# ZONING PRINCIPLES IN ELECTRICITY DISTRIBUTION AND ENERGY PRODUCTION ENVIRONMENTS

Jens-Tobias ZERBST
Vattenfall AB – Sweden
jens.zerbst@vattenfall.com

Erik HJELMVIK
Sweden
erik.hjelmvik@gmail.com

Iiro RINTA-JOUPPI
Vattenfall AB - Sweden
iiro.rinta-jouppi@vattenfall.com

## *ABSTRACT*

*Because of the technological change and increased integration, Industrial Automation and Control Systems (IACS) are more and more exposed to threats which aggravate intentional and unintentional risk scenarios. This paper defines zoning principles for electricity distribution and energy production environments based on a Zone model, assessment methods, and security controls. The zoning principles are designed to mitigate these risks and to enable the secure integration of IACS in business processes according to international standards and best practices.*

## INTRODUCTION

Electricity production, transmission, and distribution operations are increasingly dependent on Industrial Automation and Control Systems (IACS) [1]. IACSs are therefore crucial for a reliable and sustainable operation of this critical infrastructure. At the same time, IACSs in production, distribution or transmission operation environments are increasingly exposed to intentional or unintentional risk scenarios. The increasing risks of IACSs and IACS depending operations are based on the following technological business strategic changes:

- The integration and interconnection of IACS functions in business processes and with business IT systems leads to a neutralization of the strict technical separation between the operation and business IT. This weakens the protection and could have an impact on the stability, availability, and integrity of the operation environment [2].
- Due to cost reduction, performance, and functionality reasons, IACSs are increasingly based on commercial-off-the-shelf (COTS) hardware and software solutions. This leads to a heavy exposure of vulnerabilities with well-known exploits and attack methods.
- Electricity distribution uses an increasing number of IACSs in special distributed computing and intelligent terminal units, due to tightening requirements for quality of supply. This opens up a new kind of controllability, but at the same time new risk scenarios arise.
- Common business IT protection methods, like patch management or antivirus software, can only be applied in a limited way to IACS to eliminate inadvertent consequences. Furthermore IACS environments are not suitable for deployment, management, and maintenance of certain security technologies.
- Many IACS specific protocols, used in current installations, do not have built-in support for security functionality, such as authentication. This leads to inevitable vulnerabilities and threats, which can only be mitigated to a certain degree.
- IACS and associated critical infrastructure become more and more in the focus of generic attackers and public interest, which raises the risk of attacks against IACS [3].
  Information about IACS, IACS installation, and IACS protocols are publicly available and could be easily used for terrorist attacks or cyber warfare [4] sponsored by foreign governments.

Based on these increasing risk scenarios and the potential health, safety, and environmental consequences, governance agencies, industrial communities, and standardisation institutions start initiatives to define rules and the best practice standards to protect IACS and critical infrastructure.

The purpose of this paper is to discuss zoning principles in electricity distribution and energy production environments to enable a secure, practical, and cost-efficient integration of IACS in corporate business processes. The zoning principles define basic principles to implement and follow up security controls to mitigate the described threats and risk scenarios of IACS and the depending operation.

The objective is to develop zoning principles, which are adaptable to existing contexts, compatible to best practice architecture and technology, and compliance to regulations and international standards.

## METHODS

The Zoning principles are based on

- a definition of a 'Defence in Depth' Zone model, which support and are applicable to international standards and requirements
- an assessment and categorization method to classify IACS and IT assets according to the 'Defence in Depth' Zone model
- a method to illustrate different attributes, characteristics, and dependencies of and between the different zones, like responsibilities, business functionality, security requirements, or architecture.
- a method to implement different IT security controls, frameworks, or legal requirements for different zones and to separate them. These controls ensure the

protection of these different services, but also enable the necessary business functionalities.

To guarantee a high grade of adaptability, compatibility, and compliance, the zoning principles including the possible controls were developed and based on fundamental security principles, international standards, and best practice technology architectures.

## Zone principles

The basic structure of the zoning principles is a Zone model, which consists of 6 different zone types. The zones are defined by a logical grouping of assets within an enterprise according to different protection, technological, and business functions levels. All zones are based on proper definition of requirements, controls, and organisational responsibility to meet the security and business goals.

Due to physical, organisational, technical or security reasons, a zone can consists of a number of sub zones or zone instances. A sub zone or zone instance must meet all the requirements of the parent zone.

The Zone model follows the basic segmentation of the Purdue reference model of the IEC 62254-1 standard [5] and the reference model of the IEC 62443-1 standard [6] and is compatible to other segmentations of different standards like IEC 61226 [7].

The Zone model follows the 'Defense in Depth' principle and further fundamental security principles.

### 'Defense in Depth' principle

The 'Defence in Depth' principle introduces a multilayered architecture approach [8] to provide multiple, redundant, and independent layers of protection.

Compared to a simple dual-layered architecture approach, which separate the Corporate IT from the Operation IT, the 'Defence in Depth' principle introduces a higher grade of complexity and cost [9]. Arguments supporting these additional costs and increased complexity are:

- Efficient elimination of single point vulnerabilities or failures in infrastructure or protection components. Deficiency of individual technical or organisational controls regarding error-proneness [10] and vulnerabilities makes a multi layered protection approach necessary.
- Custom fulfilment of different protection requirements in different zones of IACS, IT services, and business functions in an efficient way. The 'Defence in Depth' principle and the use of multiple zones enables the possibility of an accurate separation of the architecture like business function, responsibilities, and technology.
- Flexibility of controls in different zones without weakening the protection level.

### Further security principles

Additionally, the zone principles follow the further security principles in the overall structure as well as in the underlying controls.

- Redundancy-principle: Due to a redundant system design, the failure of a single component will not interfere with the system security functions. The system design shall reduce the likelihood and impact of problems that occur due to, for example, excessive consumption of system resources.
- Protection/detection/response-principle: Controls are implemented which aim to increase protection from, improve detection of, and enhance response to security events.
- Least privilege principle: User and system components only pose the minimal privileges and access rights they need to fulfill their defined function.

## RESULTS

As a result, the zoning principles are described in and consist of a Zone model, classification methods, and security controls. The zoning principles are adapted, compatible, and compliant to best practice architecture and international standards,

## Zone Model

The Zone model consists of 6 general zones.

- Automation: Process (equipment under control), Safety and protection, and Basic control/Local control
- Operation Control: Supervisory control
- Operation Support: Operations management
- Business Support: Business planning and logistics
- Corporate IT: Enterprise IT and common services
- External Integration: Connection and information transfer to external parties

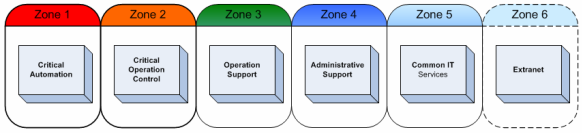


Figure 1: Zone model with 6 zones

## Classification

The classification of IACS and IT systems to a specific zone is based on the defined criteria and requirements of the different zones [11]. A system, which is classified to a certain zone, has to fulfill the specific zone requirements and policies. Special requirements or exceptions can be handled using sub-zones. If a system provides different functions, which are classified to different zones, the system should be assigned to the more stringent zone.

Following criteria and requirements are examples which could be applied. Criteria and requirements are in general a result of the business, security, and technology needs and could therefore be different for different IACSs.

**Business functionality and characteristics**
Separation and mapping from services to the different zones according to business logic and functionality, e.g.

- Coordination or connect functionality with customers, partner or vendors
- Corporate business function
- Business Planning and Logistics including production planning and plant management [12]
- Operations management [12]
- Supervisory control [12]
- Local control [12]
- Process and automation [12]

**Criticality and risk level of services**
Separation and mapping from services to the different zones according to the criticality of the system and risk attributes and levels, e.g.

- Business or society impact by malfunction of the services
- Maintainable unavailability
- Predominant security requirements of the service availability, integrity or confidentiality

**Technological approaches**
Separation and mapping from services to the different zones according to system stack or network design and compatibility, e.g.

- Network protocol, mostly focused on OSI reference model [13] Layer 2 / Layer 3 protocols, and on network architecture
- System protocols and design
- Application protocols and design

**Legal requirements**
Separation and mapping from services to the different zones according to legal requirements or regulations. The assignment to a zone and the underlying controls ensure compliance according to defined legal demands or regulations.

**Responsibility, organizational or physical attributes**
Separation and mapping from services to the different zones or sub zones according to responsibilities, organizational affiliation or physical circumstances. This is a highly organization dependent area.

## Controls

Controls are defined and documented for every zone and for integrations between different zones, to provide separation between the different zones. The controls ensure the compliance of the zone criteria and requirements.
Due to the requirement of adaptability, compatibility, and compliance the zoning principles do not define specific controls or control families. Moreover, the zone principles provide a model to assign specific controls or control families to different zones.

However, the controls shall not be reduced to network controls only, but should cover the different disciplines of IT security [14] to guarantee an integrated protection and follow up. As an example:

- Technical controls, e.g. technical system requirements defined in [15] [16] [17]
- Controls to separate the Zones, e.g. Information flow controls or conduits
- Organizational controls, e.g. responsibilities, function, follow up procedure, change management, incident management
- Physical controls

Security frameworks, legal requirements or international standards can be defined as a basic control rule set to the zones to accomplish compliance, as seen, for example, in the following table.

| | Zone 1 | Zone 2 | Zone 3 | Zone 4 | Zone 5 | Zone 6 |
|---|---|---|---|---|---|---|
| NERC CIP-002-1-CIP-009-1 [18] | X | X | X | | | |
| NIST SP 800-82 [17] NIST SP 800-53 [19] | X | X | X | | | |
| IEC 62443 series [20] ISA-99 series [21] | X | X | X | | | |
| IEC 62264 [22] | X | X | X | X | X | |
| IEC 61226 [7] | X | X | | | | |
| VGB R175e [23] | | X | X | | | |
| ISO/IEC 27000 series [24] | | | X | X | X | X |
| COBIT [25] | | | X | X | X | X |
| ITIL [26] | | | X | X | X | X |

Table 1: Assignment examples of different industrial standards, regulations, and security frameworks to the different zones

## CONCLUSION

The electricity production and distribution sector is now, more than ever, facing the challenge of technological development of IASC as well as the business demands of further integration. To ensure an efficient, applicable, and secure way to fulfil these upcoming requirements, the Zone model provides a transparent view on the IT architecture of an energy company and points out necessary controls according to the different requirements and system design.

## REFERENCES

[1] DRAFT IEC 62443-1, 2008, “Industrial communication networks - Network and system security Part 1 Terminology, concepts and models”, *7 et sqq.*

[2] Brian Krebs, 05.06.2008, “Cyber Incident Blamed for Nuclear Power Plant Shutdown”, online http://www.washingtonpost.com/wp-

dyn/content/article/2008/06/05/AR2008060501958.html

[3] Ganesh Devarajan, 2007, "Unraveling SCADA Protocols: Using Sulley Fuzzer", *Defon 15 conference*

[4] Greg Bruno, 27.02.2008, "The Evolution of Cyber Warfare", *Council on Foreign Relations (CFR)* , online http://www.cfr.org/publication/15577/

[5] IEC 62254-1, 2003, "Enterprise-control system integration – Part 1: Models and terminology", *185 et sqq.*

[6] DRAFT IEC 62443-1, 2008, "Industrial communication networks - Network and system security", *53et sqq.*

[7] IEC 61226, 2005, "Nuclear power plants - Instrumentation and control systems important to safety - Classification of instrumentation and control functions"

[8] Chad Perrin, 2008, "Understanding layered security and defense in depth", online http://blogs.techrepublic.com.com/security/?p=703

[9] Eric Byres, 2008, "Defense in Depth", *Control Engineering Asia June 2008,* online http://www.ceasiamag.com/article-4191-defenseindepth-Asia.html

[10] Avishai Wool, 2004, "A Quantitative Study of Firewall Configuration Errors", *IEEE Computer June 2004, 62 et sqq.*

[11] NIST 800-60 Volume II Revision 1, 2008, "SECURITY CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS", online http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

[12] DRAFT IEC 62443-1, 2008, "Industrial communication networks - Network and system security", *65et sqq.*

[13] ISO 7498-2, 1989, "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture"

[14] GAO, 2008, "Recommendations for Executive Action", TVA Needs to Address Weaknesses in Control Systems and Networks, pp. 42-43, online www.gao.gov/new.items/d08526.pdf

[15] Idaho National Laboratory, 2006, "Control Systems Cyber Security: Defense in Depth Strategies", online http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

[16] BDEW, 2008, "White Paper Requirements for Secure Control and Telecommunication Systems"

[17] NIST SP 800-82, 2008, "DRAFT Guide to Industrial Control Systems (ICS) Security", online http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

[18] NERC Cyber Security standards, 2006, CIP-002-1-CIP-009-1

[19] NIST SP 800-53, 2007, "Recommended Security Controls for Federal Information Systems", online http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

[20] DRAFT IEC 62443, 2008, "Industrial communication networks - Network and system security"

[21] ANSI/ISA-99, 2007, "Security for Industrial Automation and Control Systems"

[22] IEC 62264, 2003, Enterprise-control system integration.

[23] VGB R175e Richtline, 2006, "IT Security for Power Plants"

[24] ISO/IEC 27000 series, 2005, "Information technology - Security techniques - Information security management systems - Overview and vocabulary"

[25] ISACA, 2007, Control Objectives for Information and related Technology 4.1 (COBIT), online http://www.isaca.org

[26] United Kingdom's Office of Government Commerce (OGC), 2008, Information Technology Infrastructure Library (ITIL) V3