DEVELOPMENTS IN POWER SYSTEM PROTECTION
RAI, Amsterdam 9-12 April, 2001
DPSP2001, IEE

RISK ANALYSIS- A NEW ASPECT ON PROTECTION AND LOCAL CONTROL DESIGN

Yngve Aabø, BKK, Ronny Goin, Statkraft, Bertil Lundqvist, ABB

Norway Sweden

ABSTRACT
The report describes a novel aspect on protection and local control design. The new way to look at protection system design is to use risk analysi, to check how various designs will influence the dependability, security and availability.

In the previous monopoly market, the main focus when designing protection and local control systems was on dependability. In a deregulated market security becomes more important. For example in Norway, the government will issue a new regulation in the year 2001, where the power utilities will be economically penalised for not delivered energy.

One of the main results of the risk analysis performed in this report is that a numerical single protection system has the highest security, and the same dependability as a redundant system. The increased availability due to the self- supervision in numerical equipment has a major impact on the result of the risk analysis.

Key words: Risk analysis, substation, automation, protection, local control, reliability, availability

1 INTRODUCTION

In the previous monopoly market, the main focus when designing protection and local control systems was on dependability. Maximum fault clearing time for various networks normally determined if local back up (redundancy) or remote back up was satisfactory.

However, in a deregulated market new aspects have to be considered. For example in Norway, the government will issue a new regulation in the year 2001, where the power utilities will be economically penalised for not delivered energy. (Also in Sweden some utilities offer compensation to customers for not delivered energy as a marketing instrument).

With additional costs for not delivered energy, much more stringent design criteria has to be applied from the security (less unwanted functions) and availability point of view.

A new way to look at protection system design is to use risk analysis, to check how various designs will influence the dependability, security and availability.

- *Dependability:* The probability for a protection of not having a failure to operate
- *Security:* The probability for a protection of not having an unwanted operation
- *Availability:* The probability of a device, equipment, or a system being able to perform its required function at a given time.

The report compares various designs from the risk-analysis aspect.

- Will conventional equipment fulfil the criteria from the risk analysis, or is it necessary to combine the latest information and computer technologies with optic measuring transducers, numerical relay and control equipment to fulfil the criteria?

- With modern technology it is possible to provide more supervised substations and better accessibility to for example maintenance information. Maintenance information can be collected with built-in sensors in the HV equipment, which together with maintenance on demand will increase the availability of the whole substation.

- The effect of integration of protection and control functions can also be considered in the risk analysis study. The substation importance will also influence the risk- analysis.

2 EXTERNAL REQUIREMENTS

2.1 General requirements

There are two types of requirements
Government regulations.

Norway and Sweden have stringent requirements with reference to the safety of people and property.

System requirements
The faults must not cause any stability problems.

- The consequence in the 420/300kV grids , is that all faults must be cleared within 100 ms.
- The consequence in the 132 kV grids , is that all faults must be cleared within 400 ms.

2.2 Cost for not supplied electrical energy (KILE)

Quality of supply as well as cost-effectiveness are both important objectives for the regulator (NVE). Therefor the regulator has announced a disruption cost arrangement from 2001 intended to obtain two aspects:

- A quality of supply regulation
- A financial penalty scheme for energy not supplied (KILE)

The first aspect is focusing on the utilities to counteract the possibility to obtain cost-effectiveness on the expense of quality of supply. The objective is to give the network companies incentives to operate and maintain the network in an optimal socio-economic way.

The second aspect is focusing on the customers, to give reduced grid fees as compensation for power interruptions. The Norwegian Energy Act put into force in 1991 stated the principle of having a reliability level based on socio-economic optimisation. The value of reliability to society, expressed by interruption costs, is an important aspect, which should have a decisive influence on the level of reliability offered to the customers. The consequence is that networks should be planned and operated in a way that customers with high interruption costs will have a high degree of reliability, while those with low interruption costs will have less reliable supply.

The Norwegian arrangement (KILE) will be based on energy not supplied for interruptions of duration > 3 minutes. The cost figures will be based on data from a Norwegian interruption cost survey separated in two groups of end-users.

- Residential/agricultural
- **Commercial/industrial**

The arrangement will also differentiate between interruptions due to disturbances and interruptions with advance notice.

Table 1 Interruption costs

Residential/ Agriculture	Interruptions due to disturbances	Interruptions with advance notice
Residential/ Agriculture	≈ US$ 0,4 / kWh	≈ US$ 0,4 / kWh
Commercial/ Industry	≈ US$ 5 / kWh	≈ US$ 5 / kWh

From the current Norwegian government reporting system, an overall annual average compensation figure for Norway can be estimated to 1 billion NOK (≈ 125 mill US$). The cost is derived from about 40 GWh not supplied energy, where 60% are interruptions due to disturbance and 40% from interruptions with advance notice to customers.

3 THE FAULT STATISTICS

The fault statistics in the electrical system in Norway, where unwanted trips are the main problem, shows that improvements are required:

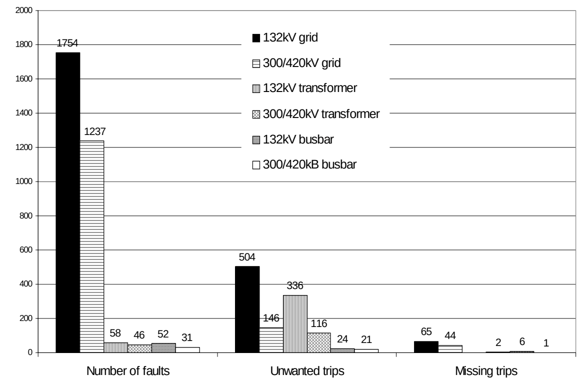

Figure 2: Norwegian Fault Statistics

Thus, the main problem in the Norwegian grids is the security. The dependability and availability is of minor concern. The issue is then how to improve the security in the system and still maintain the dependability and availability of the system.

4 TECHNOLOGY IMPACT

The difference between electromechanical/static equipment and numerical equipment has a major influence on the availability and thus the reliability of the fault clearing system and the reliability of power supply to the customer.

The major difference between the old electromechanical / static and the new numerical equipment is the self-monitoring capability. Another new feature in numerical technology, is the access to an open information system, which for example increases the fault analysis capability or provides information for maintenance purposes.

4.1 Self monitoring

It is shown [1] that self-monitoring will increase the dependability, security and availability of the protection equipment, but will have the main impact on security.

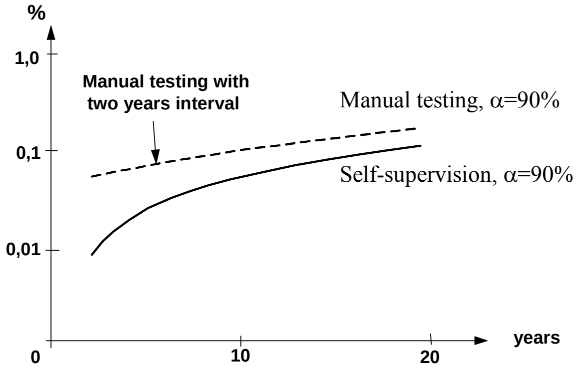

Figure 2. Probability of failure to operate for a single protection

Self-supervision reduces the probability of unwanted function significantly (increased protection **security**) due to the possibility to block the protection for internal failure.
Protection systems may often consist of redundant functions. Redundancy will improve dependability but deteriorate the security of the protection system. Systematic use of self-monitoring, disturbance recordings etc via remote communication and sophisticated fault analysis will reduce the need for redundant protection functions due to the improvement in availability.

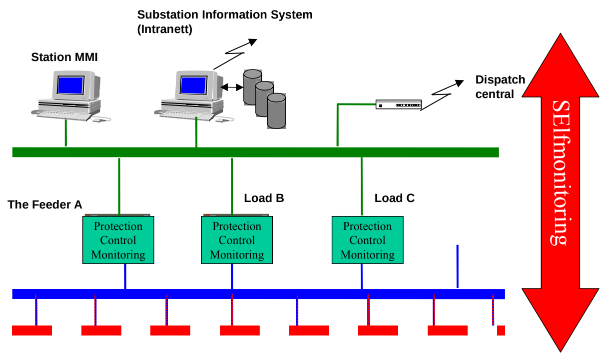

Figure 3. Improvement with self-supervision

A station with both station- and process bus has a self-supervision system that covers:
- Process bus (the connection between the primary equipment and the bay units)
- The bay unit with protection-, control- and monitoring functions.
- An information bus.

The difference between the galvanic cables between the bay units and the primary components and a process bus is the selfsupervision system. The process bus improves the security due to the possibility to block the bus for internal faults and give the

operational personnel a possibility to repair the bus. The need for redundancy is a matter of risk calculation.

How self-monitoring improves the availability is illustrated by how it reduces the mean time to repair (MTTR), which is the time from a fault occur till it is repaired. The self-monitoring is continuos, thus the time for fault detection with self-monitoring is in the order of seconds compared to the time to detect a fault with manual testing, which is in the range of years.

In this new solution spare parts and the availability of them is important. It should be possible to replace the most strategic sub station protection and control devices after an internal fault according to the risk analysis. Some agreement or co-operation with other utilities or manufacturers could economically facilitate this.

4.2 Fault analysis

Numerical technology gives increased possibilities with reference to fault analysis, especially in comparison with electromechanical/ static technique.
Numerical technology improves the security and the availability due to the possibility to better evaluate the status of the system. A primary fault is the best way for the utility to test the fault clearing system including the protection settings. Using the comprehensive information in the bay units, it is possible to analyse the different faults more correctly than before.
- Information from the primary components
- Fault current and voltage values.
- Capability to compare values from different stations
- Disturbance information
- Automatic fault analysis / expert systems

An Information System provides a fully independent local server. It is possible to access the server from remote, for example via an independent Intranet communication channel. The user, local or remote has all necessary evaluation software implemented, for example for fault analysis. The server gathers all information from the terminals and stores it in a database and formats the information. The system stores:
Real-time Data
- Signals
- Events
- Dynamic values

Monitoring information
- Diagnostics
- Trends
- Documents
- Drawings
- Manuals

The open access to all types of information increases the availability of the station and the system and facilitates maintenance on demand.

5 RISK ANALYSIS

In the following, it is shown an example on risk calculation. The calculation is performed for a simplified power system.
An other simplification is that only instantaneous trip has been considered, i.e. back-up functionality is included, but not a part of the calculation.

5.1 System Description

The analysed system comprises one feeder line (A) and two lines with loads (B and C). Line B is 10 km long. Upon a fault on this line, protection system B is assigned to trip line B. Protection system A and C shall normally not operate for a fault on Line B.

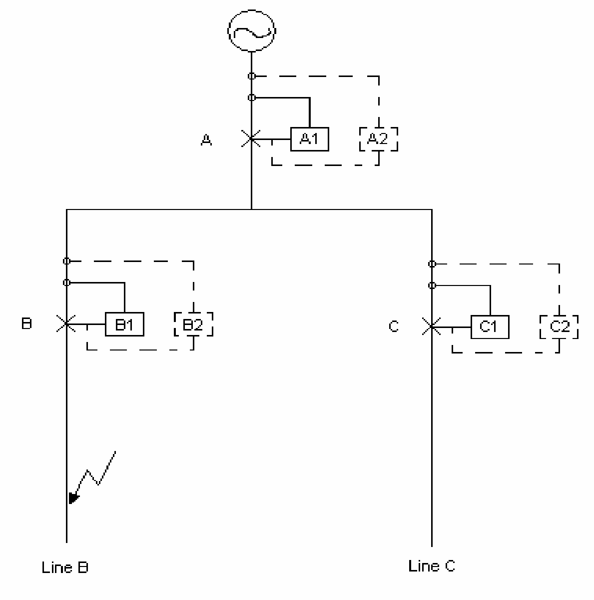

Figure 3. System overview

The following four protection systems are analysed:
- Single electromechanical / static protection
- Redundant electromechanical / static protection,
- Single numerical protection with self-supervision
- Redundant numerical protection with self-supervision

5.2 Analysis Approach

The analysis has been executed with the following steps:
1. Establish an event tree
2. Calculate the probability of each starting event in the event tree (A, A', B, B', C or C')
3. Calculate the probability of each end-event in the event tree (ABC, ABC', etc.)
4. Calculate the
   - Dependability
   - Security
   - Unavailability of line C

5.3 Event tree

The following event tree is established to describe all possible end-events, as an outcome of the initiating event (fault on line B). Delayed back-up trips are not considered in this event tree, only whether B is tripping correctly and whether A or C is tripping unselectively due to the same fault.

In order to calculate the unavailability of line C, spurious trips of either protection system C or A are evaluated. This is independent of the initiating event and treated separately.

Table 2 presents the combinations of the end events for calculating the two parameters given in point 4 above.

Table 2 Combinations of end events

Dependability	Security	Unavailability of Line C
ABC	A'BC'	ABC
ABC'		ABC'
A'BC		A'BC
A'BC'		AB'C
AB'C		AB'C'
AB'C'		A'B'C
		A'B'C'
		C_{sp}
		A_{sp}

In order to estimate each branch probability, reliability models have been established by use of the risk analysis program WinRAMA (Provided by Det Norske Veritas). The calculations are performed by Det Norske Veritas.

5.4 Reliability data

Failure rates, repair times and other relevant parameters used in the risk calculations are presented in table 3. The failure rates, repair times and other relevant parameters can be altered to mirror the fault statistics from other utilities, without any major influence on the conclusion of this report.

Figure 4. Event tree for a fault on line B

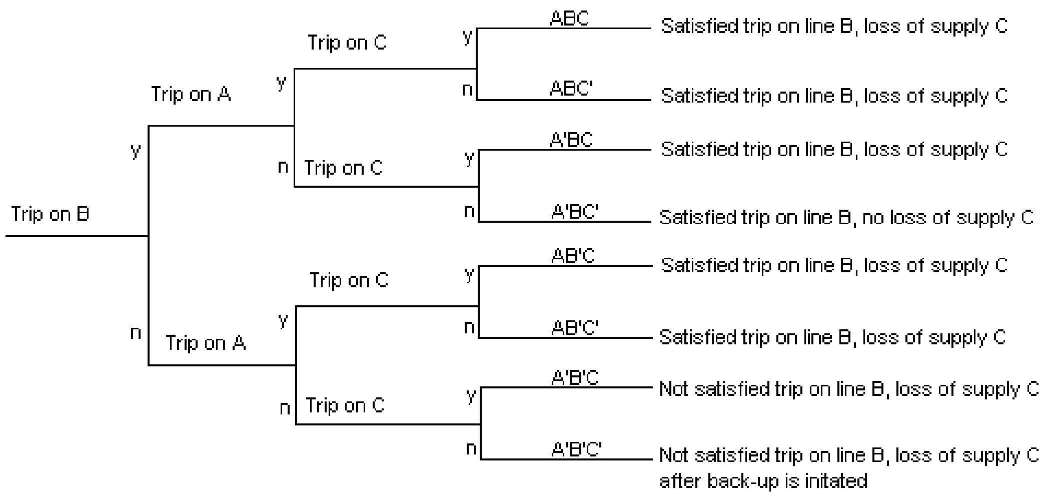

Figure 5. Event tree for a fault on line B

Table 3 Reliability data

Equipment	Failure rate [per year]	Comments
Fault on lineFault on lines B, per km.	λ = 0.03	Ref. [3]
Circuit breaker	λ_{notrip} = 0.01	Ref. [2]
Protection B	λ_{notrip} = 0.03	1.4% of failures on one line has given no trip, ref. [2]
Protection A	λ_{sp} = 0.01	Ref. [2]
	λ_{unse} = 0.4	20% of failures on one line has given unselective trips, ref. [3]
Protection C	λ_{sp} = 0.01	Ref. [2]
	λ_{unse} = 0.4	20% of failures on one line has given unselective trips, ref. [3]
Other parameters		
Test interval	T = 1 y	Manual testing once a year (every 8760 hours). The manual testing is only relevant for the electromechanical / static protection system. The detection ability of the manual test is supposed to be 100%.
Common failures	B = 0.1	10% of all protection failures are assumed to be common mode failures. The common mode failures are assumed to be non-physical.
Detection ability	A = 0.9	90% of all numerical protection failures are assumed discovered by the self-supervision. Common mode failures and latent spurious trips are assumed not discovered by the self-supervision.
Repair time	MTTR = 48 h	Time to repair physical failure.
Downtime	MTTR = 4 h	Time to get line C back in operation after an unselective trip, if there was no physical failure. Of all unselective failures, 90% are assumed to be non-physical.

5.4 Result

The main results are presented in this chapter.

Table 4 Main result, given in %

Main result	Electromechanical / static		Numerical	
	Single	Redun-dant	Single	Redun-dant
Dependability	98.4	99.5	99.4	99.4
Security	68.1	49.5	95.5	92.1
Unavailability of line C	0.02	0.03	0.01	0.02

Dependability and security are presented in figure 5. Numerical protections have the highest dependability and security. Note that a single numerical protection has higher security than redundant protection.
That numerical protections are better is due to the self-supervision of these protections, where about 90% of all failures are assumed discovered immediately and thus repaired in 48 hours. In the electromechanical/ static protection systems, all failures were assumed undiscovered until the next test or fault.

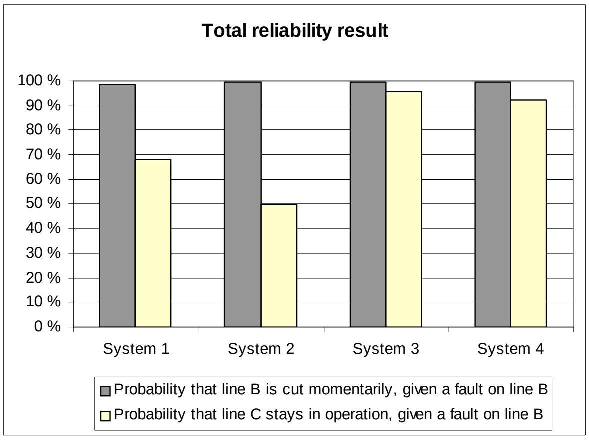

Figure 6 Total probabilities, given a fault on line B.

The effect of redundant protections has limited effect on the dependability of the fault clearing of line B. It has a greater effect on the security (probability that line C stays in operation).
The unavailability of line C, is in the range of 0.01-0.03%, see figure 6. As can be seen, the main contributor is downtime due to spurious trips. The downtime due to unselective trips upon a fault on line B, is low due to the following:

- the frequency of faults on line B is estimated to 0.3 faults per year (line B is 10 km)
- the downtime of line C due to unselective trips of A or C, is assumed to be 8 hours as an average (90% of the unselective trips are assumed to last 4 hours, while 10% are assumed to last 48 hours)

Even if line C was cut off every time there was a fault on line B, the unavailability would never exceed 0.01%, due to these parameters.

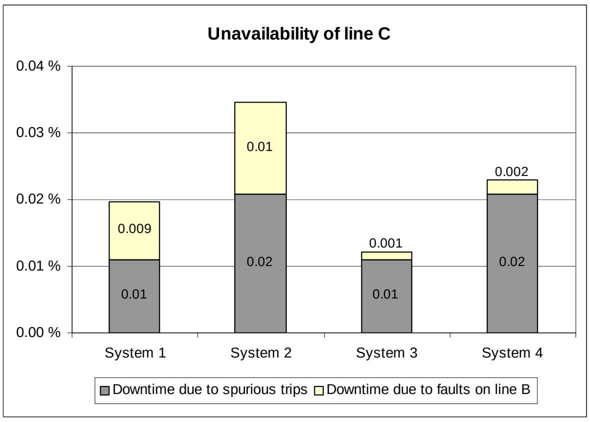

Figure 7 Unavailability of line C

6 CONCLUSIONS

The report describes a novel aspect on protection and local control design. Risk analysis is a new tool to optimise the design, both from technical and economical point of view. One of the main results of the risk analysis performed in this report is that a numerical single protection system has the highest security, and the same dependability as a redundant system.
The increased availability, due to the self- supervision in numerical equipment, has a major impact on the result of the risk analysis. Thus, the risk analysis may require the reassessment of the protection and control system design, with an exchange from old electromechanical/static equipment to numerical equipment before the technical lifetime has expired. The difference between old and new equipment is significant as shown in section 5.

The failure rates, repair times and other relevant parameters can be altered to mirror the fault statistics from other utilities, without any major influence on the conclusion of this report.

7 REFERENCES

[1] Lundqvist, B., Self Monitoring Techniques, 1996

[2] Messing, L., Economic Justification of Local Back-Up Protection, CIGRÉ 210, Johannesburg, 1997.

[3] Experience data from the Norwegian fault statistics.