# ENSURING SECURITY AND RELIABILITY OF SUPPLY BY CERTIFICATION OF CONTROL CENTRES AND NETWORK OPERATION

Josef POLSTER
Martin GLATZ
Robert SCHMARANZ
KELAG Netz GmbH - Austria
josef.polster@kelagnetz.at
martin.glatz@kelagnetz.at
robert.schmaranz@kelagnetz.at

Hendrik VENNEGEERTS
FGH e.V.
hendrik.vennegeerts@fgh-ma.de

Gerhard FESKE
TÜV SÜD Management Service GmbH
gerhard.feske@tuev-sued.de

## *ABSTRACT*

*For supporting security and reliability of supply KELAG Netz GmbH, TÜV Süd AG, the Institute of Power Systems and Power Economics of Aachen University and FGH e.V. developed a certification of control centres and network operation.*
*This paper describes the development process of certification. Furthermore, the main three columns of the requirements of certification process (process management, risk management, requirements on organisation, employees and equipment) are explained and the main benefit of certification for a distribution system operator is illustrated.*

## INTRODUCTION

The increasing interest in ensuring the security of supply and an adequate level of reliability of supply in electricity networks by both customers and regulation authorities motivate network operators to optimize their control centres and network operation due to their substantial influence on these aspects by:

- systematic and as far as possible objective monitoring and evaluation of processes as well as configuration and organisation of control centres and network operation
- external confirmation of these efforts and the results

Therefore, KELAG Netz GmbH – the DSO of the federal state Carinthia in Austria – initiated discussions, whether their control centre could be certified and on which basis [1]. This resulted in a common project with TÜV Süd AG, a leading international service organisation in the field of certification, contributing their experience in national and international standards and certification processes in comparable industry sectors. Furthermore, the Institute of Power Systems and Power Economics of Aachen University (IAEW) and FGH e.V., a research association of German network operators and electrical industry, has been involved serving as a technical expert.

## CERTIFICATION DEVELOPMENT

Due to a lack of subject-specific standards covering all aspects of control centre operation like organisation, technical equipment and operational core processes, a new certificate and a corresponding catalogue of requirements describing a management system have been developed during the project. This catalogue does not only address existing technical specifications in legislation and standards, but also applies well known and introduced methods for the evaluation of industrial processes and assets on the specific characteristics of control centres. Last-mentioned refers to international standards on process management and evaluation as well as on risk management (Figure 1). Moreover, the chosen approach has successfully been transferred to the strategic aspects of network operation, resulting in a corresponding certificate.

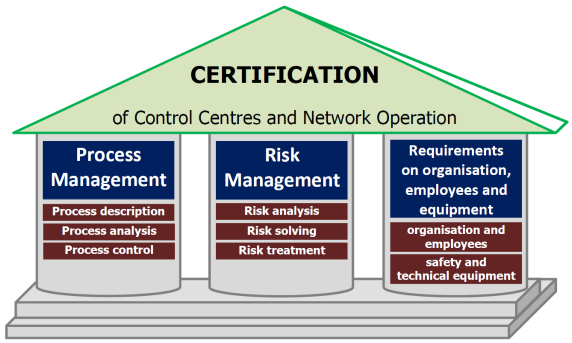


**Figure 1: The three columns of the requirements for the certification**

KELAG Netz GmbH started with the first certification in 2005. Over the last years other DSOs as well as industrial companies have utilized this new process and have been rewarded by certificates.

### Grid and Net Control and Management Standards

The Standard ISO 9001 is recognized as the main and best known determining international standard for process management and continuous improvement cycle (PDCA).

Therefore, main principles of this standard were adopted for the management system related to control centre and network operation. They are in detail:
- process approach
- definition of performance indicators and targets
- internal auditing and management review and by means of this a
- continuous improvement cycle

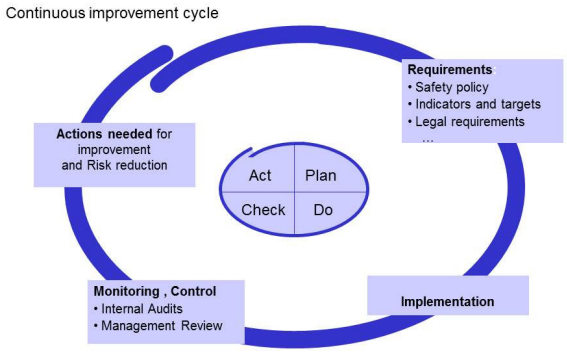


**Figure 2: PDCA Cycle**

Beside of these common aspects there are different aspects as well. While the focus of ISO 9001 standard is mainly quality related, the intention of the certification of control centre and network operations is in detail to enhance reliable power supply or „quality of power supply“ measured by appropriate industry related indicators not by measurement e.g. of customer satisfaction directly. The scope of control centre and network operation management system therefore keeps limited to processes directly related to these activities at the DSOs.
It was the target of this certification to define system requirements for DSOs in particular, not just copying all requirements of the ISO 9001. Moreover, in order to ensure security of supply, which can hardly be measured in any kind of output variable since events threatening that aspect are to be avoided as much as possible due to their major impacts, a process based approach is not sufficient. For that reason special requirements for technical equipment to safeguard operation in control centre and network operation as well as specific guidelines related to organizational structure and personnel have been included. Furthermore, risk management methods have been proven to be suitable for ensuring a sufficient security level, particularly since they are often also obliged for control centres for company overall risk assessments.
Finally, internal audits to check recent performance against control centre standard as well as a management review are proven tools to get transparency in the performance status of continuous improvement.

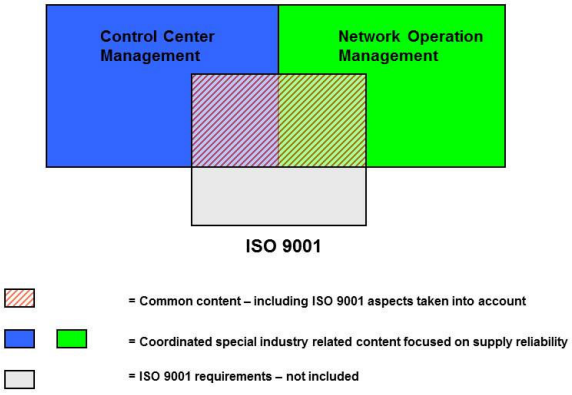


**Figure 3: Comparison ISO 9001-control centre certification**

## PROCESS MANAGEMENT

The processes addressed by the certificate cover all relevant activities inside a control centre as well as security- and reliability-relevant parts of network operation (Figure 4). The classification on management, core and supporting processes as well as the continuous improvement process provided by the management processes is based on classical process management and therefore ensures the compatibility with other management systems of the overall organization. Though, the division into sub-processes, especially as regards core and supporting processes is adjusted to the specific tasks and purposes of control centres and network operation. Moreover, the certification catalogue does not only contain a process description, but also explicit requirements like minimum extent of network monitoring, the central responsibility of the control centre in case of failures, the management of switching authorizations, test procedures for software updates and building and storage of backups.
For the certification of network operation, the regarded processes have been limited to those, that have a direct impact on the quality of supply and belong to the main tasks of a DSO. Therefore, e.g. the daily operation in the field has not been addressed. Moreover, the recording and evaluation of statistical data as a basis for the optimization of operational processes, network design and equipment choice has been defined as a core process with challenging demands in detail like the type and age-specific recording of equipment defects.

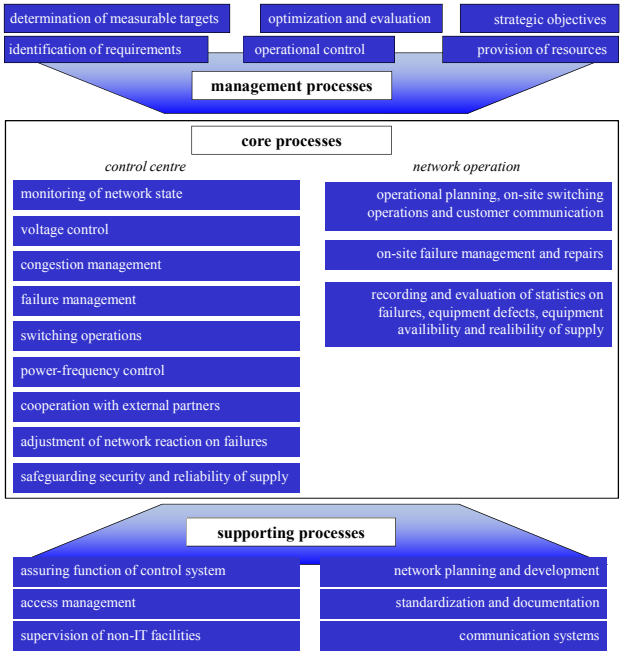


**Figure 4: Overview of processes applied in network control and operation**

All core processes have to be described in-depth by the DSOs. Usually these descriptions can be derived from existing network operation manuals. A new challenge for DSOs is the management of these processes by performance indicators and corresponding targets, since often only a functional evaluation of processes has been carried out. Therefore it is not surprising, that a number of proposed and applied performance indicators by DSOs in fact measure this functionality like the absence of malfunction by personnel or number of faulty demands for switching operations. Nevertheless, during the installation and further improvement of the process management, more quantitative indicators have also been introduced. In most cases this indicators are already calculated or can been derived from existing or for some other reasons also needed monitoring data. Examples are the ratio between network energy losses and distributed energy or the so-called DISQUAL-indices to describe the average reliability of supply in a network. Though, for this kind of indicators it has to be taken into account, that they are not exclusively influenced by network control and operation and subject to probabilistic fuzziness. Thus it is recommended to evaluate trends over a broader time frame and to analyse this indicators in detail.

## RISK MANAGEMENT

Risk management is the second column within the scope of certification of control centres and network operation and is divided into three essential parts:

- Risk analysis (risk identification, cause of risk and evaluation concerning probability of occurrence and consequences)
- Risk solving (strategy)
- Risk treatment (organizational execution of risk management)

For the purpose of **risk analysis** check lists containing all potential risks are developed. As a consequence a systematic coverage of essential risks is ensured. For structured considerations the complex system of a control centre is divided in subsystems. All supply systems and downstream applications (energy supply, air conditioning system, communication systems, etc.) are included in these considerations. For an appropriate risk-evaluation it is necessary to analyse potentially appearing problem cases and to inspect relevant facilities. After the finalized analysis of the possible risks an evaluation of the impact on the total system and/or on subsystems as well as risk identification in the procedure based on process description is necessary.
For structured risk analysis methods like failure impact analysis, fault tree analysis and failure progress analysis are used. The identified risks are evaluated separately and illustrated in a risk cadastre (Figure 5). The position in this risk cadastre is regulated by qualitative evaluation classes. Quantitative evaluation classes are not used because most of the risks are rare events and statistically not measureable, so there would exist a spurious accuracy [2].

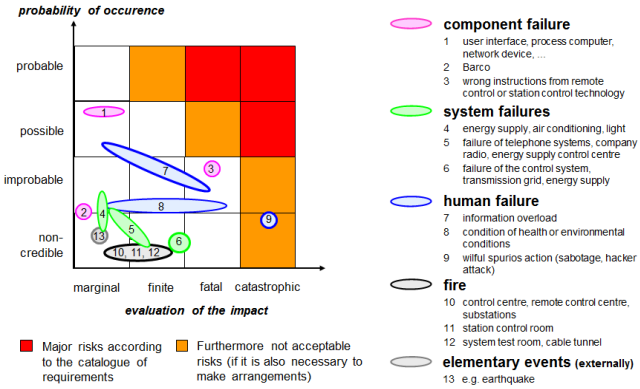


**Figure 5: Example of a risk analysis for control centres**

Furthermore, the impact of risk and probability of occurrence of the particular risk position are evaluated and illustrated. The impact of risk can be divided into the categories marginal, finite, fatal and catastrophic. The probability of occurrence of the risks is divided in non credible, improbable, possible and probable.
Within the scope of **risk solving** in case of risk occurrence, measures are defined for every particular risk in the major risk range (orange and red range in risk cadastre of Figure 5). The complete course of actions for risk solving is listed in the measures catalogue, which is executed and enhanced on a regular basis.
Within the scope of **risk treatment**, a risk analysis is conducted and the risk overview and related sanctions are updated. Measures against risks, which cannot be eliminated immediately, are taken into account of medium term

planning. Risk treatment is also integrated in the company organization and modifications of risks or measures are documented.
Since beginning of certification in the year 2005 a risk optimization was carried out in several sections by applying the risk identification and implementing adequate measures. Furthermore, for risks which cannot be neutralized completely, measure plans were developed. Since beginning of this certification process several measures were carried out for risk reduction.
Tangible measures were implemented in following sections:

- Fire risk was examined by a surveyor and concrete measures were taken
- Personal capacities for occupation of important assets in case of a malfunction of network control system were analysed and preventative measures were taken
- Measures against information overload in the control centre were adopted
- A revision of the access control system was carried out

## REQUIREMENTS ON ORGANISATION, EMPLOYEES AND EQUIPMENT

Reliability and security of power supply is significantly influenced by qualification of personnel involved as well as by the standard of technical infrastructure; means infrastructure related to control centre, supporting equipment and network operations.
Therefore, it is evident that these issues are considered adequately in the new catalogue of requirements for this certification.
Transparency in organizational structure, clear definition of tasks including representatives regulations, regulations for foreign staff as well as selection, qualification and training of personnel are the main issues to be considered and fixed.
In several certified DSO´s TÜV Süd could see that for instance training to safeguard conflict situations and information overload was considered useful.
On the other hand the technical equipment used should be at least equal to „state of the art“. In sense of risk prevention infrastructure e.g. of control centre should ensure that for control centre management essential functions are still running even if one component (hard- or software) failed.
Emergency power supply is just one topic to be checked and evaluated. Talking about risk prevention and security definitely the following infrastructure aspects have been taken into account:
- Access control to the control centre and
- Data security

For several years especially data security gets more and more important and hence has its place in the requirement catalogue for this certification.

## CONCLUSION

For building the new certificate parts of risk- and process-management-systems were used. This composition has proofed to be successful also in reality. The supply guarantee with a high social relevance needs minimum standards. Minimum standards also would be evolvable as a result of risk-management, but in context with certification introduction is easier and comparable quality standards and simplified explanation for third party is ensured.
Due to the security relevance of control centres it is the ultimate ambition to avoid the total loss of grid operations management and also extraordinary failures have to be handled. For ensuring this main functions of control centres implementing a risk management system is absolutely essential.
The coverage of all facilities and processes has proved to be successful for observing all risks and not alone obvious risks.
Based on the experience in the subsequent years the following conclusions were detected:

- Effort for documentation, installation of management processes and first accomplishment of process and risk analyses is limited by already existing organizational structures and internal guidelines.
- Moreover, analyses have anyway to be carried out due to restructuring planning and company-internal risk management and deliver valuable contributions.
- Measures due to high identified risks or unsatisfying processes in the field of the configuration of control centres like fire protection, IT-redundancy and availability of skilled personnel in case of major events were already carried out before the first implementation of the management system. Other aspects like the interface between operational planning and the operation itself – in both control centre and the field – ask for a continuous monitoring and evaluation.
- Structured analysis on the basis of the certification catalogue of requirements and developed procedures and forms enhances the current practice. Further, a regular update is ensured. The current effort for yearly updating the certification system is low and the benefit of an actual documentation is essential. The developed management systems have proved to provide an efficient and practical method for this constant evaluation.

## REFERENCES

[1] Egger H., Stepken A., Haubrich H.-J.: „Zertifizierung von Netzleitstellen”, Energiewirtschaftliche Tagesfragen 56 (2006), 1/2, 44 - 47

[2] Polster J.: „Risikomanagement und Anlagen-management in Elektrizitätsunternehmen“, Graz University of Technology, 2003