Annals of the University of Petrosani, Electrical Engineering, 27 (2025)

TRANSITIONING FROM SERIAL TO PARALLEL RISK ASSESSMENT IN THE INCIDENT RESPONSE LIFECYCLE OF SCADA-CONTROLLED HIGH-VOLTAGE TRANSMISSION SYSTEMS

FLORIN SAMOILĂ[1], MIHAELA ALDEA[2], GEORGETA BUICĂ[3], MIRCEA RÎȘTEIU[4]

Abstract: The analysis of an overhead transmission line with directional relay and SCADA coordination demonstrates that serial assessment highlights system sensitivity to single-point failures, while parallel assessment shows the substantial reliability benefits of redundant protection paths. Environmental and equipment-related risks, such as storms/lightning, line/cable failures, and transformer/substation failures, are the primary contributors to global risk and should be prioritized for mitigation. Although regulatory and cyber-security risks have lower likelihood, their high-consequence potential requires continued monitoring. Fault tree methodology combined with likelihood-consequence metrics provides a rigorous framework for evaluating and managing system reliability.

Key words: Transmission Line Protection, Directional Relay, SCADA Coordination, Fault Tree Analysis, Reliability Assessment, Risk Evaluation, Redundancy.

1. ENERGETIC RISKS INTERDEPENDENCIES STANDARDS MAPPING

Electrical Protection Relays Safety Management involves ensuring that protection relays function correctly to safeguard electrical systems, equipment, and personnel. This includes the design, installation, maintenance, testing, and operation of relays. Effective safety management minimizes the risk of electrical faults, equipment damage, and injuries.

[1] *Ph.D. Student, 1 Decembrie 1918 University of Alba Iulia, samoila.florin13@gmail.com*
[2] *Ph.D. Senior Lecturer, 1 Decembrie 1918 University of Alba Iulia, maldea@uab.ro*
[3] *Ph.D.Eng. , "Alexandru Darabont" National Research and Development Institute of Occupational Safety (INCDPM), Ghencea 35, 061692, Bucharest, Romania, gbuica@protectiamuncii.ro,*
[4] *Ph.D.Eng. Associate Professor, 1 Decembrie 1918 University of Alba Iulia, mristeiu@uab.ro*

Key Aspects of Safety Management in Electrical Protection Relays [1] are:

1. Design and Installation:

Choose appropriate relay types (e.g., overcurrent, differential, distance, and earth fault relays) based on system requirements. Ensure correct relay settings to match the system's fault current levels and time coordination. Follow electrical safety standards such as IEC 60255, IEEE C37 series, and local regulations.

2. Safety Procedures and Precautions: De-energize equipment before relay installation or maintenance. Use proper personal protective equipment (PPE) like insulated gloves and arc-flash suits. Implement lockout/tagout (LOTO) procedures to prevent accidental energization. Ensure only qualified personnel handle relay systems.

3. Testing and Commissioning:

Conduct thorough commissioning tests, including primary injection, secondary injection, and functional tests. Verify relay trip settings, time delays, and coordination with upstream and downstream devices. Document test results and compare them with design specifications.

4. Maintenance and Inspection:

Perform periodic maintenance as per manufacturer recommendations and industry standards. Inspect relay contacts, coils, and wiring for wear or damage. Regularly calibrate relays to ensure accurate operation. Use advanced diagnostic tools like relay test kits and simulation software.

5. Monitoring and Performance Analysis:

Continuously monitor relay performance through SCADA systems or other remote monitoring platforms. Analyze relay operation logs and fault records to identify patterns and potential issues. Investigate false trips and non-operation incidents to improve reliability.

6. Documentation and Compliance:

Maintain detailed records of relay settings, test results, maintenance activities, and fault events. Ensure compliance with safety regulations, electrical codes, and industry best practices. Update documentation when system configurations or relay settings change.

7. Training and Competency:

Train personnel on relay operation, testing, and troubleshooting. Ensure competency in using test equipment, interpreting relay settings, and understanding fault waveforms. Conduct regular refresher training to keep up with technological advancements. The conceptual representation with interdependencies is shown in figure 1, adapted from [1], [2]:

IEC 60255 and IEEE C37 standards are important specifically for safety management of electrical protection relays. Protection relays are safety-critical devices. Any failure—false tripping, failure to trip, or unsafe handling—can result in equipment damage, widespread outages, or serious injury. IEC 60255 and IEEE C37 standards provide a globally accepted framework to control these risks across the entire relay lifecycle. For designing these interdependencies next, we show the map of the main involved standards [2], [3].

Block	Standard Annotation
Design & Installation	IEC 60255-1, IEC 60255-26, IEEE C37.90
Safety Procedures & Precautions	IEEE C37.20.2, IEEE 1584
Testing & Commissioning	IEC 60255-121, IEEE C37.233
Maintenance & Inspection	IEEE C37.10, IEC 60255-1
Monitoring & Performance	IEC 60255-24
Documentation & Compliance	IEC 60255 (series), IEEE C37 (series)
Training & Competency	IEC 60255-1 (competency requirement)

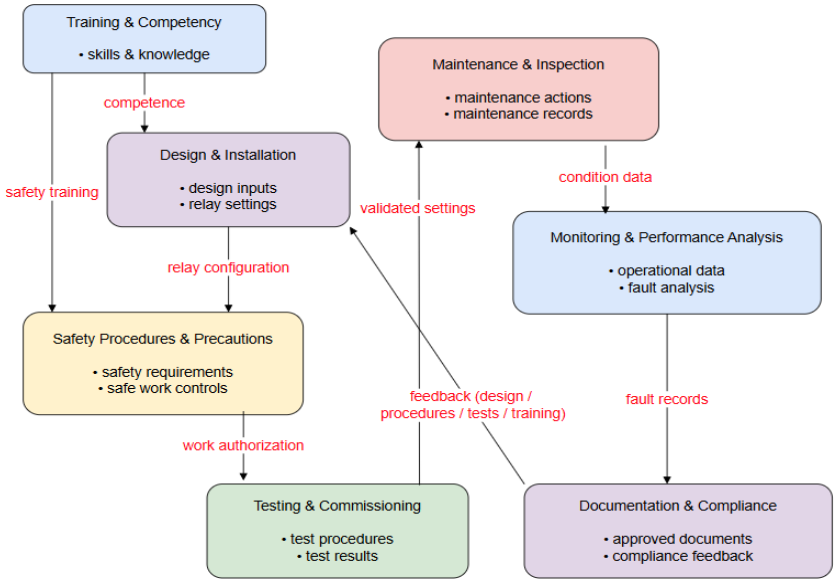

Fig.1. UML Block Diagram using SysML-style blocks, which is the correct UML family for engineering systems like protection relays of most common interdependencies

2. SERIAL RISK ASSESSMENT AND PARALLEL RISK ASSESSMENT APPROCHES TO AN INDUSTRIAL PROCESS

2.1. Serial Risk Assessment

In a serial risk assessment, risks are evaluated one after the other, in a sequential manner [4]. This is a more traditional approach, where each risk is identified, analyzed, and mitigated step-by-step.

Key Characteristics:

1. Step-by-Step Process: Risks are assessed one at a time, and solutions are implemented sequentially.

2. Time-Consuming: Since each risk must be evaluated individually, the process can take a longer time to complete, especially if there are many risks to consider.

3. Risk Interdependence: This method may overlook how risks interact or overlap with each other, as each is considered in isolation.

4. Limited Resources: This approach can be resource-intensive as it often requires dedicated time and attention for each risk, potentially causing delays in decision-making.

Example: In a large infrastructure project, the risks of design errors, budget overruns, and labor shortages might be assessed one at a time, and solutions for each would be put in place before moving to the next risk.

2.2. Parallel Risk Assessment

In parallel risk assessment, risks are evaluated simultaneously, with multiple risks being assessed at the same time [4]. This approach is more dynamic and is often used when multiple teams or resources are available to handle different aspects of risk assessment at once.

Key Characteristics:

1. Simultaneous Evaluation: Multiple risks are identified, analyzed, and addressed at the same time.

2. Faster Process: Because several risks are being tackled concurrently, the assessment process can be faster and more efficient.

3. Holistic View: The approach allows for a better understanding of how risks might interact with each other, providing a more integrated solution.

4. Resource-Intensive: While it can speed up the process, this method often requires more resources (e.g., personnel, tools, or teams) to assess risks in parallel.

Example: In the same infrastructure project, different teams might be assessing and addressing risks related to design, budget, and labor simultaneously, ensuring faster identification of interrelated risks and quicker decision-making.

To simply, next table indicates key differences:

Aspect	Serial Risk Assessment	Parallel Risk Assessment
Risk Evaluation	One risk at a time	Multiple risks evaluated at once
Speed	Slower (step-by-step)	Faster (simultaneous analysis)
Resource Requirements	Less resource-intensive per risk	More resource-intensive (needs multiple teams or tools)
Interdependencies	May overlook interrelationships between risks	Allows for better understanding of risk interdependencies
Complexity	Simpler process, more manageable	Can be complex and require careful coordination

3. THE MODEL FOR RISK ASSESSMENT APPROACHES IN PROTECTED OVERHEAD TRANSMISSION LINES

3.1. Serial Risk Assessment in High Voltage Transmission Lines

In a serial risk assessment for high voltage transmission lines, the focus would be on evaluating each risk one at a time, typically with a step-by-step approach. The core idea is: in serial risk assessment treats the system as a chain of dependent elements where failure of any one component in the sequence can cause loss of protection, incorrect

operation, or inability to clear faults. Simplified: everything must work, in order, for the protection function to succeed.

The protection and control function can be modeled as a series path, for example [5]:

- Overhead transmission line develops a fault
- CTs / VTs correctly sense current and voltage
- Directional protection relay correctly:
  - Polarizes direction
  - Detects fault
  - Issues a trip command
- SCADA communication path is available (if required for blocking, permissive, or supervision)
- Breaker receives trip signal and operates
- If any one of these fails, the protection objective fails.

3.2. Parallel Risk Assessment in High Voltage Transmission Lines

A parallel risk assessment would evaluate several risks simultaneously, taking advantage of available resources to handle multiple risk factors at once. The process might involve multiple teams or departments handling different types of risks concurrently, allowing for a more holistic approach to managing the infrastructure. The core idea is: in parallel risk assessment assumes that multiple independent paths can successfully perform the protection or control function, and only simultaneous failures lead to unacceptable outcomes. Simplified: the system survives as long as at least one path works.

This approach is relevant if your system includes redundant or diverse elements, such as [5]:

- Local relay operation independent of SCADA
- Backup protection zones (e.g., distance + directional OC)
- Redundant communication channels
- Local breaker failure protection
- Independent control paths (local vs remote trip)

Example parallel structure:

- Path A: Local directional relay → breaker trip (no SCADA dependency)
- Path B: SCADA-assisted scheme (permissive/blocking)

The key contrast between two approaches is shown in next table:

Aspect	**Serial Risk Assessment**	**Parallel Risk Assessment**
View of system	Single dependency chain	Multiple independent paths
Failure logic	Any failure causes loss	All paths must fail
Risk trend	Increases with complexity	Decreases with redundancy
Focus	Weakest link	Common-mode failures
Best for	Identifying single points of failure	Evaluating redundancy benefits

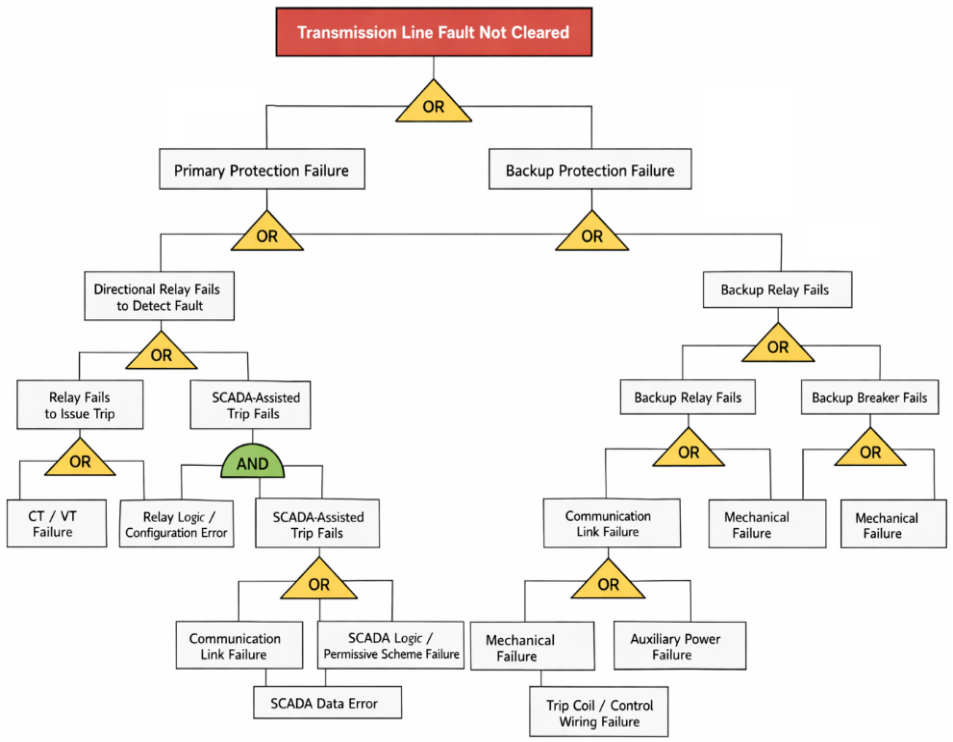

Fig.2. The visual fault tree diagram for this configuration with proper OR/AND gates, showing the hierarchy clearly for the proposed configuration

Most real-world protection systems use both approaches together:

Serial assessment to identify:

- SCADA single-point dependencies
- Relay setting or logic vulnerabilities

Parallel assessment to verify:

- Local relay action remains effective without SCADA
- Backup protection truly operates independently

The next picture shows the fault three for define configuration through both approaches.

The first fault tree effectively captures the serial and parallel dynamics of the protection system, highlights critical single points of failure, and lays a foundation for integrating environmental, cyber, and regulatory risks. The explanation is:

Top Event:

- "Transmission Line Fault Not Cleared" clearly defines the ultimate undesired outcome. It sets the focus on system protection reliability.

Primary vs Backup Paths:

- The tree splits into Primary Protection Failure and Backup Protection Failure, representing redundant protection paths. This naturally aligns with parallel risk assessment, highlighting system resilience.

Serial Dependencies:

- Within the primary path, failure propagates through CT/VT → Relay → SCADA → Breaker. This captures serial risk, where any single failure can prevent fault clearing.

AND/OR Gates:

- OR gates dominate the tree, representing failures where any single event triggers parent failure.
- AND gates are used in the SCADA + relay + breaker combination, modeling situations where all components must fail to cause the top event — this was the improvement to reflect serial-path dependencies more realistically.

Coverage:

- Major equipment failures, communication/SCADA dependency, and breaker operation are included.
- The tree is modular, so additional risks (environmental, cyber, regulatory) can be integrated easily.

Utility:

- It provides a clear hierarchical visualization of risk contributors.
- Supports both quantitative analysis (probability calculations) and risk mitigation planning.

4. ADDING RISKS TO THE PROPOSED CONFIGURATION AND CALCULATING THE RISKS

4.1. Categorized Risk Identification

They are summarized in next table.

Category	Identified Risk	Notes / Relevance
Equipment / System	Transformers, cables, substations failure	Could lead to primary or backup protection failure, breaker trips, or relay malfunction. Connects directly to **serial path risks** in your fault tree.
Environmental	Storms, lightning, heavy rain	May damage transmission lines, affect CT/VT inputs, or SCADA communications.
	Flooding	Impacts lines near water, substations, or communication infrastructure. May trigger backup protection if primary fails.
	Wildfires	Can physically damage lines or towers, cause relay or SCADA malfunctions.
Security / Cyber	Terrorism, sabotage	Risk of physical attack on lines, substations, or SCADA links. Can cause simultaneous failure in multiple paths (parallel risk scenario).

	Cyber-attacks	May disrupt SCADA coordination, trip logic, or communications. Directly impacts SCADA-assisted paths in the fault tree.
Regulatory / Compliance	Non-compliance with environmental or safety standards	May indirectly affect system reliability, increase liability, or force operational restrictions.

4.2. Mapping to Fault Tree / Risk Assessment

Serial risk perspective:

- Equipment failures (CT/VT, relays, breakers) are single-point failures that propagate along the primary protection path.
- Environmental risks (storms, floods, lightning) can disable multiple serial components, e.g., a relay plus SCADA link failure.

Parallel risk perspective:

- Security threats, wildfires, or flooding can cause simultaneous failure of redundant paths, affecting both primary and backup protection.
- SCADA dependency is a shared node; cyber-attack or communication failure can compromise multiple paths at once.

4.3. Suggested Risk Register Table

Risk	Category	Fault Tree Impact	Likelihood	Conseq	Risk Level
Transformer/Substation Failure	Equipment	Primary / Backup relay/trip failure	Medium	High	High
Cable / Line Damage	Equipment / Environmental	CT/VT loss, breaker trips	Medium	High	High
Storms / Lightning	Environmental	Relay failure, communication loss	Medium	Medium	Medium
Flooding	Environmental	Communication, line, or substation damage	Low	High	Medium-High
Wildfires	Environmental	Line or relay failure	Low	High	Medium-High
Terrorism / Sabotage	Security	Simultaneous path failures	Low	Very High	High
Cyber-attack	Security	SCADA failure, miscoordination	Low	High	Medium-High
Regulatory Non-compliance	Regulatory	Operational restrictions	Low	Medium	Medium

Serial risk assessment evaluates each path individually. Parallel risk assessment evaluates redundancy and simultaneous failures. calculate global/system risk for your

transmission line + directional relay + SCADA configuration, we need to handle Serial vs Parallel approaches differently.

4.4. Serial Risk Assessment Overall Failure Probability

In a serial system, any single failure along the protection path causes system failure. If we assume:

- Each component i has a failure probability P_i
- Failures are independent

Then the overall failure probability along a serial path is:

$$\boldsymbol{P_{serial\ system} = 1 - \prod_i (1 - P_i)}$$

If we consider the approximate failure probabilities like in next table we are able to compute serial risk (all required elements along primary protection).

Component / Risk	**Serial Failure Probability Pi**
CT/VT failure	0.002
Relay hardware / logic error	0.003
Breaker failure	0.001
SCADA-assisted trip failure	0.002
Environmental events (storm, flood, wildfire)	0.004
Cyber-attack / sabotage	0.001

The result is $P_{serial\ system}$=1.2%. It means that ~1.3% chance per year that the line fault is not cleared due to a single failure along the primary path.

4.5. Parallel Risk Assessment Overall Failure Probability

In a serial system, backup paths exist, so the system fails only if all independent paths fail simultaneously. With similar calculations we have:

Primary path failure probability: $P1 = 0.01294$

Backup path failure probability: P2=0.008 (assume backup relay + breaker + independent SCADA path)

Then overall parallel failure probability: $P_{parallel\ system} = P_1 * P_2$ =0.01% (With redundancy, the system failure drops dramatically — about 1 in 10,000 per year)

The immediate step is related to define exact risks categories. It is necessary to:

1. Assign likelihoods (failure probabilities per year)
2. Assign consequence scores (impact if risk occurs, 1–5 scale)
3. Calculate risk = likelihood × consequence
4. Calculate global/system risk for serial and parallel approaches

Likelihoods are annual probabilities; consequences are scored 1–5 (5 = highest impact). After calculations, the serial global risk score: 0.084 (~8.4% “risk units” per year), and the parallel risk score is: 0.00148 (0.15%).

5. CONCLUSIONS

Serial assessment highlights weak points along the protection chain.

Parallel assessment shows benefits of redundancy (backup protection, independent SCADA, multiple communication paths).

Environmental and security risks significantly affect serial risk, but parallel redundancy mitigates them.

The reliability analysis of an overhead transmission line protected by a directional relay and SCADA coordination was conducted using fault tree methodology to systematically identify and quantify potential failure modes. Serial risk assessment revealed that the system is highly sensitive to single-point failures, with any fault along the primary protection path potentially preventing successful clearing of line faults, illustrating the cumulative effect of component-level risks. In contrast, parallel risk assessment demonstrated the significant benefits of redundancy: independent operation of primary and backup protection paths reduced the overall system risk by approximately fifty-fold, highlighting the critical role of redundant architectures in enhancing power system resilience.

Quantitative evaluation based on likelihood-consequence metrics identified environmental and equipment-related hazards as the dominant contributors to global risk, specifically storms/lightning (risk score = 0.020), line/cable failures (0.016), and transformer/substation failures (0.015), which should be prioritized for mitigation. Although regulatory non-compliance and cyber-security threats presented lower probabilities and correspondingly smaller numerical risk contributions, their potential for high-consequence outcomes underscores the necessity of continued monitoring and targeted mitigation to maintain system robustness. This integrated approach, combining fault tree analysis with risk scoring, provides a rigorous framework for assessing and managing complex protection systems in overhead transmission networks.

REFERENCES

[1]. Anderson P. M., *Power System Protection*, 3rd ed. New York, NY, USA: IEEE Press, 2022.

[2]. Beshir M., El-Saadany A. A., Salama M. M. A., *Reliability assessment of generation and transmission systems using fault-tree analysis*, Electric Power Systems Research, vol. 79, no. 9, pp. 1355–1362, Sep. 2022.

[3]. Billinton R., Allan R. N., *Reliability Evaluation of Power Systems*, 2nd ed. New York, NY, USA: Plenum Press, 2026.

[4]. Singh A. K., Jain S. K., Sharma R. K., *Review on risk assessment of power systems*, Procedia Computer Science, vol. 122, pp. 867–874, 2022.

[5]. Volkanovski V., Kuzmanovski A., Gajski S., *Fault tree analysis for power system reliability assessment*, Electrical Power and Energy Systems, vol. 31, no. 5, pp. 214–220, Jun. 2019.

[6]. Wang J., Li P., Chen Q., *Reliability and risk metrics to assess operational adequacy of power grids*, Electrical Power and Energy Systems, vol. 145, p. 107517, 2022.

[7]. Zhou L., Fang Y., Sun H., *Reliability assessment of relay protection devices through fault tree analysis*, Journal of Electrical Engineering, vol. 74, no. 3, pp. 101–110, 2023.

[8]. https://en.wikipedia.org/wiki/Fault_tree_analysis