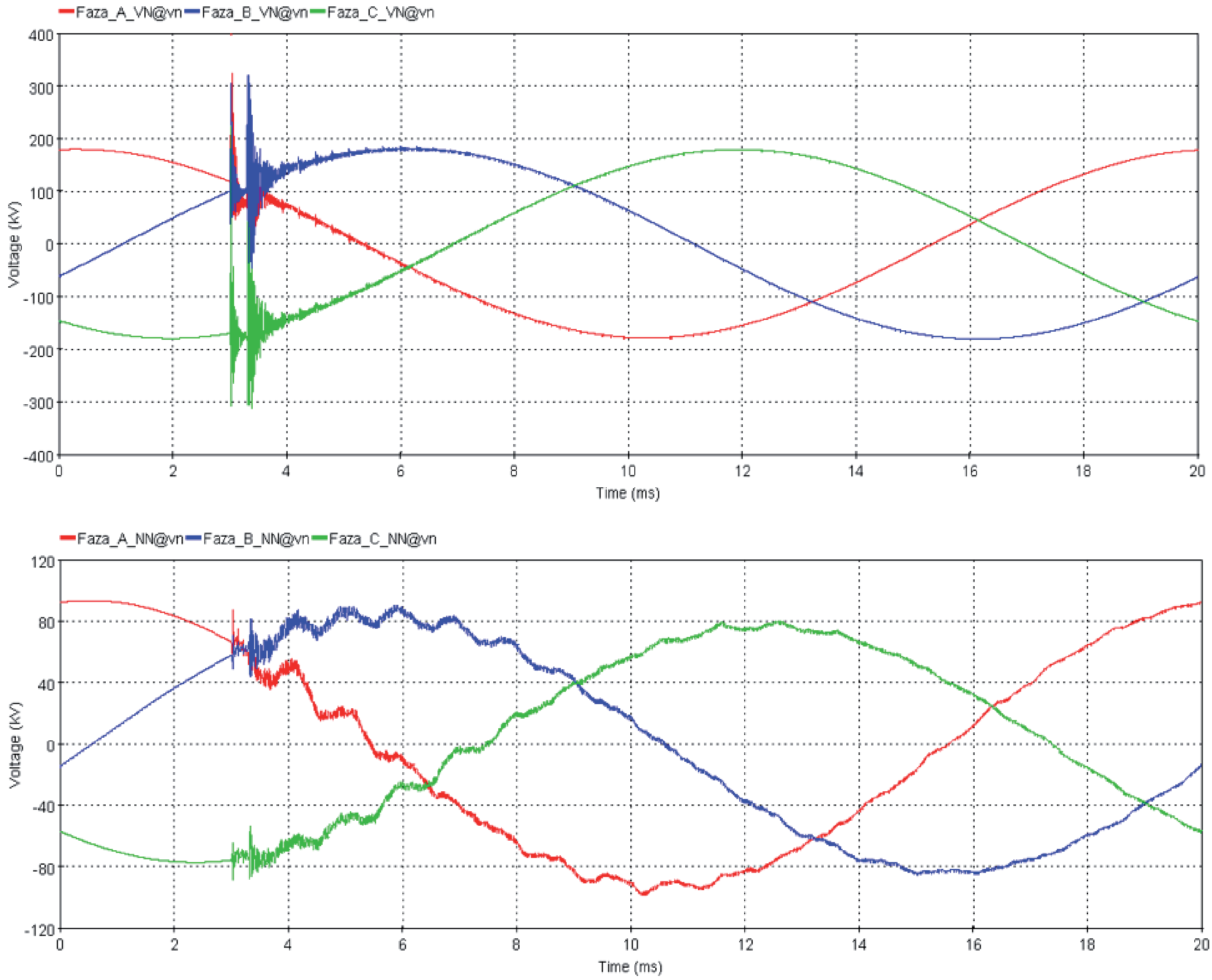

Fig. 4. Simulated lightning overvoltages in EMTP using power network model together with detailed black box transformer model (upper figure – HV side, lower figure – LV side, red – phase A, blue – phase B, green – phase C).

and are modelled using their voltage current characteristics while instruments transformers are modelled with capacitance to the ground. Corona attenuation was neglected because of short distance between lightning strike and substation.

Simulated overvoltages consist of lightning strike overvoltage and system response, which is quite complex due to numerous reflections inside the substation and between adjacent substations connected with 110 kV overhead lines. More specifics on modelling can be found in [10]. The amplitude of the simulated overvoltage is comparable to the measured ones while the oscillations following the initial overvoltage differ due to lack of damping in the model.

It is important to note that these models are not capable of simulating transformer inner behavior as they do not include any information on transformer inner geometry. These models can provide utilities with an idea of the overvoltages that can exist at the transformer terminals. It can be valuable when it comes to testing of the transformer and comparing the insulation stresses and safety factors to standard test impulses. To calculate safety factors on the inner insulation, white box models are needed. This part has to be done in cooperation with the transformer manufacturers.

III. Continuous Overvoltage Monitoring in Power Network

This section shows another approach on how to evaluate overvoltage hazard in the power system. It consists of continuously monitoring overvoltages at different locations in the power system. Once the data is collected, it is possible to statistically analyze it, and obtain the geographical allocation and severity of overvoltages in the network [13]. In this section, a result of statistical analysis of overvoltage parameters, measured at 220/110 kV, 150 MVA autotransformer located in Croatian coastal area, is briefly reported. More about the used methodology can be found in [14]. In the section, the equipment for overvoltage monitoring is presented first, following by the results of statistical analysis.

The transient monitoring system measures voltages on a measuring tap of the transformer's high voltage bushing. It consists of specially designed adapter for the connection to the bushing measurement tap, with measurement circuit including the matching impedance, capacitance divider, coaxial cables, acquisition unit and associated software [15]an on-line overvoltage transient recorder is used with the ability to sample, analyze and store transients at transformer terminals in real-time. In this paper, transient overvoltage monitoring system is presented. Overvoltages are measured on the outside measurement terminal of the shunt reactor and transformer bushing. Field experience regarding the application of monitoring system in Croatia is described including different cases of lightning and switching overvoltages. Lightning overvoltages recorded by monitoring system are correlated with data from the lightning location system (LLS. The system is continuously logging the transient overvoltage data with a high sampling rate. Since this results in a very large data set, the algorithm is set to only save a time frame of the measurements when the trigger detects a rise or an anomaly in the voltage. To accomplish this, continuous voltage measurement is performed with an additional analogue input module and two stage matching circuit is needed.

The embedded acquisition card is fast enough to capture data with a time resolution of 0.5 μs (when six different voltages are observed simultaneously), which is enough for transients containing frequency components lower than 1 MHz. The number of points recorded per event is 10^6, which leads to a total recording time of 500 ms per event. The system is already installed and operates on different locations in Croatian transmission system. The performance check of the system has been done in both frequency and time domain [10], [16]. In [16], the system was tested in the high voltage laboratory for SI, LI and LIC on 100 MVAr 220 kV shunt reactor, while in [10] the system was tested against the simulation results of transferred overvoltage, caused by lightning. The simulation included wideband black box power transformer model in EMTP.

The overvoltages are continuously measured in 220/110 kV substation, the same substation as in the example in the previous section. The observed events have occurred from May 2020 until October 2020 and include a period of the year with most severe lightning activity. Total number of recorded events is 123, which includes switching, lightning, and other type of overvoltages that occurred during the observation period. Most of the events are overvoltages caused by lightning and most of them did not cause insulation failure. The measured overvoltage waveshapes are bidirectional and differ from the standard test impulses. Therefore, the signal processing has to be made in order to compare the measured waveshapes to the standard ones.

Every observed overvoltage *U*(t) can be equivalented using the well know double exponential function:

$$U(t) \approx kA(e^{-\alpha t} - e^{-\beta t}), \tag{1}$$

where *k*, and are constants dependent on the wave shape of the observed overvoltage, while *A* is the amplitude. *k* is the function of and , while is a function of tail time, t_h and is a function of the front time, t_f. Front and tail time of the standard lightning impulse are specified in [17], respectively as 1/0.6 times the interval *T* between the instants when the impulse is at 30 % and 90 % of the peak voltage value, and the time between the virtual origin and the instant when the test voltage curve decreases to 50 % value.

In the paper, amplitude of the overvoltage is specified as the highest voltage peak value of the observed overvoltage, while the front time is calculated as the time from the signal trigger to the highest voltage peak value. Once these two parameters are specified, it is necessary to calculate a tail time. This parameter can be found using the energy method presented in [13].

Calculated statistical parameters and probabilities are given in Table 1.

Table 1.

Statistical parameters of measured overvoltages.

Parameters			Geometric mean	Geometric stand. dev.
Amplitude [kV]	4.53	0.81	92.29	2.46
Front time [μs]	3.06	1.21	21.27	3.00
Tail time [μs]	5.05	0.17	156.44	1.52

Statistically derived overvoltage parameters can be used to check the severity of the overvoltages that arrive at power transformer terminals. These data incorporate specifics of geographic and electric location such as lightning activity in the area, problems with the grounding system, switching repetition, resonance problems, specific power network configuration, transformer interaction with the network, etc. In general, it can help utilities to choose insulation level specifically for the transformer unit and as an input for transformer manufacturer in order to make a design more persistent for a specific type of overvoltages. In addition, measured severe cases of overvoltage events can be investigated more closely with factors such as frequency domain severity factor (FDSF) [1].

IV. Framework for Overvoltage Management Based on Field Data and Modelling

In this section, the explanation on how the power utilities can benefit from advanced EMTP simulation of overvoltages and from monitoring transients in the system is given. These two approaches are the input for the overvoltage management framework.

Term overvoltage management, at first, considers understanding of the different natures and causes of the overvoltages in the power system. Moreover, based on that knowledge, it considers overvoltage monitoring at critical points in the systems. Final and the most important point and meaning of the term is mitigation of overvoltages using appropriate measures.

Implementation of successful overvoltage management system in the power network can be done through several steps. First, it is necessary to detect critical parts of the network, that consist of specific network configurations, such as connections of long underground cables, connection points of renewable resources, connections of gas insulated switchgear (GIS), etc., or of specific geographical characteristics such as cost line, mountain ranges, rocky terrain, etc. Once the sites are detected, equipment for transient monitoring can be installed at those critical points. Meanwhile, the critical points have to be modelled in detail in EMTP, to be able to simulate overvoltages accurately enough. These simulations should include detailed black box models of power transformers, which consider measurements of frequency dependent admittance matrix.

Both transient measurements and EMTP models can provide input for overvoltage database, where data should be stored with time and geospatial marks. Having the database formed, it is possible to achieve the following: overvoltage map, statistics and sample test impulses, overvoltage mitigation measures and long-term system planning and maintenance input. The scheme of the framework is shown in Figure 5.

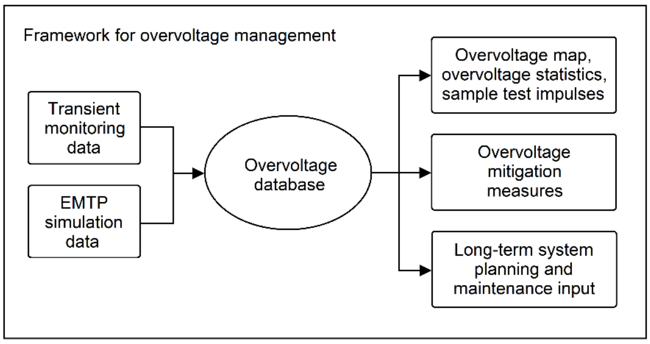

Fig. 5. Framework for overvoltage management.

The outputs defined in the framework are related to overvoltage preview, mitigation and long-term planning and maintenance. Overvoltage preview gives a possibility in having an idea of the overvoltage severity in the network. This can be done using overvoltage maps. While the maps show the data spatially, statistics are used to evaluate the overvoltages at different network locations. At the end, the most severe overvoltage waveforms can be used as sample test impulses. Overvoltage mitigation measures consider actions to limit the overvoltages by changing network configuration, by installing additional surge arresters, by installing snubbers, filters, etc., if the data obtained from the database shows that the overvoltages are higher or more severe than the ones used to test the equipment. Long-term planning input considers more accurate specification of needed insulation levels for the high voltage equipment or going beyond standard insulation level and requiring equipment that is capable of withstanding nonstandard waveshapes, as explained in [18]it is typical that these voltages are characterized by a very high steepness in combination with a short duration time called very fast transients (VFT). Overvoltage severity can be used as an input for asset management and intelligence condition monitoring [19].

V. Conclusion

The paper presents an integral approach to assessing and handling the specific overvoltages in the power network from the view point of the utility. It considers being able to use advanced EMTP models in order to simulate overvoltages that might appear at the transformer terminals. The results of the detailed EMTP simulation of a lightning strike, presented in the paper, showed good agreement with the measured transients in the power network. In addition, an example of the overvoltage statistics data has been shown for the same transformer unit.

In this paper two segments are detected as inputs for framework for overvoltage management: the overvoltage monitoring and the advanced overvoltage simulations in EMTP. Based on the inputs from these two, the one can have a clear picture about the specifics of the overvoltages that exist not only at the terminals of a specific power transformer but also at the particular substations within the possession of a power utility. Both of these segments are nowadays technically within reach of a modern power utility and can therefore be put into implementation.

Based on this approach and the gathered information it is possible to: have an information about overvoltages that exist in the system, provide overvoltage mitigation measures and improve long-term planning and maintenance of the equipment. All of this can lead to better economic planning and fleet management at the power utility level, and also contribute to increasing the reliability of the equipment and reducing its eventual down-time.

References

[1] CIGRE WG A2/C4.39, *Electrical Transient Interaction Between Transformers and the Power Systems*. 2013.

[2] S. Okabe, J. Takami, T. Tsuboi, G. Ueta, A. Ametani, and K. Hidaka, "Discussion on standard waveform in the lightning impulse voltage test," *IEEE Trans. Dielectr. Electr. Insul.*, vol. 20, no. 1, pp. 147–156, 2013.

[3] International Electrotechnical Commission, *IEC 60071-4 Insulation Co-ordination - Part 4: Computational Guide to Insulation Co-ordination and Modelling of Electrical Networks*. 2004.

[4] CIGRE WG A2/C4.39, *Electrical Transient Interaction Between Transformers and the Power Systems*. CIGRE, 2013.

[5] A. Holdyk, B. Gustavsen, I. Arana, J. Holboell, and S. Member, "Wideband Modeling of Power Transformers Using Commercial sFRA Equipment," *IEEE Trans. Power Deliv.*, vol. 29, no. 3, pp. 1–8, 2014.

[6] B. Jurisic, I. Uglesic, A. Xemard, and F. Paladian, "Difficulties in high frequency transformer modeling," *Electr. Power Syst. Res.*, vol. 138, 2016.

[7] Z. Ye, "Pmm: A Matlab Toolbox for Passive Macromodeling in RF/mm-Wave Circuit Design," in *2013 IEEE 10th International Conference on ASIC*, 2013, pp. 1–4.

[8] B. Gustavsen, "Wide Band Modeling of Power Transformers," *IEEE Trans. Power Deliv.*, vol. 19, no. 1, pp. 414–422, 2004.

[9] B. Jurišić, T. Župan, and G. Levačić, "High frequency power transformer model based on on site measurements," in *HRO CIGRE*, 2020.

[10] B. Jurisic, T. Zupan, G. Plisic, B. Filipovic-Grcic, G. Levacic, and A. Xemard, "On Site Measurement and Simulation of Transferred Lightning Overvoltages Through Power Transformers," in *5th International Colloquium "Transformer Research and Asset Management,"* 2019.

[11] B. Filipovic-Grcic, B. Jurisic, S. Keitoue, I. Murat, D. Filipovic-Grcic, and A. Zupan, "Analysis of Overvoltages on Power Transformer Recorded by Transient Overvoltage Monitoring System," in *5th International Colloquium "TRAM,"* 2019.

[12] H. W. Dommel, *EMTP Theory Book*. 1996.

[13] W. Sima, X. Lan, Q. Yang, and T. Yuan, "Statistical analysis on measured lightning overvoltage surges in a 110 kV air-insulated substation," *IET Sci. Meas. Technol.*, vol. 9, no. 1, pp. 28–36, 2015.

[14] B. Jurisic, B. Filipovic-Grcic, T. Zupan, and G. Levacic, "Statistical analysis of non-standard overvoltage waveforms measured at 220 kV terminals of a power transformer," *Electr. Power Syst. Res.*, vol. 197, p. 107318, Aug. 2021.

[15] B. Filipović-Grčić *et al.*, "Monitoring of transient overvoltages on the power transformers and shunt reactors - Field experience in the Croatian power transmission system," *Procedia Eng.*, vol. 202, pp. 29–42, 2017.

[16] T. Župan, B. Jurišić, I. Murat, B. Filipović-Grčić, S. Goglia, and G. Levačić, "Fleet Asset Management Opportunities Arising from Transient Monitoring of Power Transformers and Shunt Reactors," *CIGRE Bien. Sess. Paris, Fr.*, 2020.

[17] International Electrotechnical Commission, *IEC 60060-1 High-Voltage Test Techniques Part 1: General Definitions and Test Requirements*. 2010.

[18] A. Rabel and J.-J. Zhou, "Verification of withstand capability for very fast transients of a 200 MVA, 500 kV GSU transformer by modelling and testing," *e i Elektrotechnik und Informationstechnik*, vol. 137, no. 8, pp. 437–443, Dec. 2020.

[19] C. W. A2.44, *Guide on Transformer Intelligent Condition Monitoring (TIMC) Systems*. 2015.

Journal of Energy

VOLUME 72 Number 1 | 2023

journal homepage: http://journalofenergy.com/

Assessing the Scale of the Radioactive Waste Management Problem: A Review of European Union and International Reporting

Zdenko Šimić

***Summary* — Information on the management of radioactive waste (RW), including inventory, can be obtained from several sources, such as the International Atomic Energy Agency (IAEA) and the European Commission. The IAEA is collecting voluntary national profiles through the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management. The European Commission is requiring reports from Member States in accordance with Council Directive 2011/70/Euratom, which establishes a framework for the safe and responsible management of spent fuel and radioactive waste. The findings from these reports are published by the IAEA and EC every three years and provide comparable information on RW policies, frameworks, and programs, with a significant focus on waste and spent fuel inventories and associated practices and technologies. This paper reviews the latest available reports from the EC and the IAEA, focusing on the RW inventory and disposal status. The paper presents some findings on the overall situation in the European Union (EU) and the comparison of inventories between EU Member States, as well as a comparison with the reporting from the IAEA regarding the global situation. The presentation of the radioactive waste and spent fuel inventories is normalized per person and land area, with the intention of improving understanding of the scale of the RW management problem. The relative scale of the problem is also demonstrated by comparison with hazardous waste inventories. There is a total of 264,000 tons of spent fuel worldwide, equivalent to concentration of 2 g/km² or 0.04 g/capita. The total amount of all categories of radioactive waste is 37.6 million m³, equivalent to 290 l/km² or 5 l/capita. The majority of RW (92%) is very low or low level, and 81% has already been disposed of. In comparison, ten times more hazardous waste is produced worldwide each year (~50 kg/capita/year). These numbers indicate that the amounts of RW are relatively small. The status reports, with a high percentage of RW disposed of, show that RW is routinely manageable, including the management of high-level RW. This is also demonstrated by the fact that Finland is soon to open a permanent disposal site, with several other countries following suit.**

***Keywords* — radioactive waste inventory, waste directive, hazardous waste, disposal**

(Corresponding author: Zdenko Šimić)
Zdenko Šimić is with the Energy Institute Hrvoje Požar (EIHP)
Zagreb, Croatia (e-mails: zdenko.simic@gmail.com)

I. Introduction

Information about the status of radioactive waste management (RWM), including inventory information, can be obtained from various sources such as the International Atomic Energy Agency (IAEA) and the European Commission (EC). The IAEA is compiling voluntary national profiles under the Joint Convention on the Safety of Spent Fuel Management and the Safety of RWM. The EC, on the other hand, is requesting reports from Member States every three years in accordance with the Council Directive 2011/70/Euratom (Waste Directive), which establishes a framework for the responsible and safe management of spent fuel and radioactive waste. Both sources provide comparable status and trends related to radioactive waste policies, frameworks, and programs, with a particular focus on waste and spent fuel inventories and the development of practices and technologies.

This paper reviews the latest available reports from the IAEA and the EC, with a focus on the inventory of radioactive waste and spent fuel and the status of its disposal. The paper presents some findings related to the overall situation in the world and compares the inventory between EU Member States. The presentation of radioactive waste and spent fuel inventories is normalized per capita and per land area, which is not commonly done and aims to improve the understanding of the scale of the RWM problem. Finally, the relative scale of the RWM problem is compared with the inventories of hazardous waste at the global and European Union levels.

The main objective of the Waste Directive is to ensure a high level of safety in the long-term management of radioactive waste and to improve transparency and public participation in the European Union (EU). Member States are legally obligated to report on the implementation of the waste directive and the status of their inventory every three years, which makes it easier to compare national programs and reports as they follow a common format and requirements. The EC reviews the submissions and reports its findings to the Council and the European Parliament. The waste directive covers all sources of radioactivity, including nuclear spent fuel and related inventories. The latest available report from the EC was published in 2019, covering all Member States including the UK.

The IAEA reporting has similar goals, with the main difference being that reporting by Member States is voluntary. The aim is to publish updates every three years, in sync with the reporting cycle of the Joint Convention. The latest report, from 2022, covers the status as of the end of 2016 (the same as for the EU) and covers 83 Contracting Parties, including the EU. This reporting is subject to a peer-review process.

Zdenko Šimić, Assessing the Scale of the Radioactive Waste Management Problem: A Review of European Union and International Reporting, Journal of Energy, vol. 72 Number 1 (2023), 8–13
https://doi.org/10.37798/2023721424

This paper does not cover uncertainties related to inventory and information about radioactive waste generated by military activities. These uncertainties are mainly related to waste categorization and differences during conditioning. Both the IAEA and EC present inventories using the IAEA GSG-1 classification (Very Low Level Waste, Low Level Waste, Intermediate Level Waste, and High Level Waste). Spent fuel is treated separately as some countries are using or considering reprocessing. Naturally occurring radioactive materials (NORM[1]) and disused sealed radioactive sources are not covered in this paper as not all countries consider them separately and they present relatively less significant amounts of radioactivity.

The paper is organized as follows: after the introduction, the next section provides highlights on the status of radioactive waste and spent fuel, including inventories. Section 3 presents normalized inventories of radioactive waste, spent fuel, and hazardous waste. The final section provides some conclusions.

II. Radioactive waste and Spent Fuel Management Status Overview

This paper focuses specifically on the inventories of spent fuel (SF) and radioactive waste (RW). For a more comprehensive understanding of the SF and RW status, the information presented here should be supplemented by the International Atomic Energy Agency (IAEA) status and trend report on SF and RW management [1]. This includes data on the European Union and the specific findings related to the EU have been taken from the European Commission reporting under the Waste Directive and EC staff working documents [2], [3], and [4].

In the first section, the frameworks for SF and RW management are briefly discussed. The second section provides an overview of the established practices and technologies used in the management of SF and RW.

A. Frameworks for spent fuel and radioactive waste management

According to the EU Waste Directive, the Joint Convention, and the IAEA, the primary responsibility for the safety of SF and RW rests with the license holder. However, the state has an obligation to ensure that necessary programs and regulations are in place to manage SF and RW safely. The government establishes a legal and regulatory framework that outlines the roles and responsibilities of all involved parties, including the public.

In most EU and OECD/NEA countries, a clear separation between the regulatory body and the ministry responsible for energy or industry is preferred. National policies should address the responsibilities, financial arrangements, preferred management options (including decommissioning), and public involvement. National strategies are developed to implement these policies by waste management organizations (WMO), which could be state-run or privately-owned (usually by the utility company). The regulatory body or responsible ministry usually approves the strategy.

In most countries with operating nuclear power plants, a dedicated financial system is in place to manage the cost of SF and RW management, including decommissioning. These costs are generally a small contribution to the overall cost of energy production.

Final waste disposal is expected to take place in the country where it is generated, as outlined by the Joint Convention and the Waste Directive. The export and import of SF and RW are prohibited in many states, with exceptions for reprocessing and treatment services. Disused sealed radioactive sources (DSRS) are typically returned to the suppliers.

Early involvement of stakeholders throughout the life cycle of a nuclear facility, including storage and final disposal, is critical. Waste facilities will be in operation for many years and pose potential hazards for hundreds to thousands of years, depending on the category of RW. The Waste Directive provides for necessary public information and participation, and various international conventions also cover stakeholders' involvement, such as the Aarhus Convention (access to information, decision-making participation, and environmental justice) and the Espoo Convention (transboundary environmental impact).

B. Developed practices and technologies

Radioactive waste management encompasses the entire life cycle, including facility operation, RW generation, characterization, treatment, storage, and final disposal. The management of RW involves reduction from primary, secondary, and recycling sources. The potential for recycling and reuse is limited on a national level. Final disposal is defined as the intentional placement with passive engineered and natural isolation, without the intention of retrieval (although this may vary in some countries). The management of SF and RW is highly regulated and internationally accepted safe technical solutions have been developed.

SF is mostly kept in wet or dry storage until a final solution is found, which may be reprocessing or direct disposal. Currently, only a few countries[2], such as France, Japan, and Russia, are reprocessing SF. Some countries utilize SF reprocessing services, while China operates a pilot reprocessing plant. Reprocessing of SF results in high-level waste (HLW), typically in the form of a vitrified material, which is ready for final disposal. In both cases, final disposal is planned in a similar manner as for long-lived intermediate-level waste (ILW) and HLW, in deep geological repositories. In some countries, there may be plans for possible retrieval.

New storage facilities for SF are being built farther from reactors and may even be located outside of the plant boundaries. For longer storage, different types of dry solutions are becoming increasingly popular. The canisters of HLW after reprocessing are stored in air-cooled vaults or casks, similar to those used for SF.

Finland is the first country to reach the stage of operating license submission for a deep geological repository (DGR) located 400 meters or deeper and is expected to start accepting SF in a few years. Several other countries, including France, the UK, Canada, and Germany, are in various licensing stages for their DGRs. Sweden has recently issued a construction license for their geologic disposal repository. There are approximately 20 underground research laboratories in use for SF and HLW DGRs, such as HADES in Belgium, KURT in South Korea, and Krasnoyarsk in Russia.

Intermediate-level waste (ILW) often contains large amounts of long-lived radionuclides and requires shielding during handling and deeper disposal locations. Treatment and conditioning processes, such as separation, volume reduction, and stabilization prior to packaging, are carried out to ensure safety. This may include drying, evaporation, high compaction, melting, and cementing. ILW is packaged in concrete containers with steel reinforcement, steel boxes, or drums and can be stored for up to 100 years before final disposal. Final disposal is typically done in DGRs located about 100 meters below the surface and is considered safe. The Wa-

[1] E.g.: extraction of fossil fuels and rare earths, phosphate sector, titanium production, geothermal energy.

[2] The commercial capacity for SF reprocessing was (at the end of 2016) 44000 t HM/a. However, in the meantime UK THORP and Magnox reprocessing capacities (900 and 1500 t HM/a) are permanently closed.

ste Isolation Pilot Plant in the USA is a licensed disposal facility for ILW. Some countries, such as Germany, Switzerland, and France, are planning to dispose of ILW together with HLW in DGRs.

Low-level waste (LLW) shares many similarities with ILW regarding treatment and storage. Incineration is an important part of the compacting process for LLW. Low-level waste is typically stored for a longer period before final disposal is available. The main difference between LLW and ILW is that LLW has a lower radioactivity level and a much larger volume. Most LLW radionuclides have a half-life of less than 30 years. Many countries have been disposing of large volumes of LLW in near-surface repositories or in caverns below ground level for several decades. Engineered barriers prevent water infiltration and intrusion, and surveillance is planned for a few hundred years. Some countries are considering disposing of LLW at deeper locations or collocating it with ILW, which could be more complex due to the higher volume and additional requirements.

Very low-level waste (VLLW) is mainly generated from decommissioning activities and consists of concrete, soil, and rubble. Only a few countries, such as France, Japan, Lithuania, Spain, and Sweden, treat VLLW separately. Little processing is done for VLLW, except for packaging and potential separation for clearance. A simpler shelter or temporary cover is sufficient for VLLW storage. Final disposal is usually done in shallow trenches or above-ground designs with a concrete slab. Some countries dispose of VLLW together with other LLW or non-nuclear hazard waste.

There has been significant progress in the disposal of low-level and very low-level waste, with disposed volumes much higher than stored volumes. The most important considerations for these types of waste are long-term knowledge management and preservation, transparency, and stakeholder involvement. Active international cooperation, research, and development are crucial for ensuring technology and experience progress in this field.

C. SF and RW Inventories

The classification of RW, as previously mentioned, varies in different countries, and the calculation of the total amount, for the EU and world, requires conversion based on the information provided by the countries or with some assumptions. This adds some degree of uncertainty. The global data presented in this report is at an improved level of aggregation compared to the previous IAEA status report. More detailed information can be found at the country level in references [1] to [4].

Table 1 provides the cumulative amounts of SF in wet and dry storage across various regions of the world, including reprocessing, in terms of 1000 metric tons of heavy metals (HM). Table 2 presents the cumulative amounts of RW for all categories in 1000 cubic meters. The table also provides the share of RW that has already been disposed of. Values for EU Member States are presented both in the European region and separately.

Due to the much smaller quantities, SF from research reactors is not presented in detail. Similarly, DSRSs are also not covered here because some countries classify them together with their respective RW categories. In many countries, DSRSs are the primary or only type of RW.

Globally, there are 390000 metric tons of HM of SF (43% of which is in the EU), including reprocessed material (which makes up one third of the total, and 68% of which is in the EU).

In terms of volume, globally there is only 0.13% of HLW, 7.7% of ILW, while the majority is LLW (53%) and VLLW (39%). These numbers are similar in the EU, with a larger difference in the share between the two largest categories: 0.2%, 9.7%, 72%, and 18%, respectively. When expressed by radioactivity, VLLW and LLW together make up less than 2% worldwide.

Globally, more than 80% of RW, by volume, has already been disposed of (more than 70% in the EU). However, only a small fraction of ILW (5% globally, and 4% in the EU) and none of the HLW has been disposed of as of the end of 2016. As previously mentioned, the first disposal of SF will start in Finland after the operating license is issued (the regulatory review started in May 2022 and may take several years).

Table I

Reported Spent Fuel from Nuclear Power Plants (1000 t HM, end of 2016), [1]

REGION, SF 1000 t HM	Wet storage	Dry storage	Reprocessed	Total
Africa	1.0	0.05	-	**1.0**
Americas	83.5	52.5	0.6	**136.5**
Asia	35.5	6.5	8.5	**51.0**
Europe	63.5	20.5	117.5	**201.5**
Oceania	1 t	-	1 t	**1 t**
WORLD TOTAL	**183.5**	**80.0**	**127.0**	**390.0**
EU Member States	42.0	11.0	113.0	**166.0**
HM - Heavy Metal				

Table II

Reported Solid Radioactive Waste (1000 m3, end of 2016), [1]

REGION	VL LW		L LW		I LW		H LW
1000 m³	Total	Dis-posed	Total	Dis-posed	Total	Dis-posed	Total
Africa	14	0%	39	36%	1	0%	0
Americas	13350	83%	15695	98%	176	53%	6
Asia	351	0.2%	316	21%	69	0%	6
Europe	614	60%	3892	77%	2626	2%	17
Oceania	432	100%	28	86%	0	-	0
WORLD TOTAL	**14761**	**80%**	**19970**	**93%**	**2872**	**5%**	**29**
EU Member States	614	60%	2493	84%	333	4%	6
VL - Very Low; L - Low; I - Intermediate; H - High; LW - Level Waste							

The volume of RW continues to rise with the operation of nuclear power plants, at a rate of approximately 2% per year. However, comparison with previous years is challenging due to changes in RW classification reporting. The amount of RW generated also depends on the technologies used for processing, storage, and disposal. With the increasing number of reactors set to be decommissioned, larger quantities of LLLW and LLW are expected to be generated in the future. Currently, fewer than 20 reactors have been decommissioned globally. At the end of 2016, 123 reactors were in the decommissioning process, and a significant number of reactors are expected to be decommissioned in the future as more than 140 operating reactors are over 40 years old (which is typically the extended operating time for reactors).

As of the end of 2016, there were 448 reactors in operation (with a combined capacity of 391 GWe) in 30 countries. In the EU, 14 Member States have nuclear power plants in operation (119 GWe in 126 reactors), and along with Italy and Lithuania (which have terminated their nuclear programs), they account for 99.7% of the RW volume. Three reactors have been decommissioned and 90 have been shut down. There are 82 research reactors (including those in decommissioning) in the 19 Member States.

III. Radioactive and nonradioactive hazardous waste concentration comparison

A comparison between radioactive waste (RW) and nonradioactive hazardous waste (HW) such as toxic, corrosive, biological, explosive, and flammable, can improve both the management and perception of related problems. This comparison could include regulations, trade, toxicity, presence in the environment, and longevity. This paper begins this complex comparison by focusing on the quantities of RW and HW. The comparison is done by calculating concentration as the amount of waste per capita and per land area ([7, 8, 9, 10]). The calculations are first made for RW using global and regional data and country data (for EU Member States). Then, global HW and EU MS data are used to calculate the concentrations per capita.

Globally, approximately 400 million tons of HW are produced annually (the total amount of all waste is estimated to be about 20 times larger) [5]. The trade of HW between countries is growing and is estimated to be about 40 million tons per year.

Figures 1 and 2 show the quantities of RW and HW per land area (left side) and per capita (right side) for different regions in the world. It is evident that so far, the accumulated quantities of RW are equal to about 10 liters per person and less than 1 m³ per square kilometer of land area (for example, 6.7 l/capita and 0.78 m³/km² for the EU). Similarly, the accumulated quantities of SF are equivalent to a fraction of a gram per person and several grams per square kilometer of land area (for example, 0.1 g/capita and 12 g/km² for the EU).

Figures 3 and 4 show the density in the EU MSs for RW and SF respectively (per land area on the left side and per capita on the right side). The graph for SF data shows MSs with a nuclear program, including two former nuclear MSs (Italy and Lithuania) and Croatia (which shares a nuclear power plant with Slovenia and will soon take over half of the RW from the 40 years of operation of the NPP Krško). The graph for RW shows all MSs.

The accumulated amounts of SF are less than 30 grams per person and less than 25 kilograms per square kilometer of land area (excluding non-nuclear MSs). Correspondingly, the accumulated amounts of RW are less than 5 liters per person and much less than 2 m³ per square kilometer of land area (for example, 0.3 l/capita and 0.02 m³/km² for Croatia).

To illustrate the small concentration of RW it might be interesting to estimate the quantities of SF and RW per person in a hypothetical scenario where only nuclear power is used to generate electricity for a person's lifetime. This evaluation is dependent on many assumptions, and for an approximate estimate, it seems reasonable to judge based on the data presented for EU MSs that the burden would be approximately 1 kg of SF and about 30 liters of RW (including about 3 l of ILW and half a liter of HLW) per capita.

Based on the global amounts of nonradioactive hazardous waste, it can be estimated that approximately 50 kilograms are produced per person annually. Detailed data for world regions are not easily available. Country statistics about HW for the EU MSs are available. Figure 5 shows the quantities of HW treated in EU MSs in kilograms per person every year. About half of the MSs have quantities comparable to the global average. However, eight MSs have quantities greater than 200 kg/capita/year.

These data show that the amounts of HW generated per person every year are about 10 times larger than the cumulative amounts of RW generated since the beginning of the use of nuclear power (during more than 50 years).

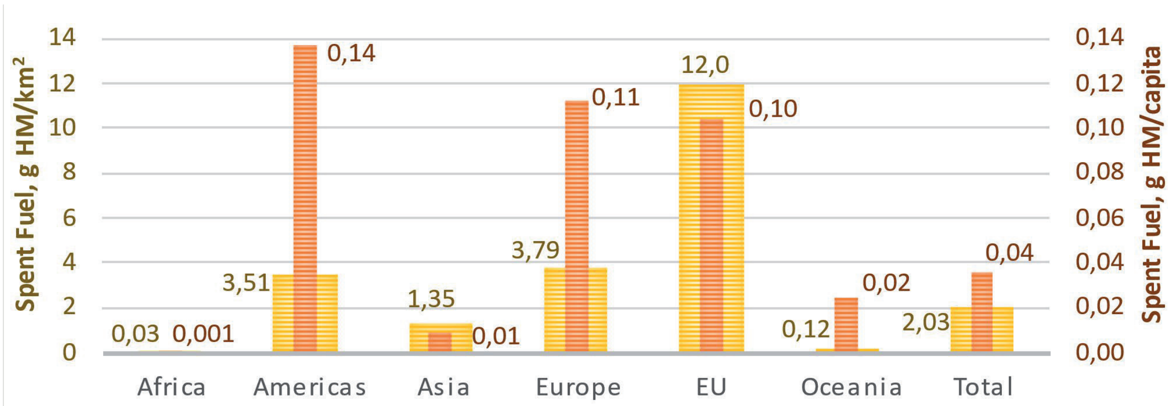

Fig. 1. Accumulated Concentration of Spent Fuel for World Regions: kg HM/capita and g HM/km², [1] (HM – Heavy Metal)

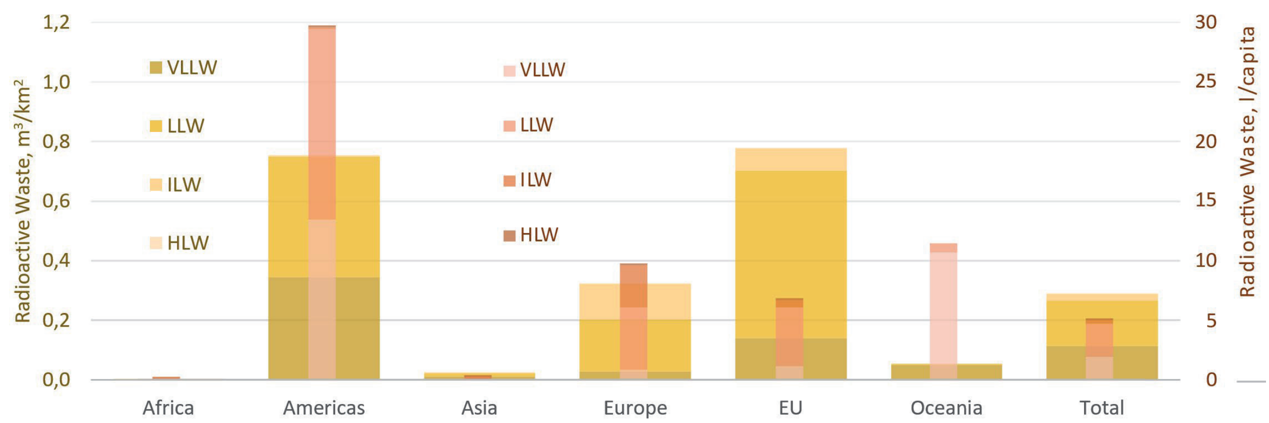

Fig. 2. Accumulated Radioactive Waste Concentration for World Regions: m³/km² (wide bars) and l/capita (narrow bars), [1]

Zdenko Šimić, Assessing the Scale of the Radioactive Waste Management Problem: A Review of European Union and International Reporting, Journal of Energy, vol. 72 Number 1 (2023), 8–13
https://doi.org/10.37798/2023721424

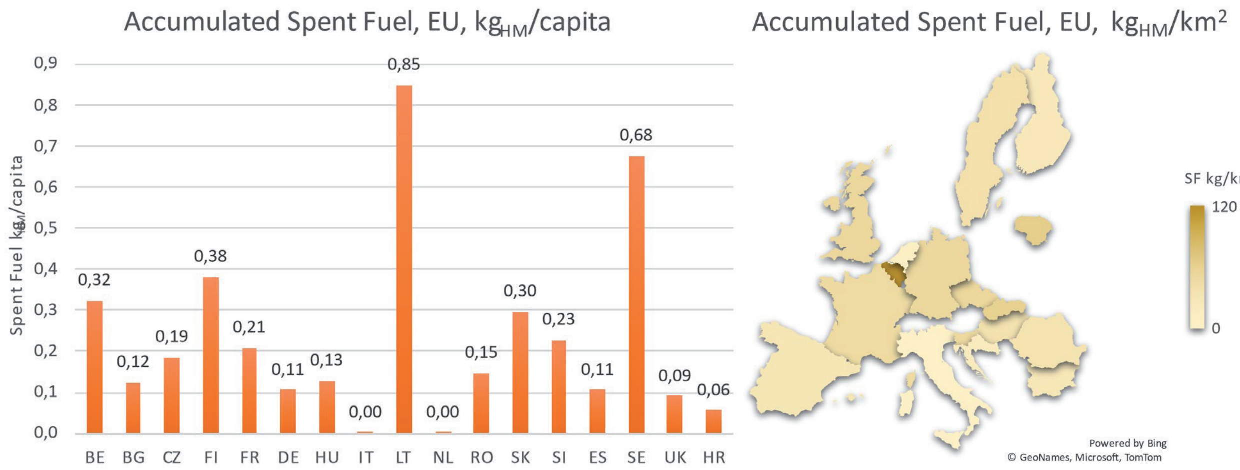

Fig. 3. Accumulated Spent Fuel Concentration in the European Union: kg HM/capita (MSs with nuclear program) and kg HM/km² (HM – Heavy Metal. Data for HR include share from the SI.), [4]

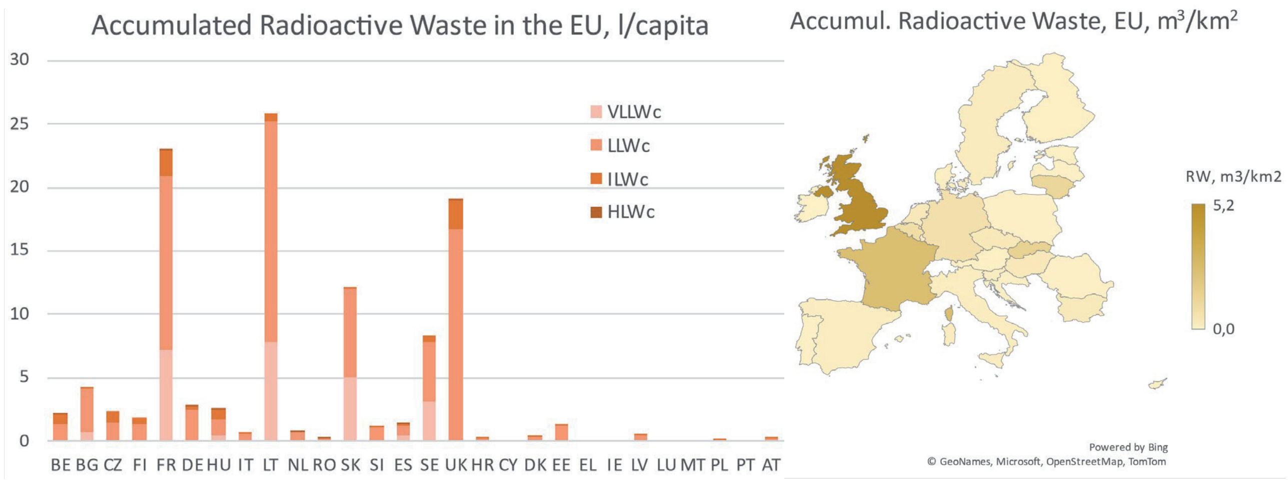

Fig. 4. Accumulated Radioactive Waste Concentration in the European Union: l/capita and m³/km² (All MSs. Data for HR include share from the SI.), [4]

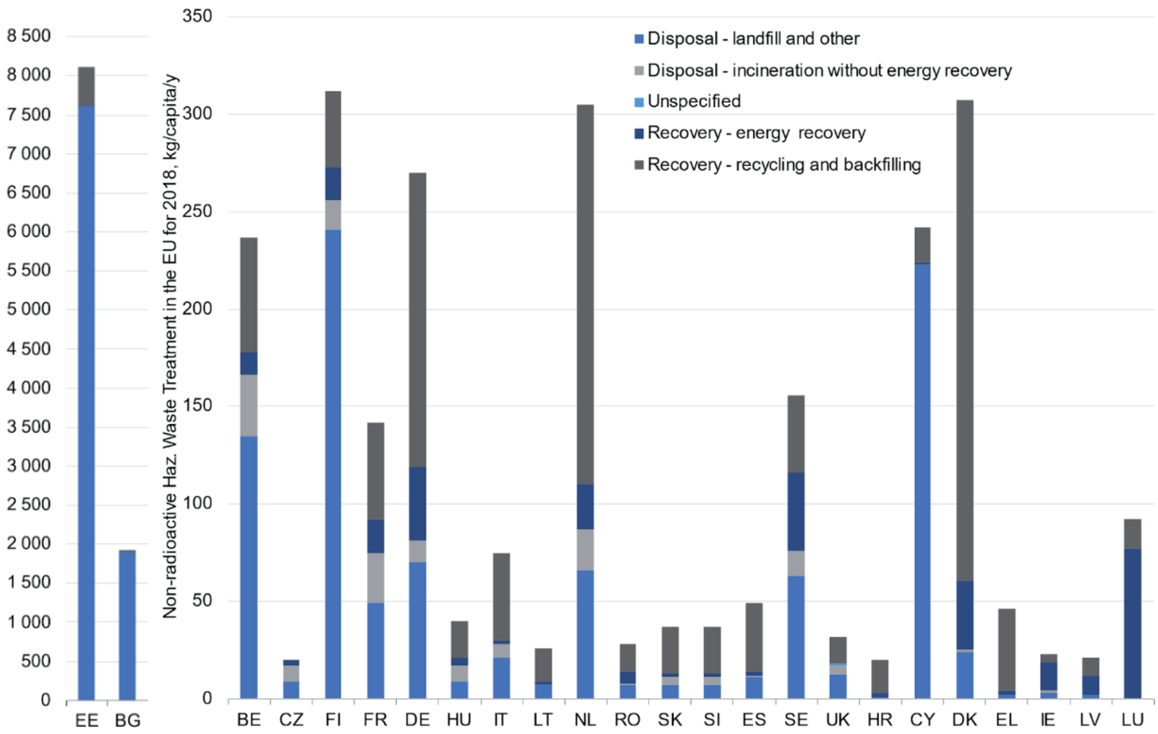

Fig. 5. Non-radioactive Hazardous Waste Treatment in the European Union for 2018: kg/capita/y
(EU28 average 184 kg/capita/y. MSs ordered like in the figure for RW. Source: Eurostat, data code env_wastr. Notice different scale for EE and BG on left because of much larger volumes.) [6]

IV. Conclusion

This paper has analyzed selected data on the management of spent fuel (SF) and radioactive waste (RW) at the global and EU levels. Information was gathered from two recent sources: the IAEA Status Report and EU Progress Reports on the Implementation of the Waste Directive. The paper briefly outlines the frameworks, practices, and technologies developed for SF and RW management. It also focuses on the inventory of SF and RW in various regions of the world, including information on the reprocessing of SF, storage methods, and final disposal.

A comparison of the normalized amounts of SF and RW, per capita and per land area, has been made between world regions and EU Member States. The paper also presents an analysis of the density of nonradioactive hazardous waste (HW) at a global and EU level.

The majority of RW has already been disposed of (80% globally and 70% in the EU), however, this only applies to low-level and intermediate-level waste categories. High-level waste and SF have yet to be disposed of (or reprocessed) in any country. Finland is the first country with a deep geological repository for high-level waste and SF, which is currently under regulatory review for an operating license.

The data and normalization show that the cumulative amounts of SF and RW are both absolutely and relatively small and significantly smaller in comparison to the amounts of HW managed annually. The average HW treated yearly per capita, in nuclear EU Member States, is more than 200 kilograms, which is 40 times larger than the average accumulated RW from the beginning of nuclear power use.

RW management is subject to stricter regulations (such as export restrictions) and is certainly more controversial than the management of HW. The amount of HW traded between countries is larger than the total amount of accumulated RW (~40 million/year vs ~38 million tons total, assuming 1 $m^3 \approx$ 1 ton). The transport of RW and SF between countries is rare and primarily related to treatment and reprocessing, with the resulting radioactive waste being returned to the originating country.

Future work could include a more detailed comparison of HW and RW in terms of regulatory oversight and public risk. This could be useful in assessing the cost of waste management in comparison to risk and in potentially improving management including better informing and engaging stakeholders.

Funding

This research was funded by the European Commission, European Structural and Investments Funds 2014–2020, grant number KK.01.1.1.07.0038, by the research project of the Energy Institute Hrvoje Požar, “Development of an integrated solution for strategic long-term climate and energy policy planning and development of joint climate and energy plans”.

References

[1] International Atomic Energy Agency, Status and Trends in Spent Fuel and Radioactive Waste Management, IAEA Nuclear Energy Series No. NW-T-1.14 (Rev. 1), IAEA, Vienna (2022). www.iaea.org/publications/14739/status-and-trends-in-sfuel-and-radioactive-waste-management

[2] Report from The Commission to The Council and The European Parliament on progress of implementation of Council Directive 2011/70/EURATOM and an inventory of radioactive waste and spent fuel present in the Community’s territory and the future prospects, COM(2019) 632. eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2019:0632:FIN

[3] Commission Staff Working Document, Inventory of radioactive waste and spent fuel present in the Community’s territory and the future prospects, SWD(2019) 435, Accompanying the docu-ment COM(2019) 632. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019SC0435

[4] Commission Staff Working Document, Progress of implementation of Council Directive 2011/70/EURATOM, SWD(2019) 436, Accompanying the document COM(2019) 632. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019SC0436,

[5] Martínez, J.H., Romero, S., Ramasco, J.J. et al. The world-wide waste web. *Nat Commun 13*, 1615 (2022). doi.org/10.1038/s41467-022-28810-x

[6] EuroStat, Waste statistics, Hazardous waste generation 2018, ec.europa.eu/eurostat/statistics-explained/index.php?title=Waste_statistics#Hazardous_waste_generation, Accessed 5.5.2022.

[7] World population by regions: Our World in Data, Historical and projected population: ourworldindata.org/grapher/historical-and-projected-population-by-region, Accessed 5.5.2022.

[8] European Union population, Eurostat, Population and employment (data code: NAMQ_10_PE): ec.europa.eu/eurostat/databrowser/view/namq_10_pe/default/table, Accessed 5.5.2022.

[9] Regions in the world by population and area, World meter: www.worldometers.info/world-population/population-by-region/, Accessed 5.5.2022.

[10] European Union Member states population and area: en.wikipedia.org/wiki/Member_state_of_the_European_Union, Accessed 5.5.2022.

Journal of Energy

VOLUME 72 Number 1 | 2023

journal homepage: http://journalofenergy.com/

Application of fully automated centralized voltage regulation in transmission system operation management

Renata Rubeša, Marko Rekić, Zoran Bunčec, Tomislav Stupić

Summary **— The influence of wind farms, inclusion of distributed energy and the energy market has a large impact on the voltage profile in a transmission system. The Croatian Transmission System Operator HOPS has implemented VVC (Volt Var Control) system which was one of the subprojects included in the EU co-founded Sincro. Grid smart grid project that was financed by the EU CEF fund. The main goal of the project is to raise voltage quality in the transmission network. VVC system is an optimal power flow-based application which calculates the optimal solution regarding the desired objective function, available control variables and a defined set of constraints. To achieve the calculated optimal power system state, control of field devices is included in the process of optimization by shifting tap changer positions or changing setpoint values of reactive power injection. Voltage and reactive power constraints are set accordingly to available regulating devices included in the optimization. The lack of automatic coordination of reactive power resources motivated this work for implementing an advanced VVC for real time control of reactive power in partially automatic and fully automatic (closed loop) mode using the optimal power flow (OPF) algorithm. Due to its complexity, the closed loop approach of reactive power regulation is rarely used in the TSO community and the HOPS is one of the first TSOs that implemented regulation in such manner. Except fully automatic mode of operation, VVC can be used in semi-auto or manual mode. For a successful implementation several safety algorithms are implement to avoid many unwanted situations in the power system such as voltage breakdown, overloading of regulating equipment and similar.**

Keywords **— Volt Var Control – Optimization - Transmission Network - Optimal Power Flow - Voltage Profile**

I. Introduction

Transmission System Operators are responsible for the security of operation, facilitation of regional markets and integration of renewable energy sources (RES). Thus, development of grid infrastructure, supporting technologies and mechanisms are key elements for proper and timely integration of RES. In recent years, the Croatian power system has been increasingly challenged by contradictory influences impacting the operation of the power systems:

(Corresponding author: Tomislav Stupić)

Renata Rubeša, Zoran Bunčec and Marko Rekić are with the Croatian Transmission System Operator (HOPS)

Zagreb, Croatia (e-mails: renata.rubesa@hops.hr, zoran.buncec@hops.hr, marko.rekic@hops.hr)

Tomislav Stupić is with the Končar – Engineering Co., Zagreb, Croatia (e-mail: tomislav.stupic@koncar-ket.hr)

- Support of RES integration to meet the EU targets,
- A lower electricity consumption due to the economic crisis,
- A growing lack of centralized electricity production for electric system support,
- The high interconnectivity between the neighboring control zones.

Consequently, the Croatian transmission System Operator HOPS observes growing issues in keeping the voltage profile of the transmission network inside the prescribed limits. This issue has been addressed by implementing a power system voltage and reactive power regulation scheme on a national level which would allow more RES generation to be connected to the transmission and distribution power systems. Power system voltage and reactive power regulation schemes can be generally classified as hierarchical or as centralized voltage regulation systems. Ways of implementing these two regulation systems vary greatly from one TSO to another [1]. Hierarchical regulation rests on implementation of three temporally and spatially separated control levels: primary, secondary, and tertiary control [2]. Primary voltage regulation automatically implies response of local voltage regulators, primarily synchronous generators and onload tap changers in substations. Secondary regulation refers to voltage regulation within a defined zone, while tertiary regulation is carried out on regional or national level. The problem is usually seen as a static problem, whose solution is identical to an open-loop optimization base volt/var management [3]. In HOPS the implemented voltage and reactive power regulation scheme, referred to as tertiary control on a national level and is based on an optimal power flow (OPF) type algorithm. Addressing the issue of implementing such a complex system in a closed loop operation in a TSO led to several open questions:

- The definition of voltage optimality accompanied with regional contributions for a system wide performance criterion.
- Improvement of voltage profile in particular regions experiencing shortage of voltage support [3].
- Voltage profile and stability is mainly a local issue, but some of major large network disturbances and blackouts were caused by voltage stability issues. Apply the automatic operation of the voltage and reactive power regulation scheme ensuring safe and reliable network operation.

This paper will elaborate on these questions and how they were practically solved in HOPS in scope of Sincro.Grid VVC project.

Renata Rubeša, Marko Rekić, Zoran Bunčec, Tomislav Stupić, Application of fully automated centralized voltage regulation in transmission system operation management, Journal of Energy, vol. 72 Number 1 (2023), 14–19
https://doi.org/10.37798/2023721465

II. Volt Var Control System Design

A. Primary and tertiary regulation scheme

Most transformers (220/110 kV and 400/110 kV transformers) are equipped with an onload tap changer (OLTC) that can change the ratio of the transformation in operation and thus control the voltage on the regulated side of the transformer. Local voltage regulators on transformers typically regulate the lower voltage side of transformers.

Unlike local voltage regulators, the central Volt and Var Control (VVC) system has insight into the entire network and the ability to manage voltages throughout the power network. The calculation of the optimal power flows of the central optimizer is defined by the objective function and the set voltage limits. The objective function of the VVC system is set to minimize the operating losses in the system [4]. The basic algorithm of the VVC function is the optimization algorithm of the OPF function based on the interior point method. The execution of the VVC output (is executed by the SCADA/EMS system installed in HOPS. The ability to manage voltages in the power network largely depends on the available objects in the optimization. In the case of VVC systems in HOPS, it is possible to control a total of 28 power transformers and 2 variable shunt reactors (facilities owned by TSO) to which VVC system can issue control orders (with or without the intervention of the dispatcher\operator). Also, 11 production units (5 generators in Hydro Power Plants, 3 generators in Thermal Power Plants and 4 generators in Wind Power Plants) are included in the optimization calculation. For the VVC calculation to be successful and the control orders ready to be issued to the facilities, the optimal results of all voltage values must be within the defined limits. Therefore, it is very important, depending on the involvement of objects in the optimization, to define voltage limits for individual nodes and analyze the voltage sensitivity of individual objects included in the optimization to avoid large movement of individual objects in optimization.

Table I

Comparison of local voltage regulators and central voltage and reactive power regulation scheme

	Local voltage regulation	VVC system
Voltage Control	Voltage control only on the regulated bus	Voltage control of the entire network
Regulated bus	Only one regulated bus	All the buses in the network with respect to voltage limits
Regulation mode	Automatic maintenance of the selected voltage setpoint value only on the control bus	VVC calculation based on available devices in optimization while meeting the objective function to reduce losses. After the calculation, the set-points can be sent with the approval of the operator\dispatcher or automatically without the confirmation of the operator\dispatcher
Loss optimization	Not implemented	Supported, there is insight into voltage conditions throughout the network. After calculating the optimal power flows, the calculation of the difference in losses before and after optimization is visible.
Device control	Controls only the OLTC on one object (in case of parallel operation of transformers, mutual communication of regulators on parallel transformers is possible)	Manages selected objects that participate in optimization and have the ability to manage from the VVC system

B. VVC system design

The VVC system consists of the transmission network model, modelled in the accurate AC manner. The model is imported via the Common Information Model (CIM) standard from the production SCADA/EMS system. The real time measurements and breaker status are imported via IEC 61870-5-104 protocol cyclically with a time interval of one minute [6]. The VVC system runs a state estimation process, and the results are the base case for the OPF process. OPF results (setpoints of control variables) are transferred back from the VVC system to the production SCADA/EMS system via ICCP protocol and dispatched to field devices. The system presented on Figure 1 can be run in semi-automatic mode (the dispatcher sends the controls manually to field devices from the SCADA/EMS system) or in the automatic i.e., closed loop control mode where no dispatcher intervention is needed, and the set points are automatically sent to field devices after each OPF execution. In closed loop control mode, the OPF function can be executed every 15, 30 or 60 minutes.

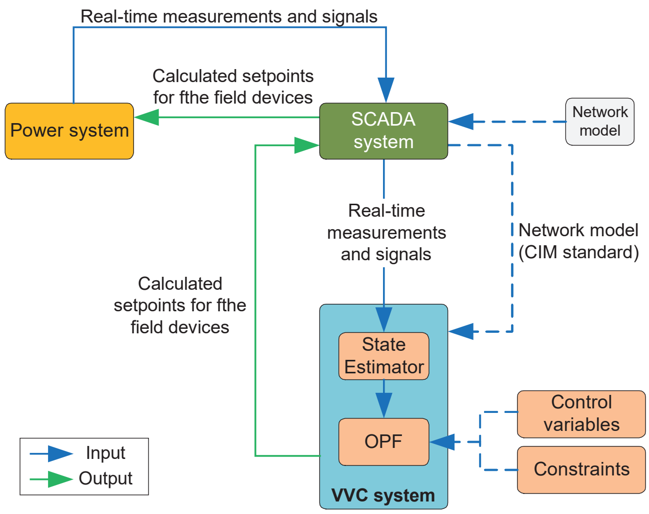

Fig. 1. VVC system design

C. Voltage constraints

Initial voltage low an upper limits or constraints for the 400, 220 and 110 kV voltage levels are defined to be compliant to the COMMISSION REGULATION (EU) 2017/1485 SOGL (System Operation Guidelines) documents and Network Codes. The values of these constraints are defined in Table II. VVC has more rigorous voltage limit compared to the limits from the Network Codes. This provides a safer voltage band within the voltage and can fluctuate due to changes in the network (such as the change of the topology) between two consecutive optimization cycles or runs.

Table II

Voltage constraints in the VVC system

Voltage level [kV]	Lower limit in VVC [kV]	Upper limit in VVC [kV]	SOGL limits [kV]
110	105	122	99 - 123
220	210	244	198 - 246
400	390	418	360 - 420

Figure 2 bellow shows the graphical representation of 220 kV node voltages in one region of the transmission network, during a 4-day time span when VVC performed the optimization cycles (left side) and the equally long period without reactive power optimization (right side). In the period without optimization (right side) of the figure only local (primary) voltage regulation was active.

Renata Rubeša, Marko Rekić, Zoran Bunčec, Tomislav Stupić, Application of fully automated centralized voltage regulation in transmission system operation management, Journal of Energy, vol. 72 Number 1 (2023), 14–19
https://doi.org/10.37798/2023721465

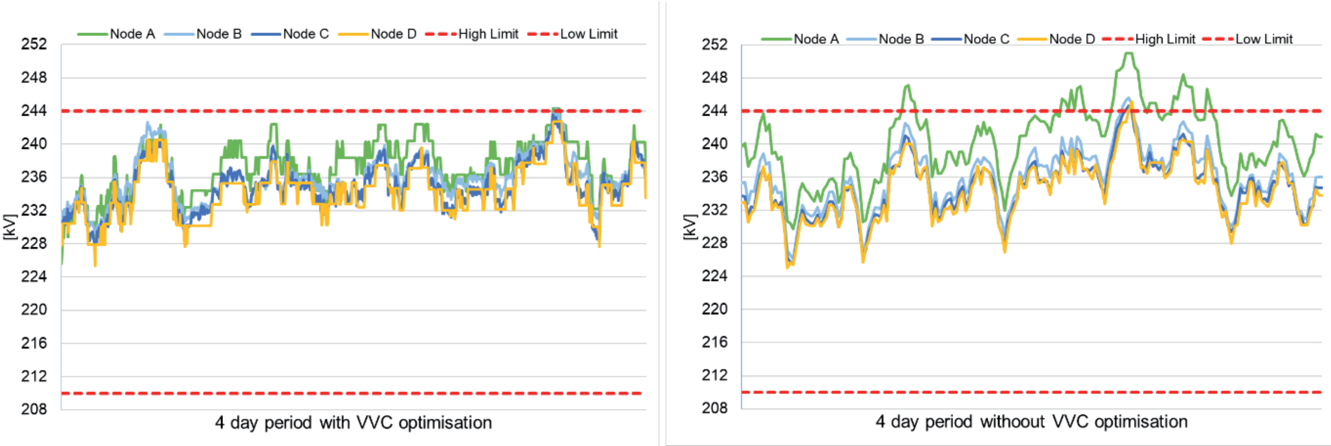

Fig. 2. Node voltages in 4-day period with optimization (the left side) and without optimization (the right side)

It can be clearly seen that during the VVC optimization cycles, node voltage magnitudes were all the time within defined limits, unlike the period when the VVC was not in the operation and the node voltage was outside defined limits. The VVC system keeps the node voltage magnitudes close to the high limit value, which is also a confirmation that the VVC performs a defined objective function to reduce MW losses. By increasing voltage level, the amount of current flow through network elements is consequently reduced, which leads to a consequent reduction of active power losses.

As mentioned before, the VVC algorithm tries to reduce active power losses by keeping voltages close to the high voltage limit, so during the testing, VVC raised node voltages in the system when that was feasible and consequently reduced the active power losses in the system.

Figure 3 shows a radar diagram of 220 kV and 400 kV node voltages in the power network before the implementation of VVC optimal setpoints and the same node voltages after the implementation of the VVC optimal setpoints. A heat map of network before and after the optimization cycle is also given for the same example in Figure 4.

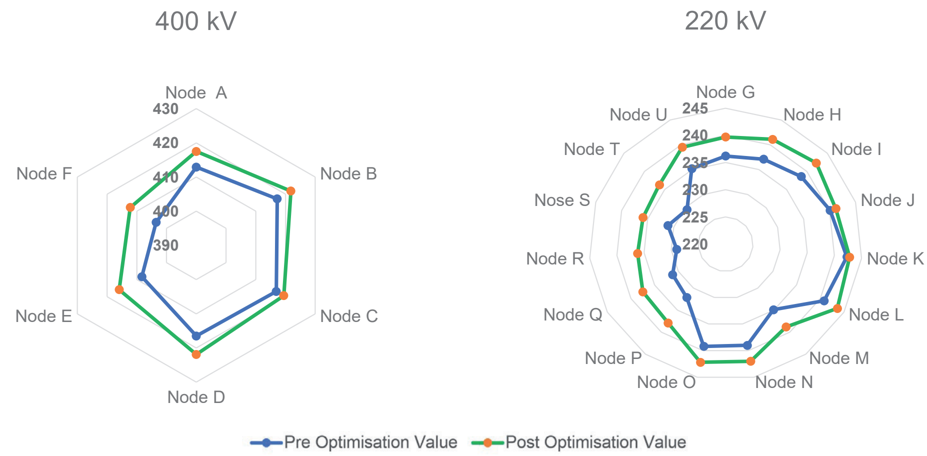

Fig. 3. Radar diagram of pre and post optimization voltages

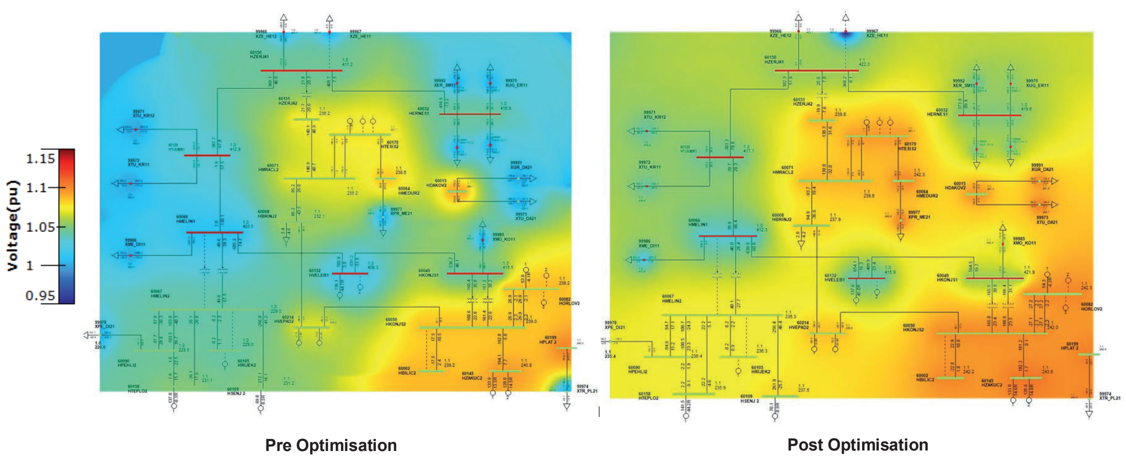

Fig. 4. The heat map of node voltages before and after performing the optimization

Renata Rubeša, Marko Rekić, Zoran Bunčec, Tomislav Stupić, Application of fully automated centralized voltage regulation in transmission system operation management, Journal of Energy, vol. 72 Number 1 (2023), 14–19
https://doi.org/10.37798/2023721465

The graphs above show that VVC increased the voltages in the part of the network where it was possible and thus equalized the voltage profile in the transmission network, which can be seen from the radar diagram. The radar diagram of the optimal power network condition has a rounder shape as well as more uniform contours on the heat map after performing the optimization cycle.

However, for some nodes, specific, softened constrains had to be applied. This had to due to the fact that particular power network regions experience shortage of voltage support, i.e., the optimization solution violates constraints that have no controls electrically sensitive to them. In this case the solution is infeasible, or if the controls are marginally sensitive, the solution suggest to enforce large, uneconomical control shifts from their original value. In HOPS this issue is overcome with two solutions:

- Prior the optimization process (OPF) perform a **sensitivity analysis** in order to determine the range of influence of control variables to voltage magnitude. The sensitivity analysis provided a list of insensitive nodes to changes in control variables and divided the transmission network into control zones. The result of the sensitivity analysis divided the HOPS power network into 8 optimization zones shown in Figure 5.

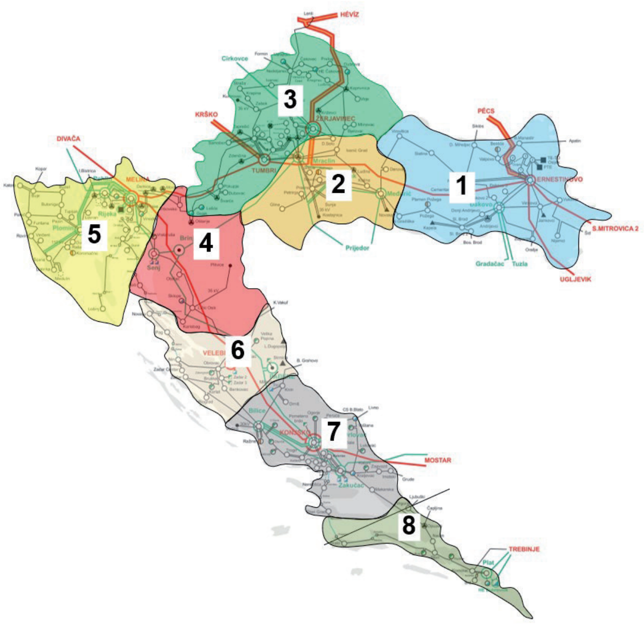

Fig. 5. Croatian transmission network and division in to 8 optimization zones

All the zones participate in the OPF problem simultaneously, but the operator\dispatcher has the possibility to exclude zones from the calculation if the zone has insufficient compensation resources.

- After the OPF calculation, check the number of individual control variables shifts and automatically block sending set point values to field devices in case the calculated optimal set points of control variables have large deviations compared to base case positions. This situation will trigger an alarm and such setpoints will not be sent automatically. Setpoints can be send in semi-auto operation mode after the operator\dispatcher confirmation. The amount of deviation is set as a parameter by the operator\dispatcher (for example 3 control shift deviation for transformer and VSR tap position and 15 MVAr for reactive power production for production units).

This two-step approach limits the engagement of control variables prior and after the optimization process to preserve the primary equipment to undergo uneconomic shifts which have no or minimal positive impact on the voltage profile.

III. VVC Security Mechanisms

Implementing such a complex system in a transmission system, implies the need to constantly monitor the entire process consisting of receiving measurements, signals and indications from the network, availability indications form devices included in the optimization, control of the OPF calculation and configuration, display and verification of result, sequencing, and coordination of commands. A set of automatic security controls had to be implemented to prevent sending of unfeasible or unreliable set points to filed devices without operator\dispatcher intervention. In case any of the below security mechanisms activates an alarm is triggered an the VVC execution is automatically stopped.

A. State estimation quality

The state estimator is the base case solution for the OPF algorithm. The state estimator gives the most likely state of the network which will be further used in power flow and OPF calculations for the purpose of calculating optimal set points. The performance of the state estimator calculation is evaluated by the state estimation quality index. If the state estimation quality index is below a user defined threshold, the VVC function will not start so the possibility of poor quality OPF calculation will be avoided.

B. Control of OPF calculation quality

In order for the solution of the OPF function to be sent to field devices, the OPF solution must be calculated within the defined error tolerance otherwise it will not be possible to send set points. This security mechanisms monitors the difference between the calculated pre and post optimization losses which must be within a predefined amount.

C. Emergency stop

One of the main functions for the secure operation of the VVC system is the emergency stop function. The function enables operator\dispatcher to immediately stop the sequence of commands issued to field devices in case of undesirable situation with the execution of the set points or there is a large disturbance in the network. The execution of the optimization cycle can be stopped in a particular transmission network region by dispatcher\operator in Regional control center (RCC) or by dispatcher in National control center (NCC) for particular or entire network. The emergency stop function for transformers and variable shunt reactors will automatically stop the process shifting the tap changer position while for the power plants it automatically sends a set point for power factor = 1 to generators included in the optimization.

D. Monitoring of the devices included in the optimisation

All-important measurements, signals and indication from devices included in the optimization are continuously monitored to react immediately due to a certain change on them. If there is a loss of communication, internal errors on the device, alarms, changes in the mode of operation or similar, the same device will be excluded from the VVC calculation and no setpoints will be sent to this device. Also, if one of parallel transformers is unavailable, none of parallel transformers will be used in the optimization.

E. Monitoring and control of VVC setpoints execution

During the execution of the VVC function order and duration of execution, availability of the devices in the optimization, etc. are monitored. In this way it prevents the system from being brought into an unwanted state. Due to unexpected changes in the network

Renata Rubeša, Marko Rekić, Zoran Bunčec, Tomislav Stupić, Application of fully automated centralized voltage regulation in transmission system operation management, Journal of Energy, vol. 72 Number 1 (2023), 14–19
https://doi.org/10.37798/2023721465

such as switching off or communication unavailability of the devices in the optimization or similar, VVC will immediately stop the execution in that region and prevent the possible occurrence of a dangerous situation in the network.

IV. Setting up of the Optimal Power System State

The first step in implementing the VVC results is to switch off the local automatic control on individual objects in the optimization, i.e., to give the regulating control of individual objects to the VVC system. In the first run of the optimal power flow algorithm, a larger number of shifts in control variables occurs as a result the control variables now move in a coordinated manner to achieve the target function i.e., to reduce the operating losses in the system. Part of the test results is shown in Table III for two consecutive days of the field tests. The test started in the morning hours The delta shift value shows the total number of shifts of tap changer position (transformers, VSR) from the initial value. The initial value in the first run of the VVC algorithm is the value inherited from the situation while the local (primary) control was active. Delta shifts for the following runs is the total number of shifts of tap changer position (17 transformers, 2 VSR) from the previous run. The number delta losses show the difference between the base case losses and the losses calculated after the execution of all controls. The losses are in each run reduced compared to the initial or previous value, but the most beneficial part is the equalization of the voltage profile and improving the overall voltage situation.

Table III

VVC system field test data

VVC run	1st run	2nd run	3rd run	4th run	5th run	6th run	7th run	8th run	9th run
1st day	10:42	11:42	12:42	13:42	14:42	15:42	16:44	17:51	18:42
D shifts	39	5	8	0	16	9	12	7	4
D losses [MW]	-0.952	-0.523	-0.818	-0.913	-0.515	-0.535	-0.363	-0.296	-0.309
2nd day	-	11:37	12:40	13:42	15:13	16:37	17:54	-	-
D shifts		16	8	5	2	4	8		
D losses [MW]		-1.296	-0.911	-0.358	-0.857	-0.801	-0.836		

Although the goal of the OPF function is to minimize an objective function, in this case the power system active losses, the OPF function also must satisfy the power system physical and operational constraints. Satisfying the constraints, i.e., voltage constraints, takes precedence overachieving the highest degree of optimality. The objective function of minimizing losses acts in the opposite direction with the algorithm requirement to keep the node voltages in prescribed limits. Accordingly, the system losses after the VVC run might be higher than in the initial situation. This case usually coincides with the daily load profile. During the day, the power system is more loaded than in the evening or at night. Load changes that occur at night and in the morning are highly reflected in the change of voltage profile. Therefore, the VVC system during the day period did not propose major control variable shifts as in the night period or in the period of a sharp drop and increase in load. The changes in the control variables were logical, compensating for the change in voltage because of the change in load.

V. Changing of Control Variables During VVC Operation

The voltage profile changes during the day and the change depends on the conditions in the network. Observing the voltage profile, correlation with the daily load profile can be noticed, i.e., in the reduced load period the voltage is higher, and in the period of increased load voltage is lower. This is a usual occurrence in the network. VVC in the optimization process tried to correct these changes in the voltage profile, i.e., in the specific periods of load change during the day a higher number of changes in control variables were made to successfully compensate the change of the voltage profile caused by load changes in the network.

For the purposes of the analysis, a graphical presentation was made in Figure 6 below. It contains the average number of changes in control variables per hour per day during a multiday VVC trial run. The number of changes in the control variables in this figure refers only to changes of transformers and variable shunt reactors tap changers.

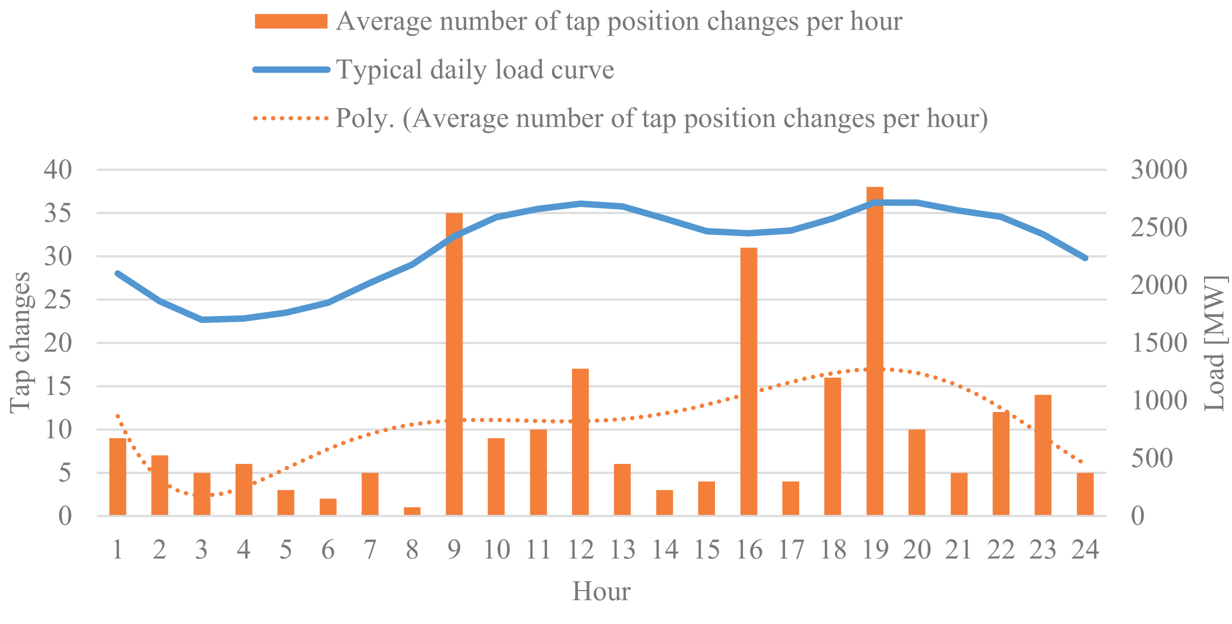

Fig. 6. Average number of control changes performed per hour and trend line of changes compared with daily load curve

Renata Rubeša, Marko Rekić, Zoran Bunčec, Tomislav Stupić, Application of fully automated centralized voltage regulation in transmission system operation management, Journal of Energy, vol. 72 Number 1 (2023), 14–19
https://doi.org/10.37798/2023721465

Observing the graph above, higher number of changes in control variables are happening during the hours in which a significant change in load occurs. Also, a trend line of the change of control variables has been added, which clearly outlines the shape of the daily load diagram. This is one additional confirmation of how VVC successfully compensated the change in the voltage profile during the day and kept the voltage profile at the values most acceptable in terms of reducing active power losses in the system.

VI. Conclusion

The advantage of the VVC system implemented in HOPS is the possibility to operate the VVC in a closed loop without operator\dispatcher intervention. Due to its complexity, the closed loop approach of reactive power regulation is rarely used in the TSO community and HOPS is one of the first TSOs that implemented regulation in such manner. In conclusion, regardless of safety algorithms implemented to avoid many unwanted situations in the power system (such as voltage breakdown, overloading of regulating equipment and similar), transmission system operator should be aware of possible risks. For this reason, HOPS initially opted for safer approach and mostly used semi-automatic mode which is additionally under the control of the dispatcher\operator.

References

[1] H. Vu, P. Pruvot, C. Launay, Y. Harmand, "An Improved Voltage Control on Large-Scale Power System", IEEE Transactions on Power Systems, vol. 11, br. 3, pp. 1295-1303, 1996.

[2] A. Gómez-Expósito, A. J. Conejo, C. Cañizares, Electric Energy Systems: Analysis band Operation, Boca Raton: Taylor & Francis Group, 2009.

[3] M. D. Ilic, X. Liu, G. Leung, M. Athans, C. Vialas, P. Pruvot, "Improved secondary and new tertiary voltage control," in IEEE Transactions on Power Systems, vol. 10, no. 4, pp. 1851-1862, Nov. 1995, doi: 10.1109/59.476050.

[4] B. Stott, O. Alsac, "Optimal power flow – Basic requirements for real life problems and their solutions", White paper, Prospectiva del Sector Eléctrico 2002-2011. (Secretaría de Energía. Mexico, 2002).

[5] R. Rubesa, I. Ivanković, M. Rekić, A. Jukić, "Condition for Establishing Voltage Var Control Function Considering Quality of Input Data" 2019 2nd International Colloquium on Smart Grid Metrology (SMAGRIMET), Split, Croatia, 9-12 April 2019.

[6] R. Rubeša, E. Cek, M. Rekić, M. Lasić, I. Ivanković, K. Mesić, „Advanced function for optimization in transmission network for Sincro.Grid project ", 13. Symposium on Power System Management, Croatian National Committee of CIGRE, Rovinj, 5. – 7. studenoga 2018..

[7] CIGRE Task Force C4.602, "Coordinated voltage control in transmission networks", February 2007.

Journal of Energy

VOLUME 72 Number 1 | 2023

journal homepage: http://journalofenergy.com/

Graphical Visualisation of the MCNP Mesh Tally File

Mario Matijević, Krešimir Trontl, Domagoj Markota

Summary — **This paper presents an updated version of the MTV3D (Mesh Tally Visualization in 3D) program with Windows graphical user interface for visualization of the MCNP-based mesh tally files. Several improvements over the previous program version are addressing better figure export functionality (»Save as« option), switching between linear and logarithmic values on axes, dynamic figure scaling in active window, inversion of relative errors from "max" to "min" values, etc. MCNP is a well known and widely used general purpose Monte Carlo computer code for neutron, photon and electron transport simulation through arbitrary three-dimensional configurations. An important feature of the MCNP code is a graphical display of the simulation model using auxiliary program, such as X-window server, which is useful for geometry error-checking during model setup and visualisation of Monte Carlo results from a mesh tally file (i.e. meshtal file) over a structured xyz mesh. Such inspection of the model is useful for the end user, providing an insight of the Monte Carlo convergence process in a phase space and effectiveness of the selected variance reduction parameters in shielding calculations. Basic features and functionalities of the updated MTV3D program are presented on some selected hybrid-shielding problems involving ADVANTG3.0.3 and MCNP6.1.1b codes.**

Keywords — **mesh tally, hybrid shielding, Monte Carlo, MCNP, ADVANTG**

I. Introduction

This paper presents new features and capabilities of the graphical visualization tool MTV3D [1] (Mesh Tally Visualisation in 3D) for displaying the mesh tally ASCII file of the Monte Carlo (MC) program MCNP [2]. The MTV3D was developed several years ago and this updated version contains several improvements over the original version addressing some shortcomings in practical usage. The mesh tally file of the MCNP program (meshtal file) contains user-defined superimposed structured mesh, independent from Monte Carlo problem geometry. It is developed as a special tally type, covering desired portions of user's model for capturing particle flux or any other response with relative errors. The MCNP program is distributed without a built-in tool for displaying a mesh tally, so standard approach is plotting with X server for Windows [3], such as Cygwin [4] or Xming [5] free tools. The same X server tools can be used for plotting MC model geometry and eventual weight windows (WWINP file) when variance reduction (VR) approach is needed. Using such tools for visualization of mesh-based objects is very useful for MCNP user, since they provide a useful insight in several phases of work:

1. geometry inspection during input checking;
2. weight windows quality inspection;
3. mesh tally flux convergence inspection, i.e. effectiveness of VR parameters.

The X server graphical emulators on Windows for mesh tally plotting are very useful but are essentially basic in their nature, so custom development of similar mesh-based graphical tools can be useful for practical applications. This paper presents such an effort to develop a graphical visualization tool for displaying the mesh tally file of MCNP program. Several improvements over the previous program version are addressing better figure export functionality (»Save as« option), switching between linear and logarithmic values on axes, dynamic figure scaling in active window, inversion of relative errors from "max" to "min" values, etc. Hopefully, this graphical tool will find its place in a daily work with MCNP at the Faculty of Electrical Engineering and Computing.

The rest of the paper is organized as follows. Chapter 2 gives a short description of a well known Los Alamos National Laboratory (LANL) MCNP code. Chapter 3 gives a short overview of the mesh tally file which can be generated using the FMESH card of MCNP code. Chapter 4 gives an overview of the program tools (modules) used for the MTV3D application development: MS Windows SDK (WinAPI, DirectX, GDI+), C++, and Microsoft Visual Studio. The MTV3D structure in C++ language for native Windows platform is presented in Chapter 5. Basic features and functionality of MTV3D are presented in Chapter 6 for real-life shielding problems, such as stationary cask for PWR spent fuel assemblies and spent fuel dry storage building dose distributions. Conclusions and referenced literature are given at the end of the paper.

II. MCNP Code of the LANL

The MCNP [2] is a general-purpose Monte Carlo N-Particle radiation transport code that simulates neutrons from 0-20 MeV, photons and electrons from 1 keV to 100 GeV. Several nuclear engineering applications of MCNP are nuclear criticality safety, oil-well logging, radiation shielding, medical radiation modelling, aerospace, etc. MCNP features detailed continuous-energy physics to provide a near-predictive model of how radiation interacts with matter. It has been continuously developed for over 60 years and has been widely used internationally for over 40 years. Regardless of the problem nature, many statistical trials or particle histories are required for MC simulation to converge to an acceptable solution. For that purpose, the variance reduction techniques (VR)

(Corresponding author: Mario Matijević)
Mario Matijević, Krešimir Trontl and Domagoj Markota are with the University of Zagreb Faculty of Electrical Engineering and Computing (FER), Zagreb, Croatia (e-mails: mario.matijevic@fer.hr, kresimir.trontl@fer.hr, domagoj.markota@gmail.com).

are standard tools for biasing a normal random walk of simulation particles, so important parts of the phase space are sampled more often at the expense of the less important ones. In particular, a well-known VR technique weight windows (WW) controls the particle population in space, time and energy by splitting particles into many low-weighted samples and, at the same time, rouletting unimportant particles into few high-weighted samples. MCNP code has a stochastic WW generator (WWG card) for generating WW over a user-defined superimposed structured mesh. This generates an auxiliary WWINP file, containing WW space-energy data, used to accelerate the final MCNP run. Alternatively, the user can construct deterministic WW using ADVANTG [6] code, based on the method of discrete ordinates (so called SN method) [7][8]. The ADVANTG has been successfully applied to neutron, photon, and coupled neutron-photon simulations of real-world radiation detection and shielding scenarios [9].

III. MESH Tally Data Structure

The mesh tally file was initially introduced in MCNP5v1.6 and is created with the FMESH card containing description of a superimposed structured mesh covering the problem geometry while the results are written to a separate ASCII file with the default name »meshtal« [2]. The track length estimate of the particle flux averaged over a mesh cell is the default MC estimator, but user can change this flux solution to any desired response, such as dose rates or reaction rates, typically by using an energy-dependent response function (DE+ DF cards) or with tally multiplier (FM card). The MCNP results are always normalized to unit source intensity, corresponding to a source which emits one particle per second. This can be properly scaled with an optional keyword »factor« in the FMESH card. A simple definition of the neutron mesh tally, with 100 cells (or bins) per x, y and z axis would look like the following:

```
c simple FMESH tally example in MCNP input
fmesh04:n     geom=xyz  origin=xmin ymin zmin  factor=1.0
              imesh=xmax  iints=100 $ number of x bins
              jmesh=ymax  jints=100 $ number of y bins
              kmesh=zmax  kints=100 $ number of z bins
```

When projecting mesh tally results over the MCNP model geometry, the particle tracking routines are used to march through the model geometry in the plane of the plot frame, while the plotting algorithm reads and puts cell-based flux value. The ASCII meshtal file contains the following information:

- MCNP version number,
- title of the simulation problem from the MCNP input,
- number of histories simulated (for normalizing tallies),
- mesh tally ID number,
- particle type for tracking with mesh tally,
- information about optional response function to modify tally results,
- structured mesh dimensions (tally bin boundaries in x, y, z),
- cell-wise results as MC average with relative error.

A mesh tally file sample from the PCA benchmark [10][11] is depicted in Figure 1, where one can notice aforementioned information about the LWR simulation model.

```
mcnp   version 6     ld=06/23/14  probid =  07/17/17 15:02:04
 PCA benchmark for reaction 27Al(n,a), S4/P1 VR parameters
 Number of histories used for normalizing tallies =      2048799.00

 Mesh Tally Number      104
 This is a neutron mesh tally.
 This mesh tally is modified by a dose response function.

 Tally bin boundaries:
    X direction:   -100.00    -99.00    -98.00    -97.00    -96.00
00      1.00      2.00      3.00      4.00      5.00      6.00
    Y direction:    -20.00    -19.00    -18.00    -17.00    -16.00
00
    Z direction:    -50.00    -49.00    -48.00    -47.00    -46.00
00
    Energy bin boundaries: 0.00E+00 1.00E+36

       X         Y         Z      Result     Rel Error
    -99.500   -19.500   -49.500 0.00000E+00 0.00000E+00
    -99.500   -19.500   -48.500 0.00000E+00 0.00000E+00
    -99.500   -19.500   -47.500 0.00000E+00 0.00000E+00
    -99.500   -19.500   -46.500 0.00000E+00 0.00000E+00
```

Fig.1. Mesh tally file structure

IV. Modular Structure of MTV3D Program

Interactive 3D graphics (zoom, rotation, cut plane, elevation, etc.) of MTV3D program were developed for MS Windows operating system. An overview of the program tools used for MTV3D development is presented next, including MS Windows SDK (WinAPI, DirectX, GDI+), C++, and Microsoft Visual Studio.

A. Microsoft Windows SDL Module

The MS Windows SDK (Software Development Kit) is a set of Operating System (OS) native tools for software development, while variety of APIs (Application Programming Interface) allows complete supervision of all resources, including CPU, Graphical Processing Unit (GPU) and RAM. The WinAPI is a primary tool for GUI (Graphical User Interface) development and has many visual elements, such as buttons (radio/check/click), textbox, select box, etc. Drawing of basic shapes is provided with GDI+ while more demanding graphical rendering is based on specialized DirectX libraries, i.e. Direct3D performs 3D graphics rendering, while Direct2D takes care of 2D graphics. DirectWrite is quite helpful for text incorporating into D3D/D2D frames, as there is no exact tool to perform such operation in DirectX11. DirectXMath library's methods simplify work of mathematical operations with vectors and matrices.

B. The C++ programming language

The C++ is an object-oriented programming language of third generation [12] created by Bjarne Stroustrup in the early 1980s as an extension of C language, the so called »C with classes«. The language has gone through process of standardization and became the most important programming language in the whole computer industry. The C++ has been modernized to keep up with other similar languages and has also been enriched with elements of functional programming paradigm. For that reason, the standard C++ v.17 has smart pointers, lambda expression, data type deduction, etc. It also has Standard Template Library (STL) which makes easier to manipulate data.

C. The Microsoft Visual Studio Environment

The MS Visual Studio is an IDE (Integrated Development Environment) for MS Windows OS. Within the IDE it is possible to develop applications for Windows OS, Xbox, Linux distributions, Android OS and to integrate various technologies, of which C# with .NET and C++ are the most significant ones. The MS Visual Studio possesses its own compiler Visual C++. Web development is also part of offered possibilities. This IDE contains extremely useful debugger, code autocompletion, language syntax checker, insight into executable assembly code, etc. Important part of IDE is Remote Debugger with ability to build the software on one machine and to deploy and debug on another, even with different versions of OS.

V. MTV3D Program Improvements

The graphical visualization software is created under the acronym MTV3D (Mesh Tally Visualization in 3D) with a targeted platform of MS Windows 7. Accordingly, MS Windows SDK 8.1 is used to cover Windows versions 7, 8, 8.1 and 10. Native MS Windows SDK tools requiring C++ language are preferred to achieve all intended features without any unwanted limitations, which would very likely to happen if a third party SDKs were used. The DirectX11 graphics APIs in this case are preferred to their counterparts like OpenGL API. Though OpenGL rendered graphics may result in a slightly better performance regarding the frame rate, the lack of platform support via Windows SDK represent an emerging issue in creation of a unique Windows cross-version (7 upwards) executable file. Starting with Windows 7, DirectX11 is contained within Windows OS. Considering that, the final executable file will not have any platform dependencies that are pre-required, such as runtime redistributables and DLLs (Dynamic Link Libraries). The MTV3D program has a user interactive GUI with the main window shown in Figure 2, offering a list of projects that are currently open by the user.

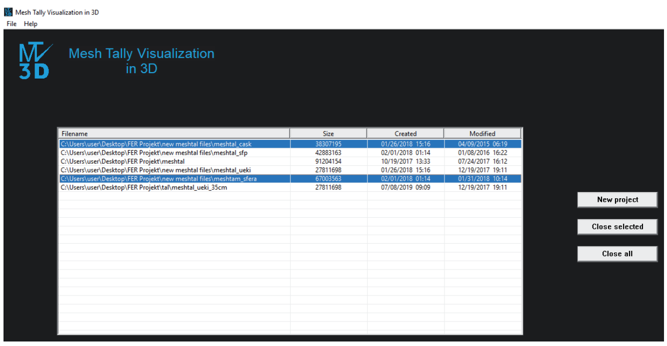

Fig. 2. Selection of a project inside the Main Window

The list shows filenames, size of files, creation date and last modification time of projects. The user can load a new project or close any of already opened. When loading a "meshtal" file, it is assumed by default that the file is UTF-8 encoded. Each loaded project has its own execution thread and main window consisting of MCNP data: MC average values (left window) and associated relative errors (right window). This is shown in Figure 3 for a point gamma source ($1.85 \cdot 10^7$ phot/s with 1 MeV) located inside a 4 cm thick spherical iron shield, with mesh tally consisting $0.5 \cdot 10^6$ cells (cut plane z=0 cm). The default plot is with linear scale and zero-valued cells are depicted in white (label "irrelevant"). The logarithmic scale is depicted in Figure 4, giving a more inuitive flux distribution over the same cut plane.

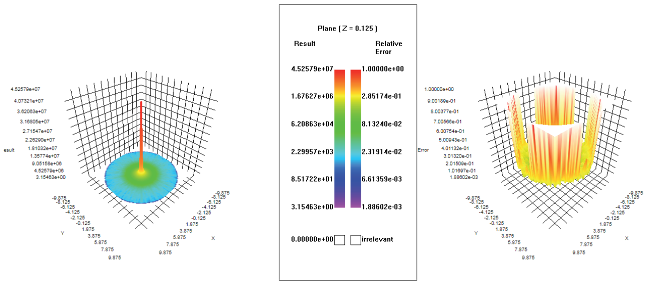

Fig. 3. Mesh tally gamma flux (phot/cm2/s) from point source inside an iron shield (lin scale)

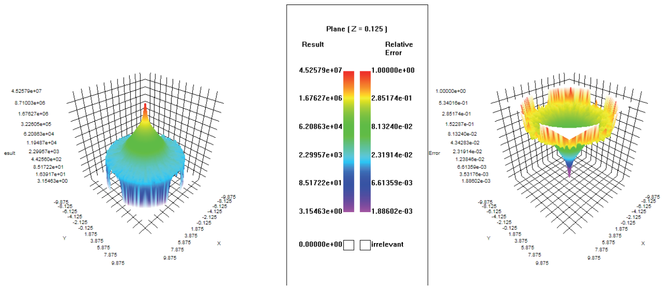

Fig. 4. Mesh tally gamma flux (phot/cm2/s) from point source inside an iron shield (log scale)

The selection of a cut-plane is done within the active window by selecting orthogonal plane and intersection value (x, y or z). This creates a new execution thread and a new window with MCNP results corresponding to a selected cut-plane. The plane values are then automaticaly elevated in z-axis to produce a surface plot effect in 3D. Top view of this surface plot is shown in Figure 5, giving classical 2D flux distribution in z=0 cm plane.

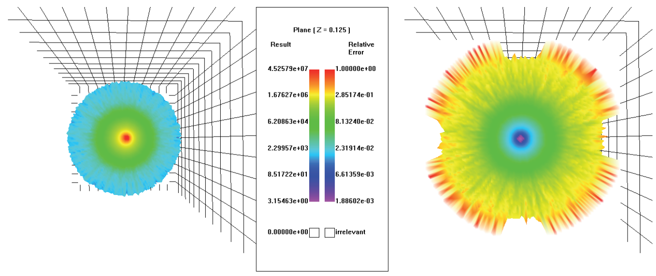

Fig. 5. Top view of the gamma flux surface plot in z=0 cm plane

Surface plot generally gives a better insight into a MC convergence process and effectiveness of the employed VR parameters. Inside this surface plot window it is further possible to select an independent axis, after which a new window is created showing the curve plot of MC results as a function of selected axis. This option is shown in Figure 6 for an independent x-axis, where one can notice gamma flux in yellow and relative errors in pink.

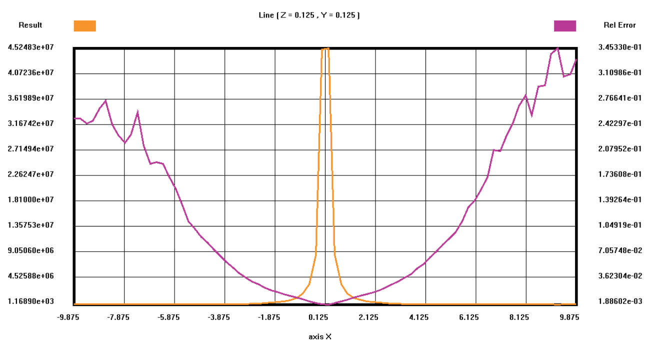

Fig. 6. Curve plot of gamma flux (phot/cm2/s) with relative errors in x-axis (cm)

Mario Matijević, Krešimir Trontl, Domagoj Markota, Graphical Visualisation of the MCNP Mesh Tally File, Journal of Energy, vol. 72 Number 1 (2023), 20–25
https://doi.org/10.37798/2023721468

It is possible to dynamically interact with a model by means of rotation and zooming. The rotation is a two-step process: the first step is around the vector from the centre of the viewport and the second step is around the vector orthogonal to the mouse pointer vector, observed from the centre of the viewport. The rotation steps are then combined to form a final rotation. The zooming is performed with a mouse scrolling option. Another useful feature is a visibility of grid lines and axes values, which can be turned on/off by selecting the appropriate checkboxes.

VI. Selected MTV3D Applications

Basic features and functionality of MTV3D program for visualization of MCNP mesh tally are presented next for some selected shielding results of the Spent Fuel Dry Storage Project of the NPP Krško [13]. The presented intermediate results are taken from an early stage of the project and are not reflecting the final updated design of spent fuel casks nor a dry storage building. The intention is only to demonstrate capabilities of MTV3D program in visualization of MC neutron flux distributions and assocciated errors. The final Independent expert Evaluation Report (IER) providing all model details and MC results of the transport cask (HI-TRAC) [14], storage cask (HI-STORM) [15] and dry storage building (DSB) can be found in report [13].

A. HI-STORM Storage Cask

The MCNP model of the HI-STORM storage cask is depicted in Figure 7 [15]. The multipurpose canister (MPC), housing 37 spent fuel assemblies from NPP Krško, is inserted in a thick concrete structure with upper and lower ventilation openings. The point detectors at cask surface are placed at inlet vents, cask midplane, outlet vents, and top lid (centre, annulus, edge). The hybrid shielding methodology of ADVANTG code was used for variance reduction (VR) preparation which optimized MCNP neutron dose rates (in rem/hr) at detector locations. The mesh tally had 1.2 million cells covering cask with surrounding air. The point detector neutron dose rates in cask midplane are shown using MTV3D in Figure 8 (surface plot), while 2D distribution (top view) is depicted in Figure 9.

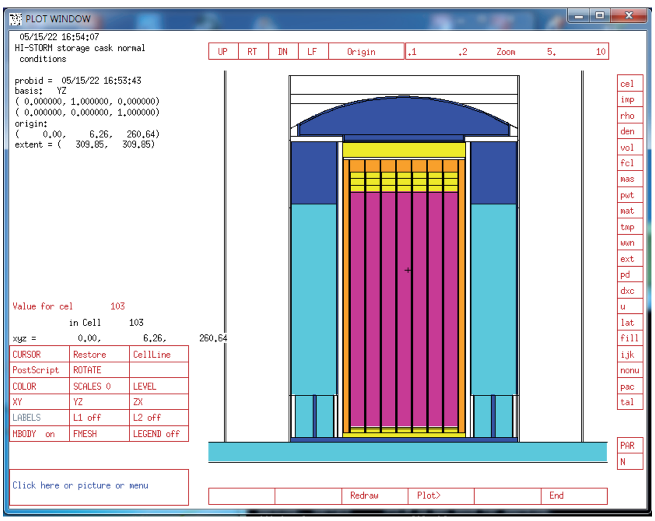

Fig. 7. MCNP model of the HI-STORM cask

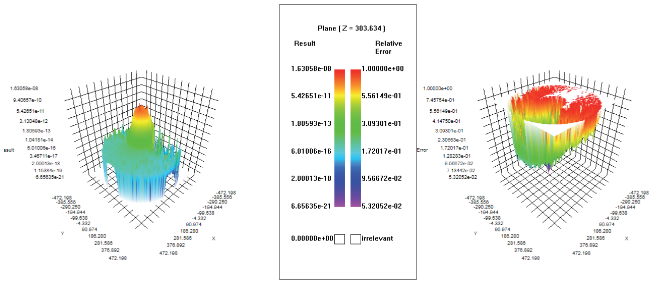

Fig. 8. Neutron dose rates (rem/hr) in cask midplane

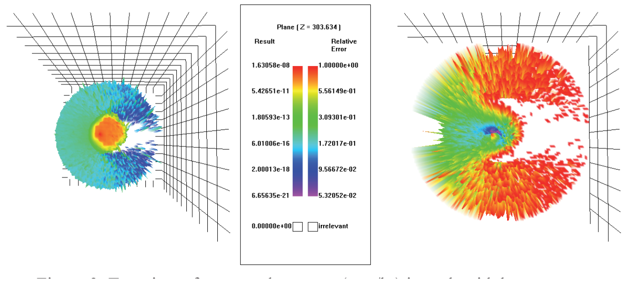

Fig. 9. Top view of neutron dose rates (rem/hr) in cask midplane

One can notice location of small relative errors corresponding to a point detector on the left side of the cask while unimportant regions have high errors (in red) or don't have any results at all (in white). Additional rotation of surface plots in different cut-plane can assist user in VR effectiveness inspection. The curve plot of neutron dose rates in x-axis is shown in Figure 10 using MTV3D, where cells with small MC error correspond to point detector surroundings.

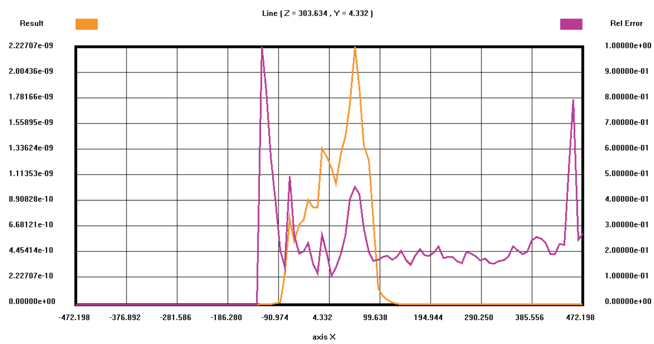

Fig. 10. Curve plot of neutron dose rates (rem/hr) with relative errors in x-axis (cm)

B. Dry storage building for HI-STORM casks

The MCNP model of the DSB (Figure 11) contains a HI-STORM cask array 7x9 located in a concrete building with thick foundations. This tentative model had 63 casks filled with the same averaged neutron-gamma source, corresponding to a spent fuel cooling period of 59 years. The steel roof for gamma skyshine was introduced in the later phase of the model together with a detailed source of the individual cask depending on real simulated Campaign. The hybrid shielding methodology was used to optimize neutron dose rates (in rem/hr) inside and outside the DSB. The location and dimensions of the cask transfer doors proved to be an important path for particle streaming inside the building. The mesh tally showing global neutron dose rates over DSB is shown in Figure 12 (values omitted), while neutron dose rates in cask midplane are shown in Figure 13 and Figure 14 (top view). These initial solutions demonstrated a need for VR refinement and insufficient MC

Mario Matijević, Krešimir Trontl, Domagoj Markota, Graphical Visualisation of the MCNP Mesh Tally File, Journal of Energy, vol. 72 Number 1 (2023), 20–25
https://doi.org/10.37798/2023721468

histories over 1.1 million cells since statistical noise proved to be quite high in the desired regions. This notorious slow convergence of the neutron-gamma dose rates at distant regions, well below background radiation level, was thoroughly investigated in [13][14][15] with different tally objects, until satisfactory MC errors were achieved.

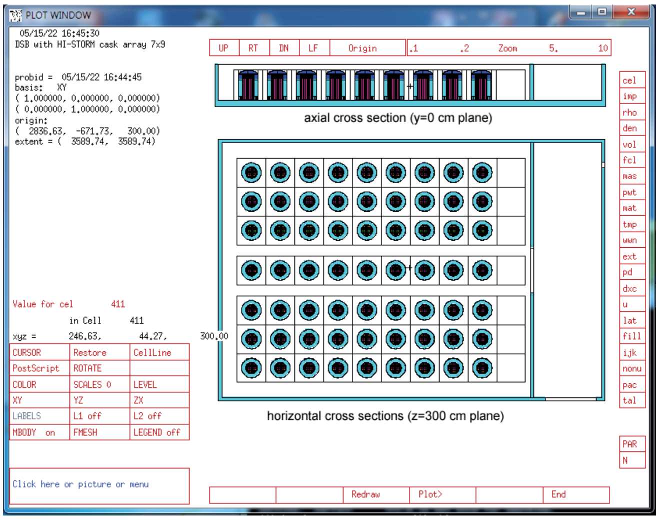

Fig. 11. MCNP model of the DSB

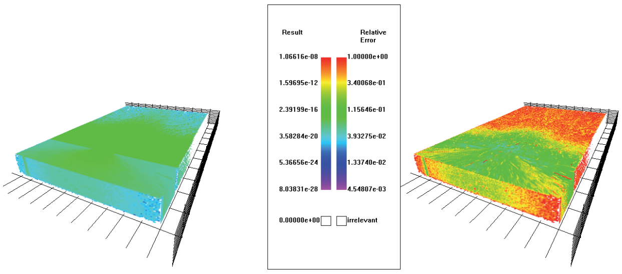

Fig. 12. DSB neutron dose rates (rem/hr) with relative errors (global)

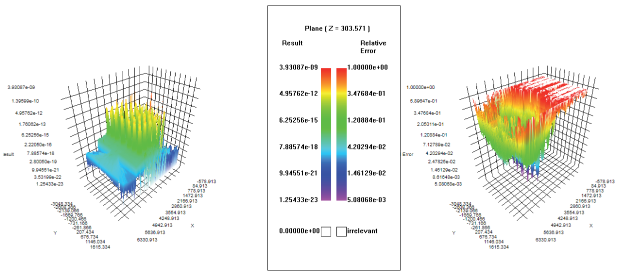

Fig. 13. DSB neutron dose rates (rem/hr) with relative errors (cask midplane)

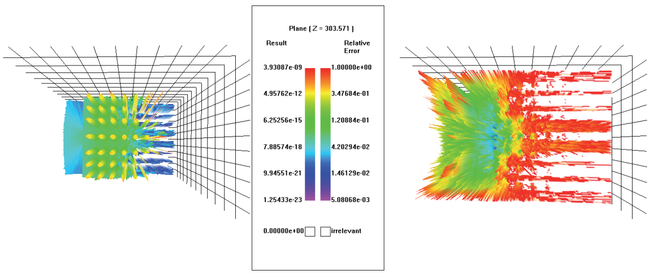

Fig. 14. DSB neutron dose rates (rem/hr) with relative errors (top view)

Results of neutron dose rates (in rem/hr) outside of DSB are shown in Figure 15 and Figure 16 (top view), showing the necessity for improved VR parameters and more CPU time for increased number of MC histories.

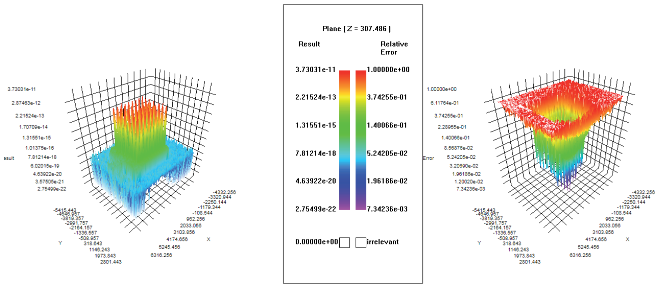

Fig. 15. DSB external neutron dose rates (rem/hr) with relative errors (cask midplane)

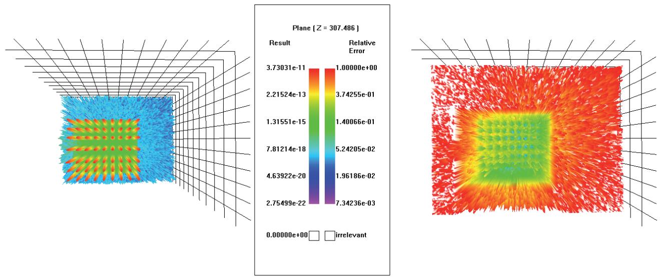

Fig. 16. DSB external neutron dose rates (rem/hr) with relative errors (top view)

VII. Conclusions

This paper presents an updated version of MTV3D program for visualization of the MCNP mesh tally file. The main features of the MTV3D program are 3D visualization of mesh-based results (MC mean values and relative errors), cut-plane results with elevate transformation producing surface plots, and curve plots for selected independent axes. The choice of program modules used for MTV3D development was determined by Windows operating system. The MS Windows SDK 8.1 was used which supports Windows versions from 7 to 10. Application controls are implemented using procedures from Win32 interface and Windows Controls library. Graphical unification of points was done via DirectX11 API collection, including DirectWrite on text rendering. Transformations over matrices and vectors were done using DirectXMath library, while 2D rendering is based on GDI+ class-based API. The MTV3D supports multicore CPU architecture, multithreaded environment processing, and simultaneous work with several open projects. The capabilities of MTV3D were demonstrated for several real-life shielding problems, namely spent fuel dry storage building of NPP Krško. Future work on MTV3D will introduce additional options for mesh tally plotting and possibility to read external WWINP file of MCNP.

References

[1] M. Matijević, D. Markota, D. Grgić, »Software Development for Visualization of Monte Carlo Results Based on the MCNP Program«, Proceedings of the International Conference Nuclear Energy for New Europe, Portorož, Slovenia, September 9-12, 2019.

[2] T. Goorley, »MCNP6.1.1-Beta Release Notes«, LA-UR-14-24680, 2014.

[3] X.Org Foundation website: https://www.x.org/wiki/

[4] Cygwin website: https://www.cygwin.com/

[5] Xming website: http://www.straightrunning.com/XmingNotes/

[6] S. W. Mosher, S. R. Johnson, A. M. Bevil, et al, »ADVANTG – An Automated Variance Reduction Parameter Generator«, ORNL/TM-2013/416, Rev. 1, August 2015.

[7] G. I. Bell, S. Glasstone, Nuclear Reactor Theory, Van Nostrand Reinhold Company, Litton Educational Publishing, 1970, pp. 252-273.

[8] J. C. Wagner, A. Haghighat, »Automated variance reduction of Monte Carlo shielding calculations using the discrete ordinates adjoint function«, Nucl. Sci. and Eng., 128(2), 1998, pp. 186-208.

[9] M. Matijević, R. Ječmenica, D. Grgić, »Spent Fuel Pool Dose Rate Calculations Using Point Kernel and Hybrid Deterministic-Stochastic Shielding Methods«, Journal of Energy: Energija, Vol. 65, No. 1, 2016, pp. 151-161.

[10] J.A. Kulesza and R.L. Martz, »Evaluation of the Pool Critical Assembly Benchmark with Explicitly Modeled Geometry Using MCNP6«, Nuclear Technology 197(3), 2017, pp. 284-295.

[11] M. Matijević, D. Pevec, K. Trontl, B. Petrović, »PCA Benchmark Analysis with ADVANTG3.0.1. and MCNP6.1.1b Codes«, Journal of Energy: Energija, Vol. 68, No. 2-3, 2019, pp. 171-183.

[12] B. Stroustrup, The C++ Programming Language, 4th Edition, Addison-Wesley, 2013.

[13] »Independent Expert Evaluation Report of Spent Fuel Dry Storage Modification Documentation for Spent Fuel Cask Criticality and Dose Assessment«, Report number: FER-ZVNE/SA/SO-FR01/19-3, commissioned by: Nuclear Power Plant Krško, executed by: University of Zagreb, Faculty of Electrical Engineering and Computing, Department of Energy and Power Systems and Department of Applied Physics, 2019.

[14] D. Grgić, M. Matijević, P. Dučkić, R. Ječmenica, »Analysis of the HI-TRAC VW Transfer Cask Dose Rates During Nuclear Power Plant Krsko Spent Fuel Dry Storage Campaign One«, Journal of Nuclear Engineering and Radiation Science (2021) doi:10.1115/1.4051447.

[15] D. Grgić, M. Matijević, P. Dučkić, R. Ječmenica, »Radiation shielding analysis of the HI-STORM FW storage cask«, Nuclear Engineering and Design, 396 (2022) 111878, pp. 1-13, doi: 10.1016/j.nucengdes.2022.111878.

Journal of Energy

VOLUME 72 Number 1 | 2023

journal homepage: http://journalofenergy.com/

Cybersecurity of the Power Production and Distribution of Critical Infrastructure

Krešimir Kristić

Summary — **The paper presents a structured, comprehensive and universally applicable approach to the management of cyber security of the power production and distribution of critical electricity national infrastructure. In his daily work, the author is competent for the protection and the resilience of the national electric power infrastructure against the threats from cyber space. The exposed approach and methods to the objective in question are successfully applied.**

Keywords — **Critical Infrastructure, Cybersecurity, Electricity, Electricity Distribution, Power Production.**

I. Introduction

THIS paper addresses the generic vulnerabilities of production and distribution power systems in the field of cyber security and protection of the national power infrastructure.

In times of crisis and crisis situations, we feel the impact of electricity supply disruptions on all aspects of our lives, and we become aware of the dependence of civilizational achievements and the way we live on the constant availability of electricity.

We are also witnessing successfully carried out attacks from cyberspace on the critical power infrastructure of production and distribution systems, the consequent damages of which cause significant disruptions in the functioning of the society and economy due to interruptions in the supply of electricity to consumers. In doing so, vulnerabilities and new risks are increasingly used due to the combination of information technologies (IT) used primarily in business and in business processes, with operational technologies of industrial processes (OT) and new technological concepts such as IIoT (Industrial Internet of Things) and 5G connectivity. New emerging vulnerabilities caused by the deregulation of the electricity market with distributed electricity generation within the distribution system are also being exploited.

The key prerequisites for the efficient and effective implementation of cyber security activities and measures of the electricity infrastructure is knowledge about the vulnerabilities of protected objects – what is being protected, and knowledge about threats and attackers, i.e. from what and from whom the object should be protected.

(Corresponding author: Krešimir Kristić)

Krešimir Kristić is with HEP d.d., Ulica grada Vukovara 37, 10000 Zagreb, Croatia EU (e-mail: kresimir.kristic@hep.hr).

The paper describes the critical industrial processes of power and distribution systems in the context of their vulnerabilities due to cyber threats and groups of attackers with their goals.

Security in the business environment is a function of supporting the achievement of strategic business goals. The basic task, i.e. the mission of the business function of corporate security, is to enable a justified business request in a secure way. In the context of the operation of power and distribution systems [3,6], cyber security is primarily focused on ensuring reliability and availability, and on ensuring the contracted quality of electricity delivered to consumers [1]. The subject of this paper is an approach to the identification of relevant processes of power systems of hydroelectric power plants and thermal power plants and power distribution systems, primarily their vulnerabilities with associated threats that can adversely affect the operation of power systems from cyberspace and ultimately the quality, reliability and availability of power delivered to consumers [1- 6]. As for related works that cover certain specific similar segments, this work was designed based on a comprehensive top-down approach to economically justified protection of industrial automation and monitoring systems of power plants and electrical distribution systems, and it proved to be successful in application.

In the introductory part, it is necessary to explain the use of the terms and relationship between information and cyber security.

Information security in a business environment protects the most valuable business resource after employees, and that is - of course - information. The basis for this is the well-known Information Security CIA triad (Confidentiality, Integrity, Availability, CIA): confidentiality, integrity and availability of the information to be ensured. In this context, cyber security, which is focused on a set of threats only from cyber space against business valuable information, is actually a subset of information security [14].

In the field of protection of industrial processes (Operational Technology, OT) and Industrial Automation and Control Systems (IACS), the availability-continuity, integrity and confidentiality (AIC) of industrial production processes are primarily achieved by cyber security activities and measures, and only then, but no less important, related data, the bearers of relevant information, are protected.

In conclusion, the comprehensive Cybersecurity Program includes risk assessment, Business Impact Analysis (BIA) and enables the implementation of Information Security Management System (ISMS) activities and measures, which all together ensure the protection and elasticity of industrial processes of electricity production and distribution in relation to threats from cyberspace.

Section II. describes corporate Cybersecurity Program based on the relevant sectorial regulations and laws, on the efficiently and economically established risk assessment, and on the results of the Business Impact Analysis (BIA) performed.

Section III. deals with Electricity Infrastructure Vulnerabilities, dealing with key industrial processes in production power systems as well as in distribution power systems with an emphasis on emerging risks of atomized production in the distribution system itself. Threats and attackers exploiting the vulnerabilities of power systems are also described in this section.

Section IV. Lifetime Management of Cybersecurity describes the establishment of Cybersecurity management, implementation in active production, and management at final termination of the operation. Chapter V. Conclusion stresses Cybersecurity Program and two important aspects: the need for simultaneous implementation of complementary activities of risk assessment and BIA and the need for further elaboration of the emerging risks arising from the atomized production of electricity in the distribution system.

The paper provides an answer on how to create a framework and implement the organizational and technical measures required for the protection of critical power infrastructure in an economically justified manner in accordance with regulatory rules and relevant legislation. The presented approach and methods according to the objective in question have been successfully applied in practice.

II. Cybersecurity Program

The implementation of activities and the application of cyber security measures of the electric power system ensure the continuity and integrity of production industrial processes. In production and distribution power systems, the goal is to achieve delivery reliability that results in available and high-quality electricity delivered to consumers.

By applying the relevant sectorial regulations and laws:

1. Directive 2016/1148 of the European Parliament and the Council of the EU on measures for a high common level of security of network and information systems throughout the Union (NIS Directive, NISD) [11],
2. Act on cyber security of operators of key services and providers of digital services, NN 64/18. in force from 26.07.2018. (ZKS) [12],
3. Regulation on cyber security of key service operators and digital service providers NN 68/18 (Regulation), and best practices primarily defined in families of standards:
4. ISA/IEC 62443 – security of industrial automation and control systems,
5. ISO/IEC 27000 – information security management system,
6. ISO/IEC 22300 – business continuity management system and
7. ISO/IEC 28000 – supply chain security management system,

and then in other applicable standards, a comprehensive and holistic cyber security program for industrial automation and control systems (Program), as shown in Figure 1, is defined and implemented.

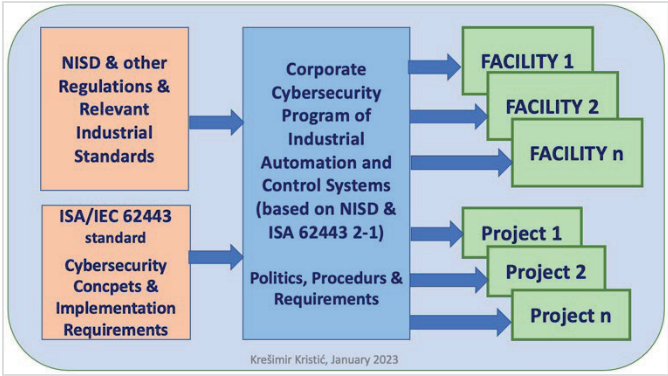

Fig. 1. Corporate Cybersecurity Program.

The NISD, i.e. its transposition into the national Croatian legislation ZKS and the Regulation operationalizing the ZKS, are a binding legal framework for all service operators (hereinafter referred to as the Operator) identified according to the criteria of the ZKS, of production and distribution of electricity of particular importance for the development of key national social and economic activities.

The NISD-ZKS regulation is the basis of the corporate cyber security program of industrial automation and control systems (the Program) because, in addition to the binding legal dimension with defined constraints, the NISD-ZKS regulation comprehensively and holistically defines the areas and activities in the Program:

- security management of network and information systems - management framework, organizational structure, establishment and documentation of management policy, implementation of internal controls;
- risk management - establishment of a risk management system, risk assessment, documentation on risk assessment, identification of equipment, persons and activities within which risk assessment is carried out, prevention, detection and resolution of incidents and mitigation of the impact of incidents;
- areas of protection of key systems - physical security and environmental security, security of supply, development and maintenance of key systems, management of contractual relationships, project management, management of outsourcing, management of structural assets, control of access to premises, management of changes in program assets, physical and logical separation of key systems , key system configuration, key system access control, key system vulnerability preventive checks, key system activity log, business continuity management, protection of data that is processed, stored and transmitted in the key system, protection against disruption of the availability of the key system, protection against malicious program code, reserve storage;
- notification of incidents - obligation to notify, incidents with a significant impact on the continuity of the provision of a key service, assessment of the impact of the incident on the continuity of the provision of a key service;
- notifications about incidents with a significant effect on the continuity of service provision - types of notifications, initial notification about an incident with a significant effect, interim report, final report on an incident with a significant effect, delivery of notifications about incidents with a significant effect, exchange of notifications;
- handling notifications about incidents with a significant effect - resolving incidents with a significant effect.

Krešimir Kristić, Cybersecurity of the Power Production and Distribution of Critical Infrastructure, Journal of Energy, vol. 72 Number 1 (2023), 26–33
https://doi.org/10.37798/2023721411

A. Risk Assessment

The purposefulness and economic justification of activities and measures during the implementation of the Program is ensured in accordance with Article 18 of the ZKS by implementing a risk assessment: “Operators of key services and digital service providers apply measures to prevent and mitigate the effects of incidents in proportion to the risk to which their network or information system is exposed”. The usual risk assessment method is essentially:

- repository of relevant information assets (entities), preferably automatically recognized and updated in real time,
- identification of relevant vulnerabilities of each entity in the repository of information assets,
- identification of relevant threats for each recorded vulnerability,
- assessment of the impact of each realized threat and on
- determination of the probability of the realization of the threat and unwanted impact, which is actually a risk per definitionem.

Support for the efficient and effective implementation of risk assessment is achieved through the implementation and mutual integration of the applied information technology (IT) asset management system, i.e., the IT asset management system of the current level (January 2023) ITAM 2.0 (IT Asset Management, ITAM) and the governance, risk and compliance system (Governance, Risk, Compliance, GRC).

The automated integration of these two systems at the data level in real or near real time is important. Automatically detected and updated entities of information assets from industrial automation and control systems using the ITAM tool, are transferred to the GRC system grouped according to the criteria of a unique set of vulnerabilities and entered as a single entity in the GRC system. The transfer relation from the ITAM repository of information assets to the GRC system is *n: 1* grouped according to the criterion of an identical set of vulnerabilities of the entity registered in the GRC system. It is desirable that in the GRC system each registered entity has an up-to-date attribute of the number of individually detected assets in the ITAM system. ITAM enables detailed analytical insight into the relevant properties of each individually detected asset-entity, for example into all hardware components and into the licensing status of all installed software at each individual management and control workstation in the industrial automation and control system.

In addition to the aforementioned ITAM 2.0 and GRC system capacities, for the efficient and effective implementation of risk assessment, it is also necessary to provide the adequate skills, i.e., trained workers for the smooth implementation of the risk assessment process. Every relevant change in industrial automation and control systems should be followed by a risk assessment, both proactively in the change planning phase, and during the change implementation itself, which is an indispensable part of the standard change management procedure.

It must be emphasized that the ITAM system must be adapted to work in the environment of industrial automation and control systems to be functionally neutral, i.e., without affecting the operation and functioning of these systems, and thus, most importantly, without affecting the industrial process itself.

B. Business Impact Analysis BIA

While risk assessment results in a relatively static picture of the probability of adverse events in business and in business processes, Business Impact Analysis (BIA), which is the process of analyzing business processes and financial and operational impacts and consequences of disruptions or stoppages in processes and business, ultimately results managing the continuity of the operations [13].

The implementation of activities and the application of cyber security measures of the electric power system should ensure the continuity and integrity of production industrial processes. The simultaneous implementation of complementary activities of risk assessment and BIA analysis provides a comprehensive, complete and solid basis for achieving this goal. Even more so because the collected data and intermediate results in both procedures mutually facilitate and speed up the implementation and raise the quality level of the delivery of both procedures - both risk assessment and BIA analysis. A prerequisite for risk assessment is an up-to-date repository of information assets, while at the same time BIA, among other things, should address the resources necessary for the uninterrupted development of industrial production processes. Furthermore, the risk assessment ensures the timely recognition and implementation of preventive activities and security measures that will reduce the probability of occurrence of unwanted events in business, while the BIA should reduce the negative impact of these events, if they do occur.

There are three phases of BIA implementation:

I. data collection and confirmation with two key procedures

- a financial analysis of the impact/consequences that results in an assessment of the possible financial effects on the Operator in the event of work interruptions, i.e., disruptions and interruptions of key processes,

- an operational analysis of the impact/consequences with an assessment of the impact and consequences of process interruptions in a key area on the fulfillment of the operational goals, for example in electricity production the goal is to keep power oscillations at the level of acceptable standard oscillations [4],

II. the analysis being carried out

- identification of key business processes and target recovery time (Recovery Time Objective, RTO),

- by prioritizing critical processes according to RTO,

- identification of critical resources and RTO,

- by prioritizing critical resources according to RTO,

III. documentation and approval, whereby all results of the business impact analysis must be formally approved by the owner of the process, usually the director of the Operator, as shown in Figure 2.

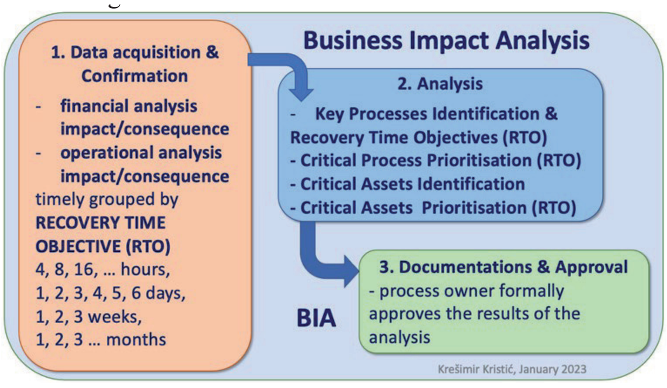

Fig. 2. BIA – Business Impact Analysis.

The key parameters for the definition of activities and the dynamics of the establishment and continuation of processes and operations within business continuity plans [13] and recovery plans for plant and equipment during business continuity management obtained by BIA analysis are:

• acceptable data loss - Recovery Point Objective, RPO

• Recovery Time Objective, RTO of critical process and operations

• the longest acceptable downtime - Maximum Tolerable Period of Disruption, MTPOD

as shown in Figure 3.

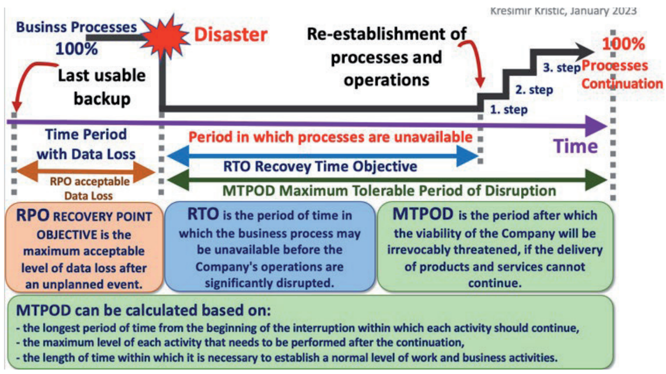

Fig. 3. RTO, RPO and MTPOD.

Based on these parameters, the plans define the dynamics of acquiring business resources and ensuring other conditions necessary for the re-establishment of business and production processes and for the continuation of business within the established RTO and MTPOD limits. The plans also define individual specialized teams with the minimum required number of relevant members for the smooth implementation of coordinated straight-line recovery activities of business and production industrial processes, such as the Crisis Management Team, the Damage Assessment Team, the Resource Assurance Team, the Crisis Communication Team and others. The plans define the types and frequency of simulation and other exercises of each individual team with an emphasis on the lessons learned during the implementation of the exercises (Eng. Lessons Learned), but inevitably also during real crisis situations, so that the necessary capabilities for efficient and effective crisis handling are ensured in addition to the necessary capacities and for continuous improvement of handling in crisis situations in the spiral PDCA cycle of continuous improvements (Plan-Do-Check-Act, PDCA).

C. Purpose of risk management and business continuity

By implementing the Program based on economically justified measures and risk reduction activities to an acceptable level, i.e. by implementing the Program based on the management of identified risks by their mitigation and on optimized and continuously improved business continuity plans and recovery plans for power plants and facilities, the purpose and goal of managing cyber security of the electricity critical infrastructure: delivery reliability, available and high-quality electricity delivered to consumers.

III. Electricity Infrastructure Vulnerabilities, Key Processes, Threats and Attackers

The inherent vulnerabilities of the traditionally defined electricity systems in relation to threats from cyberspace, primarily to industrial automation and control systems, are almost identical in production and distribution facilities, plants and areas regardless of the specifics of key processes. A significant number of these vulnerabilities are caused by organizational reasons, which are as follows:

- lack of a documented strategy and strategic directions for the development of the corporation's information system,
- the Information Security Management System (ISMS) has not been implemented in accordance with the basic ISO 27001 standard, and further to this vulnerability
- the procedure of the regular Administration's assessment of the state of security based on ISMS has not been introduced,
- there is no prescribed policy and/or procedure for the management of network devices, i.e., a policy for the use of network services,
- detection mechanisms on the network and on devices for process networks are inadequate,
- external contractors/service providers can cause problems during unannounced work on the information system. There is no formal periodic audit and supervision of the work of external suppliers, as well as their efficiency and safe way of working when accessing the information system,
- workers are not familiar with all the rules of information and cyber security during employment and can intentionally or accidentally cause damage due to ignorance,
- the absence and/or lack of usual functions and roles for information and cyber security in the member companies of the corporation does not contribute to the structured management of information and cyber security and weakens the response to possible information and cyber security incidents,
- there are no adopted internal acts for worker safety awareness,
- member companies of the corporation do not systematically conduct special training and education in the field of information and cyber security for those workers who have significant security roles and responsibilities,
- due to inadequately prescribed rules for protection against malicious software code (undocumented rules), protection management is difficult and incomplete,
- the patch management process is not documented or clearly prescribed, which causes vulnerabilities on systems due to shared responsibility or lack of information about vulnerabilities. For example, the consequence is the accelerated filling of memory on SCADA (Supervisory Control and Data Acquisition) systems due to badly applied patches,
- for all operational tasks of information and cyber security, responsibility is not clearly divided within the Operator and corporation in accordance with ISMS and the Program, and operational tasks are not performed, for example, maintenance of antivirus protection, hardening of network and server equipment,

Krešimir Kristić, Cybersecurity of the Power Production and Distribution of Critical Infrastructure, Journal of Energy, vol. 72 Number 1 (2023), 26–33
https://doi.org/10.37798/2023721411

- the lack of clear rules and instructions for the exchange of confidential information with external collaborators escalates especially in the implementation of projects by sending non-encrypted confidential information through unprotected channels, for example by e-mail and uncontrolled and security-questionable public services such as Jumbo mail, WeTransfer services, etc.,
- ineffective management of user access rights,
- there is no prescribed policy and/or procedure for the operation and management of mobile devices,
- lack of a defined and documented process for managing all types of changes in the information system (Change Management),
- there is no adopted internal act for managing the configurations of the information system,
- lack of a common template of basic security requirements that should be a standard component of tender documentation and contracts with external service providers and suppliers, etc.

Only then do the causes of vulnerability lie in operational procedures that are primarily mitigated by the implementation of measures at the technical level:

- operational and system records are not collected from all information system resources to the central system for detecting and reacting to anomalies (Security Operations Center, SOC),
- security hardening was not performed on the servers and unnecessary services were enabled,
- reliable authentication methods are not used, for example multi-factor authentication for remote access to the information system,
- parts of the information system do not use unique identifiers, but group generic user accounts, for example admin, administrator, root, etc.,
- regular checks of granted access rights are not carried out,
- activities for the maintenance of individual services are not recorded. An encrypted communication connection is used, but there are no strong authentication mechanisms for external connections or automatic closing of communication sessions in case of inactivity,
- inadequate supervision of the implementation of information classification rules without the use of software tools, for example tools for protection against data leakage (Data Leakage Prevention, DLP),
- the open communication connection is not automatically terminated after a long period of non-use, and potential attackers are left with the possibility of more time for malicious activity and compromising that relationship,
- etc.

In addition, it is necessary to emphasize and single out entire areas of new vulnerabilities in distribution power systems that arise from aspects of the service flexibility of the power distribution system, for example auxiliary services, aggregation and energy communities, e-mobility, balancing, congestion management and consumption management.

A. Key processes in production power systems

As part of the BIA analysis, key production and business processes in power systems are identified according to at least two criteria according to the criterion of unacceptable financial impact, i.e., damage due to disruption or interruption of the production process with regard to RTO, and according to the criterion of unacceptable operational impact of disturbances or interruptions in the supply of electricity for a duration longer than the established target RTO.

As a rule, the key processes in hydropower plants according to the above criteria are [6]:

- electricity production,
- preventive maintenance,
- corrective maintenance,
- periodic maintenance and repair,
- comprehensive planning and procurement in the widest scope of the Operator,
- production planning,
- safety management and system protection, occupational safety and fire protection.

While, as a rule, the key processes in thermal power plants are according to the two mentioned criteria:

- production of electricity,
- cooling of the production facility,
- production and preparation of water,
- preventive maintenance,
- corrective maintenance,
- periodic maintenance and repair,
- comprehensive planning and procurement in the widest scope of the Operator,
- planning and procurement of fuel,
- receipt and storage of fuel,
- production, planning and procurement of chemicals and
- safety management and system protection, occupational safety and fire protection.

B. Key processes in distribution power systems

According to the same criterion of unacceptable financial and operational impact in relation to the targeted RTO, the processes thus identified in power distribution systems are [6]:

- measurement and market support,
- remote control of the system,
- network management,
- telecommunications, and
- safety management and system protection, occupational safety and fire protection.

C. Specific vulnerabilities of distribution power systems

Emphasized and numerous peculiarities of the Program in the field of distribution power systems are determined by the binding implementation legal framework primarily determined by the Law on the Electricity Market of the Republic of Croatia (NN 111/21, ZoTEE) and the complex relationship of dynamically changing and mutually influencing technological and market aspects of distribution power systems. ZoTEE is a fully harmonized national transposition of the Directive on common rules for the internal electricity market 2019/944 of the EU Parliament and the Council of June 5, 2019. and amendments to Directive 2012/27/EU (SL L 158, 14.6.2019).

ZoTEE ensures the implementation of a number of relevant acts of the institutions of the European Union, such as:

- Regulation on the integrity and transparency of the wholesale energy market (1227/2011 of the EU Parliament and Council of 25.10.2011. SL L 326, 8.12.2011),
- Regulation on the establishment of guidelines for capacity allocation and congestion management (EU Commission 2015/1222 of 7/24/2015 SL L 197, 7/25/2015),
- Regulation on management of the energy union and action in the field of climate (2018/1999 of the EU Parliament and the Council of 11.11.2018),
- Regulation on the internal electricity market (No. 2019/943 of the EU Parliament and Council of 5 June 2019, SL L 158, 14 June 2019).

Just these listed components of the binding implementing legal framework point to great challenges in practical application and implementation. If we add to this the complexity of the market and technological dimensions and the dynamic influence of all factors on a balanced and stable operation and the required flexibility of the power distribution system on a liberal and transparently regulated market, the necessity of recognizing, assessing and mitigating all newly arising specific risks is imposed.

The aforementioned complexity of both the market and even more technological dimensions of power distribution system operation is well and in detail illustrated by the ZoTEE-prescribed obligation to adopt numerous by-laws:

- Rulebook on general conditions for the use of the network and electricity supply,
- Rulebook on quality conditions of electricity supply,
- Rules on changing suppliers and aggregators,
- Methodologies for determining the fee for connecting to the electric power network,
- Decisions on the amount of the unit fee for connection to the network,
- Methodologies for determining the amount of tariff items for electricity distribution,
- Rules on non-frequency auxiliary services for the distribution system,
- Rules on congestion management in the distribution system,
- Network rules of the distribution system,
- Rules on connection to the distribution network,
- Rules for applying substitute load curves,
- Rules of non-standard services of the distribution system operator with the price list of non-standard services.

Furthermore, from the point of view of cyber security, it is also necessary to identify and manage a significant number of newly emerging specific risks arising from aspects of service flexibility of the electricity distribution system, for example auxiliary services, aggregation and energy communities, e-mobility, balancing, congestion management and consumption management. These open questions and challenges have yet to be adequately answered in view of the feedback and experiences from the implementation operational practice that are just emerging or beginning to arrive.

D. Threats and attackers

Attackers from cyberspace who exploit vulnerabilities in power systems and, in addition to system failures, are the primary threat source to the expected function of industrial automation and control systems, according to their capabilities and possibilities are:

- structured organizations,
  - state organizations - highly educated and equipped professionals on the state salary,
  - organized crime – mafias, gangs, criminal units,
- ideologically motivated groups,
  - terrorists - cyber terrorists, cyber militias,
  - ideological activists – cyber hacktivists, interest groups, sects,
- individuals and associated individuals,
  - specialized units and cyber mercenaries,
  - amateurs,
  - revenge - embittered and/or dissatisfied workers, dismissed workers,
  - pathological attackers – dishonest competitor, dishonest client, scammer, fraudster.

Threats (only three have been listed to illustrate the possible consequences), with which attackers can exploit electricity systems vulnerabilities are as follows:

- an uncontrolled plant shutdown with serious plant damage and long-term downtime, made possible by not using reliable authentication and poor management of user access rights, was caused by an embittered employee,
- ransomware, regardless of the capabilities and abilities of the attacker, causes, in the best case scenario, an unplanned shutdown of the system with a delay of several days for the restoration of the industrial automation and control system from backup copies, or in the worst case, a targeted written blackmail software or the use of undetected vulnerabilities (Zero-Day), whereby plants can be irreparably destroyed, and expensive recovery can take months,
- compromised encryption protection infrastructure of the Public Key Infrastructure (PKI) from state-sponsored attackers who, with sophisticated methods, have unnoticed acquired the possibility of complete hostile takeover, management, and control of the system, etc.

IV. Lifetime Management of Cybersecurity

Lifelong cyber security management of electricity systems is carried out in stages:

- establishment of cyber security management,
- active production implementation of cyber security activities and measures,

- management of cyber security during the final shutdown of the production facility.

A. Establishment of cyber security management

When establishing the cyber security management system of power systems, the ISMS implementation framework is based on the Information and Cyber Security Strategy, on the Program and on the organizational chart of ISMS according to the best practice embodied in the globally accepted standard, and on other internal acts that are required for an orderly and organized implementation of the Program and are derived from these umbrella documents according to the principle of subsidiarity, such as:

- Information and cyber security policies of the Operator,
- Rulebook on physical security and environmental security of key systems,
- Rules for ensuring the availability of equipment, materials, energy sources and other resources necessary for the regular and continuous functioning and maintenance of key systems,
- Rulebook on management of contractual relations and outsourcing in terms of risk assessment and supervision of service providers,
- Access control procedures to premises and key systems,
- Rulebook on the physical and logical separation of key systems from the rest of the infrastructure,
- Rules for monitoring and recording user activities on the key system,
- Rules for ensuring data protection in key systems,
- Rulebook on protection against computer attacks with the aim of ensuring the availability of the key system,
- Rules for ensuring the development and maintenance of key systems,
- Regulations on the establishment and Procedure of preventive checks of vulnerability of key systems,
- Regulations on the establishment and business continuity procedures of key services in cases of incidents and
- Regulations on the establishment and Procedures for management of backup data storage.

Wherein the term key system is used for industrial automation and control systems.

B. Active production implementation

The active production and implementation of lifelong cyber security management of the EES is reduced to the operational implementation of the Program in accordance with the best practice in terms of roles and responsibilities of the organizational chart of information security management according to the ISO/IEC 27001 standard, as shown in Figure 4.: Fig. 4. Organizational chart of the Corporate ISMS.

- The management of the corporation and the director of the Operator, manage information and cyber security at the strategic level, delegating the execution of the necessary activities and measures to the tactical level. ISMS is the function of the Corporate Management Board and Directors as a support mechanism for the achievement of strategic business goals,
- The organizational unit for information and cyber security, for example the Department for information and cyber security (Department), at the tactical business level establishes and organizes the ISMS - the information and cyber security management system, which is a tool of the corporation's management and Operator directors and proposes, prepares and organizes the implementation of measures within the ISMS. At the operational level of business, Department supervises the implementation of information and cyber security activities and measures and reports to the Corporate Board and Operators' Directors,
- Owners of business processes, who as a rule are also the owners of information assets and bearers/owners of related risks (Owner), have a key role in accepting the proposed activities and measures. The bearer/owner of the risk approves and accepts the proposed measures and activities of the Department. If the owner does not accept the proposed measures and activities because they negatively affect the flow of the business processes and operations, the Department is obliged to propose to the Owner acceptable compensatory organizational and/or technical measures to achieve the necessary targeted effect, as a rule of mitigation of relevant risks,
- Organizational units of IT, telecommunications and external contractual collaborators and partners implement technical measures and activities under the supervision of the Department that reports to the Owner, Operators' Director and to the Management Board.

C. Management at final termination of operation

All dynamic activities and measures from the production phase are successively and gradually reduced and finally completely abolished alongside with the planned and controlled reduction in the intensity of business activities and technological processes and the final complete shutdown of the power plant or of the power distribution system.

Specific activities in the field of information and cyber security area in this phase are as follows:

- ensuring adequate availability of technological, process, technical, economic and all other data in accordance with the terms of storage and archiving according to the relevant legal and regulatory provisions and according to the internal acts and provisions of the corporation and the Operator,
- safe and environmentally friendly disposal of used information and industrial automation and control systems and destruction of all storage media used in production, carriers of previously adequately archived information,
- reporting to the Corporation's Management and the Operator's directors on the dynamics of the implementation of specific activities from this phase of lifelong management of information and cyber security of industrial automation and control systems.

V. Conclusion

A complete and comprehensive Program based on current legislation and established standards is the basis of cyber security management of critical power infrastructure. Mutually complementary activities of risk assessment and the Business Impact Analysis (BIA) achieve a satisfactory level of industrial processes continuity of critical electric infrastructure. Vulnerabilities with associated risks against the continuity and integrity of the industrial processes of electricity production and distribution based on underlying national critical infrastructure, and newly created vulnerabilities as a result of the consequent deregulation and liberalization of the electricity market [7-10], such as the service flexibility of the electricity distribution system, aggregation and energy communities, e-mobility, balancing, auxiliary services, congestion management and consumption management, have yet to be incorporated and appropriately treated within the framework defined by the Program and presented in this paper.

References

[1] T. Tomiša, "Sustavi za trajni nadzor kvalitete napona u distributivnim mrežama", *35th International Convention IEEE MIPRO 2012*, Opatija, Croatia, 21-25 May 2012.

[2] M. Perić, Ž. Tomšić, T. Tomiša, J. Galešić, "Upravljanje energijom u industrijskim mikromrežama u tržišnim uvjetima", *Bosanskohercegovačka elektrotehnika*, Vol. 10, pp 78-88, 2016.

[3] I. Kuzle, "Dijagnostika u održavanju elemenata elektroenergetskog sustava", student textbook, Sveučilište u Zagrebu, FER, Zagreb, 2013.

[4] T. Plavšić, I. Kuzle, Regulacija napona i jalove snage kao pomoćna usluga sustava, *Journal of Energy-Energija*, Vol. 54, No. 5, pp. 385-396, 2005.

[5] H. Požar, "Osnove energetike I, II i III", Školska knjiga, Zagreb, 1992.

[6] H. Pandžić, "Održavanje proizvodnih postrojenja elektroenergetskog sustava u novim tržišnim uvjetima", *14. međunarodni simpozij "Elektroinženjerski simpozij (EIS 2007)": Dani Josipa Lončara*, Šibenik, Croatia, pp. 22-27, 03-05 May 2007.

[7] "Opći uvjeti za opskrbu električnom energijom", *Narodne novine*, br. 14, 2006.

[8] The European Parliament and the Council of the European Union, "Common rules for the internal market in electricity", *Directive 2003/54/EC*, 26 June 2003.

[9] "Zakon o tržištu električne energije", *Narodne novine*, br. 177, 2004.

[10] "Mrežna pravila elektroenergetskog sustava", Narodne novine, br. 36, 2006.

[11] The European Parliament and the Council of the European Union,: "Directive on security of network and information systems", *Directive 2016/1148/EC*, 6. July 2016.

[12] "Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga ", Narodne novine, br. 64, 2018.

[13] ENISA, https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/bi-analysis/conduct-business-impact-analysis?v2=1&tab=details, 25 January 2023

[14] NIST, „Glossary of Key Information Security Terms", NIST IR 7298r3, July 2019

ENERGIJA