ISSN 0280-5316
ISRN LUTFD2/TFRT--5795--SE

# Implementation of IS Security Standards on Pharmaceutical Manufacturing

Gustaf Gerge

Department of Automatic Control
Lund University
June 2007

**Lund University**
**Department of Automatic Control**
**Box 118**
**SE-221 00 Lund Sweden**

*Document name*
MASTER THESIS

*Date of issue*
June 2007

*Document Number*
ISRNLUTFD2/TFRT--5795--SE

*Author(s)*
Gustaf Gerge

*Supervisor*
Joakim Moby at AstraZeneca in Södertälje
Charlotta Johnsson at Automatic Control in Lund
(Examiner)

*Sponsoring organization*

*Title and subtitle*
Implementation of IS Security Standards in Pharmaceutical Manufacturing (Implementering av IS säkerhetsstandarder i läkemedelstillverkning)

*Abstract*

This thesis addresses the issue of Information Systems (IS) security in pharmaceutical manufacturing which is closely related to the ISA 99 standard. The ISA 99 “Security for industrial Automation and Control Systems” standard is focused on the work for securing process automation systems from IS security threats. The main thought behind the ISA 99 standard is that a high level of IS security in computerized manufacturing environments cannot be achieved through just one project but needs long-term dedication. Therefore the ISA 99 standard suggests the implementation of an IS security program as the best way to reduce IS security risks to process automation systems and to sustain risk reduction over time. The overall objective of the study was to suggest an IS security program suitable for the pharmaceutical manufacturing at the AstraZeneca manufacturing and supply site in Södertälje, Sweden. The suggested IS security program can briefly be described as a long-term strategy for how to perform IS security activities in the manufacturing at the Södertälje site. The security program defines both technical and organizational requirements and recommendations. According to the ISA 99 standard, working with IS security in the process automation systems environment require both technical, cultural and organizational perspectives. The suggested security program therefore recommends the forming of a special group for working with IS security in the manufacturing within Sweden Operations. This group includes employees from different departments such as IS security, IS/IT, process automation systems managers, engineering, operators and managers in production areas as well as quality assurance personnel. The purpose with the group is to make the IS security work more effective through reducing bureaucracy, increasing communication and sharing of knowledge and business perspectives. The security program also presents IS security policies for the production at the Södertälje site. A security policy is a written document or directive that defines how the organization defines and operates IS security in the process automation systems environment. The security policy ensures both management support and understanding of roles and responsibilities for IS security in the process automation systems environment.

*Keywords*

*Classification system and/or index terms (if any)*

*Supplementary bibliographical information*

*ISSN and key title*
0280-5316

*ISBN*

*Language*
English

*Number of pages*
146

*Recipient’s notes*

*Security classification*

http://www.control.lth.se/publications/

# Acknowledgements

I have been very fortunate during this work having the best possible supervisors. Without the strong support and excellent supervision this thesis would most likely never have finished. Hopefully more students will benefit from your distinct leadership, inspiration and pedagogical skills.

Special thanks to Jessica Lindquist, Anna Östh, Tomas Ersson, Christer Gottschalk, Göran Guné, Joacim Holmgren, Patrik Stensson, Anders Wickman, Mikael Björklund, Henrik Carnborg, Robert Järn and Gunilla Norström for support, interesting discussions and nice coffee breaks.

Thanks to my family and friends for support and inspiration.

Gustaf Gerge, Södertälje, June 2007

# Table of Contents

# 1 Introduction

## 1.1 Executive summary

This is the official report from master thesis work performed spring 2007 for AstraZeneca Sweden Operations in Södertälje, Sweden.

The study addresses the problem of Information Systems security (IS security) in the computerized systems used for manufacturing of pharmaceuticals within Sweden Operations. The thesis work was performed at the Södertälje site and was supervised by the Sweden Operations Information Technology (OIT) department and the Department of Automatic Control, Lund University, Sweden. The work is closely connected to the ISA 99 and also the ISA 95 standard.

The main thought behind the ISA 99 standard is that a high level of IS security in computerized manufacturing environments cannot be achieved through just one project but needs long-term dedication. Therefore the ISA 99 standard suggests the implementation of an IS security program as the best way to reduce IS security risks to process automation systems and to sustain risk reduction over time.

The overall objective of the study was to suggest an IS security program suitable for the pharmaceutical manufacturing at the AstraZeneca manufacturing and supply site in Södertälje, Sweden. The suggested IS security program can briefly be described as a long-term strategy for how to perform IS security activities in the manufacturing at the Södertälje site. The security program defines both technical and organizational requirements and recommendations.

All production of pharmaceuticals within Sweden Operations is performed through batch manufacturing. The manufacturing is dependent on a variety of different processes and equipment and can briefly be described to consist of two main steps. Manufacturing of API (Active Pharmaceutical Ingredients) and manufacturing of drug product pharmaceuticals such as tablets, capsules or Turbuhaler devices (inhalators for respiratory diseases). The API is the substance in the drug that is intended to actively cure the consumer.

The manufacturing of API uses Distributed Control Systems (DCS) for control of the process equipment. The manufacturing of drug product pharmaceuticals mainly use process equipment with Programmable Logic Controller (PLC) systems. The DCS and PLC systems are monitored from Supervisory Control and Data Acquisition (SCADA) systems. A SCADA system is basically a PC that also collects production data such as sensor trend data, and alarms and events from the DCS and PLC systems. These systems are commonly known as process automation systems.

Due to regulatory requirements and the increasing business demands for sharing both real-time and other information within Sweden Operations, the process automation systems are becoming more and more connected to the AstraZeneca corporate network. With the increased connectivity to corporate networks and the use of commercial operating systems on SCADA clients, like Microsoft Windows, the process automation system becomes as vulnerable to IS security threats as normal office computers.

Most of the process automation systems at the Södertälje site are today connected to the DELTA network. The DELTA network is an internal network that interconnects different production area networks with the AstraZeneca corporate campus network (here named GAMMA) at the site. The DELTA network utilizes an architecture that is built upon the use of a demilitarized zone together with physical and logical network segmentations of the different production area networks. The systems and networks in the production of pharmaceuticals at the Södertälje site are presented in more detail in chapter 4.

The intention with the DELTA architecture is to provide process automation systems with a secure environment, while still connected indirectly to the corporate campus network. The DELTA architecture is segmented according to global AstraZeneca IS security standards. Other AstraZeneca sites that are building and operating site networks might therefore find this study as a contributing source in their IS security compliance work.

The first conclusion of the study is that the DELTA architecture and implemented IS security measures comply with global AstraZeneca IS security standards and recommendations. DELTA and the implemented IS security level also complies with to this date available and relevant industrial IS security standards concerning network architecture and IS security in the context of process automation systems. There are possibilities for improvements on local process automation systems in the different production areas at the Gärtuna and Snäckviken sub-sites.

The second conclusion of the study is that the most severe IS security risk that threatens the process automation systems at the Södertälje site are:

- An unknown virus from the corporate network (GAMMA) or the Internet, that the anti-virus in EPSILON (the demilitarized zone in the DELTA network) can resist, with major impact on all the different networks and production areas within the DELTA network (known as a Day zero scenario).

- An IBM error that have major effects on both the DELTA network and the production area networks. Sweden Operations have outsourced the operation of the DELTA network to IBM.

- Non-validated updates or patching of infrastructure services or network equipment prevents friendly communications or network services in the DELTA network.

- Major virus infection from system providers in a production area network with PLC based process automation systems.

- Major virus infection from direct-dial up access in a production area network with PLC based process automation systems.

- Major incident due to remote access through a direct-dial up connection in a production area network with PLC based process automation systems.

- Major incident due to virus outbreak from a non-standard SCADA client in a production area network with PLC based process automation systems.

The built in architecture and IS security safeguards address most of the identified threat scenarios, except for the Day zero scenario. The Day zero scenario potential is well known to the site Local IS security managers. This report provides suggestions for improvements for reducing the severity of these risks.

The third conclusion of the study is that the main IS security risks with the possible implementation of a MES/EBR system within Sweden Operations are:

- The scenario where the MES system malfunctions or becomes infested with a virus

- The scenario where EBR critical systems becomes unavailable or infested with a virus

- Increased wireless network vulnerabilities in the DELTA network

- Wiretapping of information in the DELTA network

- Problems with software for automatic validation of batches

- Problems with electronic storage of records and traceability of batches

The two first risks might force the production to undesired halts. Due to these risks, a conservative suggestion is to operate the MES/EBR system from inside the DELTA network. The implementation of a MES/EBR system and connection of a wireless network to the DELTA network demands thorough IS security risk assessment.

Finally the study presents an IS security program or strategy suitable for the IS security work in the DELTA network and the operation process automation systems used within the Södertälje site. The structure of the security program is based on the ISA 99 ‘Manufacturing and Control Systems Security’ standard. The ISA 99 standard is today one of the most referred IS security standards in the process automation systems area. The main thought behind the IS security program is to simplify communications and increase the sharing of knowledge in order to increase the effectiveness in the IS security work within the production of pharmaceuticals and operation of process automation systems at the Södertälje site.

## 1.2 AstraZeneca

AstraZeneca is one of the worlds leading pharmaceutical companies. The company is dedicated to the discovery, development, manufacturing and marketing of high quality, effective prescription medicines that bring benefit for patients and add value for shareholders and wider society.

AstraZeneca is a British-Swedish company with a global presence and enterprises in over 100 countries. The companies has a turnover of $26 billion and 66 000 employees. The main medical areas are cancer, cardiovascular, gastrointestinal, infection, neuroscience and respiratory and inflammation. [1]

AstraZeneca Sweden employs 12800 in research (R&D), production (Operations) and marketing (ISMO). There are sites in Lund, Mölndal, Södertälje and Umeå. The sites in Lund and Mölndal are R&D sites. The site in Södertälje is used for both R&D and manufacturing of pharmaceuticals. AstraZeneca global R&D headquarters is also located at the site in Södertälje. The site in Umeå is mainly used for packaging of already prepared pharmaceuticals. [22]

### 1.2.1 AstraZeneca Sweden Operations

The division for production and manufacturing of pharmaceuticals within AstraZeneca is Operations. Operations is the link between R&D and ISMO within AstraZeneca. The mission for Operations is to effectively produce pharmaceuticals and to provide the healthcare in different countries with valuable pharmaceuticals. The main objectives are manufacturing of active pharmaceutical ingredients (API), production and packaging of the end product and quality control. [1]

The Swedish part of Operations is called AstraZeneca Sweden Operations. Sweden Operations employs about 5000 and operate the sites in Södertälje and Umeå. 6 out of 10 of AstraZeneca globally most sold product are produced by Sweden Operations. This includes well-known products like Nexium, Losec and Turbuhaler. [22]

The Södertäje site is divided into two sub-sites, the Gärtuna site and the Snäckviken site. The Gärtuna site is mainly dedicated for tablet production. The site has the largest pharmaceutical tablet and capsule production plant in the world. The Snäckviken site is mainly used for manufacturing of API, liquid pharmaceuticals and Turbuhaler pharmaceuticals. [22]

API is for Active Pharmaceutical Ingredients. The API is the part of the pharmaceuticals that is intended to actively cure or counteract a disease or symptom. The API is the basis of all other pharmaceuticals. Liquid pharmaceuticals are products that are provided to patients in liquid and intravenous forms. Turbuhaler products are consumed through breathing in the pharmaceuticals through a special device.

### 1.2.2 Sweden Operations Information Services (OI)

Information Services is the department within Sweden Operations that provides support and services for information systems and information technology (IS/IT). OI has 80 employees at the Södertälje site.

The mission for OI is to provide solutions for IS/IT in a way that creates value for Sweden Operations. The vision is to work proactively and to work together with the different departments within Sweden Operations in a way that ensure that IS/IT improvements and solutions are realized. The goal is to make sure that IS/IT is used in an optimal and effective way within Sweden Operations. [39] [43]

OI is responsible for providing network services and assuring that a satisfying level of IS security is maintained within Sweden Operations and in the production of pharmaceuticals at the Södertälje site.

## 1.3 Problem formulation

Sweden Operations is continuously aiming to become a more effective and integrated organization. The need for sharing both real-time and other information within Sweden Operations and also with other AstraZeneca companies is an important success factor. Due to regulatory compliance requirements there is also a need for efficient storage of electronic records from the production. Therefore the presence and integration of computerized systems on all levels in the production of pharmaceuticals is increasing continuously and more and more manufacturing systems are being connected to the AstraZeneca corporate network. [44] [39]

These systems cover all areas within the manufacturing, from order handling and information collection, down to process control and automation systems (process automation systems). With the increased hierarchical integration, increased network connectivity and implementation of modern automation equipment comes both benefits and problems. Benefits include possibilities to monitor the production in real-time and possibilities for cost reductions through more efficient logistics, more efficient production processes and increased product quality. One of the major problems is to maintain a high level of IS security on the process automations systems used within the manufacturing of pharmaceuticals. [7] [5] [13]

Standard office computers are protected against IS security threats by firewalls, updates to the operating systems and the use of anti-virus software. Many process automation systems are today delivered with computers that use standard operating systems like Microsoft Windows. Some process automation systems vendors provide control systems that use custom made operating systems or old standard operating systems. These operating systems were built with the intention of being used for automation and control equipment and might focus on real-time control and process reliability or are not supported with security upgrades. They were not built for resisting computer viruses or attacks from computer hackers. Therefore they might lack proper protection against virus infections and hostile intrusion. [8] [13]

The manufacturing of pharmaceuticals is highly regulated and all equipment used in the production must be validated according to different regulations that are transformed into rules and policies within Sweden Operations. The validation assures that the products are manufactured in a way that does not jeopardize the health of the consumers. The validation also assures that all products are traceable so that defect products always can be removed from the market. This means that if software on a process automation system is changed, updated or patched in some way, the equipment and system has to be revalidated. Validation is a costly and time-consuming process that also might halt the production. Changing parameters on a process automation system might also invalidate support and warranty agreements with the vendor of the process automation system. The result of this is that a high level of IS security on the process automation systems either cannot be maintained or is very costly to maintain. [21] [53] [54] [32]

With the connection to the corporate network comes a connection to the Internet. On the Internet lurk a variety of different threat sources like computer viruses, hackers, activists, terrorists and dubious organizations and companies. The manufacturing of pharmaceutical is generating large revenues, involves a lot of business secrets and due to the use of animal testing is of some people considered as non-ethical. This makes the process automation systems used in pharmaceutical manufacturing a vulnerable and legitimate target for IS security threats. Modern operating system enables easy connection of portable computer equipment like USB memories and CD-ROM discs. This also makes both intentional and unintentional injection of virus on process automation system a very present and possible threat. [6] [24]

Thus maintaining a high level of IS security in this environment without interfering with the production is an important challenge for both Sweden Operations and Sweden Operations Information Services. Due to historical, technical and risk assessment reasons the different process automation systems used at the Södertälje site have different standards and rules for IS security. Therefore there is need for an overall strategy or program for IS security for these systems. Furthermore, the strategy must make it easy to install new systems, and should therefore follow industrial standards. One of the most referred and accepted IS security standards for IS security in process automation systems is today the ISA 99 standard. [14]

## 1.4 Objectives

*The overall objective of the study is to suggest a recommended overall IS security program suitable for the systems used for pharmaceutical manufacturing at the Södertälje site. The program must comply with the ISA 99 standard.*

In order to provide a background for the IS security program the first step is to evaluate the implemented IS architecture, the present IS security level and implemented IS security measures. The second step is to identify the most severe IS security risks that are present to the process automation systems and connect this to financial aspects to provide a business case background to the IS security program.

The goal is also to suggest important improvements for IS security measures on process automation systems and to connect the work to relevant business aspects. The work should be made in connection to relevant available guidelines and industry standards for IS security in manufacturing systems with focus on architecture and network aspects.

The ongoing installation of MES/EBR (Manufacturing execution system/Electronic batch records) components should also be taken into consideration. Therefore the objective is also to investigate how the implementation of a new MES/EBR system have impact on the IS security level in the production at the Södertälje site.

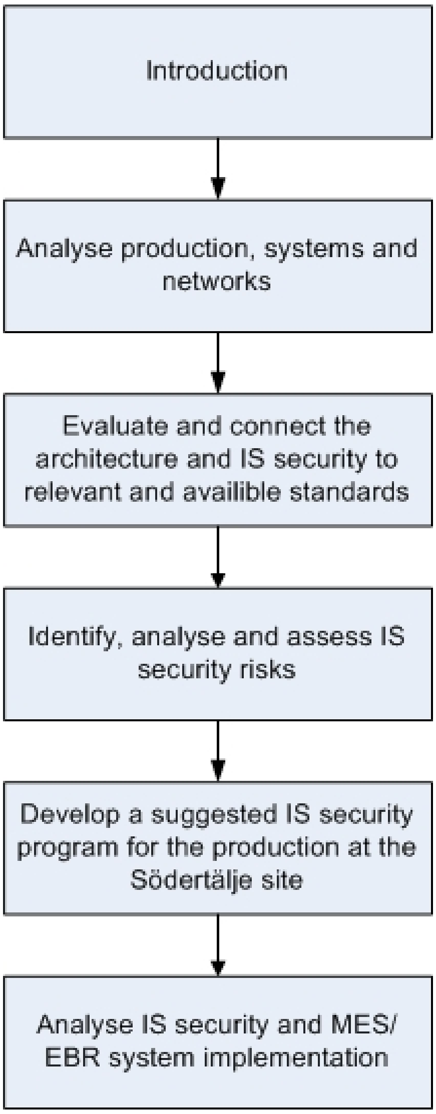

Introduction
Analyse production, systems and networks
Evaluate and connect the architecture and IS security to relevant and availible standards
Identify, analyse and assess IS security risks
Develop a suggested IS security program for the production at the Södertälje site
Analyse IS security and MES/ EBR system implementation

*Fig. 1.1 Problem formulation*

## 1.5 Production areas used in the study

At the Södertälje site there are numerous production plants and areas. To limit the study two production areas were chosen to represent the IS security context within pharmaceutical manufacturing at the site. The production areas used in the study was chosen in order to be of strategic importance for Sweden Operations, in order to be suitable in an IS perspective, in order to be suitable in a technical perspective and finally for practical reasons.

The product areas cover Active Pharmaceutical Ingredients (API) production and tablet production and thus in principal includes all the general production steps and the different automation equipment (DCS and PLC systems) that is used in the manufacturing of pharmaceuticals at the Södertälje site.

The production area used for manufacturing of API is the ALFA plant at the Snäckviken sub-site. [34]

The production area used for analysing IS security in manufacturing of tablets is the BETA plant at the Gärtuna sub-site. [42]

## 1.6 Key assumptions and delimitations

### 1.6.1 Limitations of studied natural threats and Lab aspects

The risk analysis part of the study is limited to scenarios that are induced by the threats described in the theory chapter, Wiretapping and scanning of the network, malicious code, human errors and Interference of systems and communications. Therefore physical or natural threats in the form of cables being dug up, burglary and natural events including storms, earthquakes, floods, and tornadoes are generally considered as outside the scope of the study. The physical threats and aspects of IS security are considered but not addressed and analyzed in the study.

The lab systems in the production at the Södertälje site have not been studied in detail during the study. Early in the study it was concluded that the lab systems maintain a satisfying IS security level and have limited impact on the production in the scenario of IS security incidents. Therefore the focus has been on production area systems and networks.

### 1.6.2 Practical limitations

Due to the scope of the study and for practical reasons, all systems and networks used in the production of pharmaceuticals within Sweden Operations are not investigated and observed in detail. The scope of the study is more focused on the management and support level of IS security than on technical system and network issues. The large amount and great complexity of the systems and networks within Sweden Operations also makes it impossible to perform a detailed study of all the different production areas, networks and systems.

### 1.6.3 Umeå site connection

The DELTA network today connects to the Umeå site. This study assumes that this connection not exists. Due to upcoming downsizing within Sweden Operations the site might be closed in a near future. [26]

## 1.7 Definitions and information for the reader

This section provides some useful definitions and information to increase the reading value of this report. For more definitions, please refer to the ISA 99 standard, Part 1 ‘Concepts, Terminology and Models’. [13]

### 1.7.1 Process automation systems

A system collection of hardware and software that can affect or influence the safe, secure and reliable operation of an industrial process.

These systems include, but are not limited to; industrial control systems, including distributed control systems (DCS), programmable logic controllers (PLC), remote terminal units (RTU), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. [13]

Associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing information systems (MIS), manufacturing execution systems (MES), plant information management systems, associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to batch processes are also included in this definition. [13]

Systems operated from the corporate network are outside of the scope of the study.

### 1.7.2 Information systems (IS) security

The ISA 99 standard refers to information systems security as cyber security. This study utilizes the term information systems security. The objective of IS security measures is to preclude; unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets in an effort to reduce the risk of causing personal injury or endangering public health, losing public or consumer confidence, disclosing sensitive assets, failing to protect business assets or failing to comply with regulations. [13]

This includes the concepts of identification, authentication, accountability, authorization, availability, and privacy of information systems. These concepts are applied to any system in the production process and include both stand-alone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control or exchange data with any of these control systems. [13]

*The terms IS security and security have in general the same meaning in this report. The term security has a somewhat broader meaning including more physical and natural aspects.*

### 1.7.3 Demilitarized zone (DMZ)

A demilitarized zone is a perimeter network segment that is logically between internal and external networks. The purpose of a demilitarized zone is to enforce the internal network’s policy for external information exchange and to provide external, untrustworthy sources with restricted access to releasable information while shielding the internal network from outside attacks. In the context of industrial automation and control systems, the term ‘internal network’ is typically applied to the network or segment that is the primary focus of protection. For example, a process automation systems network could be considered ‘internal’ when connected to an ‘external’ business network (here known as a corporate network). [13]

A Day zero scenario occurs when the demilitarized zone is severely infected with a virus. If the demilitarized zone is infected the virus will easily spread to all connected ‘internal’ networks since they maintain a lower level of IS security than the demilitarized zone.

### 1.7.4 Hardening of computer systems

Hardening of computer systems is the process of securing a system. This work is especially done to protect systems against potential attackers and intrusion. This includes removal of unnecessary usernames or logins and the disabling or removal of unnecessary services or applications. This may also involve, among other measures closing open USB, CD-ROM and floppy drive ports and network ports, setting up intrusion-detection and prevention systems, firewalls and a higher level of password IS security..

In this study hardening also includes the process of patching operating systems and use of anti-virus software against malicious codes, and ensuring that the possibility for an operator or user of a process automation system, to intentionally or unintentionally abuse the system is minimized. [31]

### 1.7.5 Outsourcing of IT infrastructure and services to IBM

In 2001 AstraZeneca signed a global outsourcing agreement with IBM for providing IT infrastructure and service. For Sweden Operations this creates a complex management system for management of systems, computer equipment and networks. The person or organization within Sweden Operations that is responsible for a system or a 'service', 'owns' and define the requirements the system or service must meet. Based on the requirements, IBM delivers the operating software, applications and the hardware that is necessary for the system or service. The third part in this management system is the IT services department. IT services is an AstraZeneca function that basically is responsible for ensuring that IBM delivers what is agreed. IT services also provide expert knowledge and different support services to Operations, R&D and other AstraZeneca functions.

There are of course a lot of deviations from this model. For example, for some systems used in the production, IBM only provides standard PC clients and network equipment and not the control equipment or the control software used in the process automation systems. Other systems and networks in the production are not provided by or maintained at all by IBM. These systems also have a system owner, a system manager and a system service provider but are not using IBM. This makes the network and system architecture within Sweden Operations very complex to analyze and model.

Common to all systems and networks are that they have a system owner, system manager and system providers. The system owner is responsible for the system and defines the properties of the system. The system manager is responsible for governing the system and the service provider enable or deliver the actual system.

## 1.8 Disposition

**Chapter 1 – Introduction**
The background and the objective of the study.

**Chapter 2 – Theory**
Provides the theoretical background that form the basis for the study including standards, IS security background and regulatory aspects.

**Chapter 3 – Methodology**
Describes the methodology that was used for performing the study and the tools for IS security risk analysis.

**Chapter 4 – A reference architecture for the DELTA context**
Systems and networks used in the production are presented together with a suitable reference architecture for the DELTA context.

**Chapter 5 – Evaluation of the DELTA architecture and IS security level compliance**
This chapter evaluate the DELTA architecture and the IS security safeguarding efforts that are present to the manufacturing of pharmaceuticals at the Södertälje site. The work is performed through connecting to current available IS security standards.

**Chapter 6 – Identification and analysis of IS security risks**
A complete IS security analysis of the reference architecture is conducted to provide suggested improvements and a background for an IS security program.

**Chapter 7 – DELTA ISA 99 security program**
A suggested IS security program for the DELTA context. The structure of the program is based on the ISA 99 standard.

**Chapter 8 – MES/EBR implementation and IS security**
This chapter briefly discuss how the implementation of a MES/EBR system affects the IS security level in the DELTA network. Some suggestions for the implementation are provided.

**Chapter 9 – Conclusions**
Presents the main conclusions in the study and some input for future work, investigations and research.

**Chapter 10 – References**
Information sources used in the study.

# 2 Theory

## 2.1 Overview

The theoretical background of the study is mainly based on ISA standards, AstraZeneca and various national standards, guidelines and policies. The standards and guidelines address IS security in relation to process automation systems.

Criterions for evaluating IS security and the network architecture as well as possible IS security threats and agents are also presented in this chapter. The last part of the chapter provides a brief picture of the regulations that have impact on the process of manufacturing pharmaceuticals.

## 2.2 Standards, guidelines and policies

### 2.2.1 ISA 95 Enterprise-Control System Integration

The ISA 95 Enterprise-Control System Integration standard is a technical standard that defines the interface between enterprise activities and control related activities in a company. The Standard addresses the functional hierarchy in a manufacturing company and the interconnection between the different functions. The goal is to improve the effectiveness in manufacturing by having enterprise systems and manufacturing systems that inter-operate and easily integrate. In this study ISA 95 is mainly used for providing a hierarchical model to increase the visibility of the different computer systems and networks that are involved in the study. [12]

### 2.2.2 ISA 99 Security for industrial Automation and Control Systems

The ISA 99 Security for industrial Automation and Control Systems standard address the rising problem of security in industrial automation and control systems. The standard focus on electronic security (also known as IS or cyber security) for these systems. The standard focuses on level 0 through 3 of the ISA 95 hierarchical model (section 2.3). Level 4 and above are not explicitly addressed but the integrity of data exchanged between level 3 and above are considered. The standard is still being developed and will consist of four parts. At present and unfortunately, only part one and two are close to being published. Part 1 address concepts, terminology and models related to cyber security (IS security). Part 2 address how to establish an industrial automation and control systems security program. In this study ISA 99 provides a background and framework for modelling and analysing IS security in process automation systems. The standard is also used as framework for developing an IS security program. [13] [14]

There are also two ISA 99 Technical reports available. These are used in the study to provide technical guidance, ideas and suggested improvements for IS security. [15] [16]

### 2.2.3 AstraZeneca documents

The AstraZeneca policy document Mandatory Standards and Good Practice for the Security of Process Automation Services is a global Operations policy document for how to implement security in the company's process automation systems. The AstraZeneca guideline Secure Network Isolation of Process Automation Computer Systems form a deeper background to the document above and complement with guidelines for a recommended system architecture for process control networks and systems. Both documents are composed by the AstraZeneca Global Automation Strategy Team (GAST). The documents are described in more detail below. [31] [32]

Except for the GAST documents, numerous AstraZeneca routines (RUT), standard operating procedures (SOP), Beskrivning av datoriserat system (BaDS) (English: Description of computerized system) and other AstraZeneca documents, are also used for various purposes within the study. Many AstraZeneca documents are confidential.

### 2.2.4 NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks

The NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks is a document published by the Centre for the Protection of National Infrastructure in UK. NISCC is for the National infrastructure security co-ordination centre (UK). The document discusses firewalls; common process automation networks segregation architectures and firewall implementations, configuration and management. The document is here mainly used for discussing process automation networks segregation architectures. Eight different approaches for segregation of process control and automation systems are presented and evaluated after three criteria's; security, manageability and scalability. The document also discus some special or future technologies, that might be of interest for the research area. The document is widely referred to in research papers and documents that are of interest for the scope of this study. [17]

### 2.2.5 NIST Guide to Supervisory Control and Data Acquisition (SCADA) and industrial Control Systems Security

The NIST Guide to Supervisory Control and Data Acquisition (SCADA) and industrial Control Systems Security is a document with recommendations from the National Institute of Standards and Technology (NIST), USA. The document provide an overview of industrial control systems and the IS security threats and vulnerabilities of such systems. It discusses IS security program development and deployment for such programs. It also discusses network architectures and IS security controls for industrial control systems. The document is in this study mainly used to provide ideas for suitable network segmentations. [18]

### 2.2.6 DHS Control Systems Cyber Security: Defence-in-depth strategies

Control Systems Cyber Security: Defence-in-depth strategies is a document from the department of Homeland Security (DHS), USA. The document provides information about current IS security challenges for SCADA and control systems. The intention with the use in this study is to evaluate the defense-in-depth capability of the architecture and IS security measures that are implemented, example shown in figure 2.1. The defence-in-depth strategies are presented as the use of: [11]

- Firewalls

- Creation of demilitarized zones (DMZ)

- Intrusion detection and prevention systems

- Security policies

- Security training

- Incident response capacity

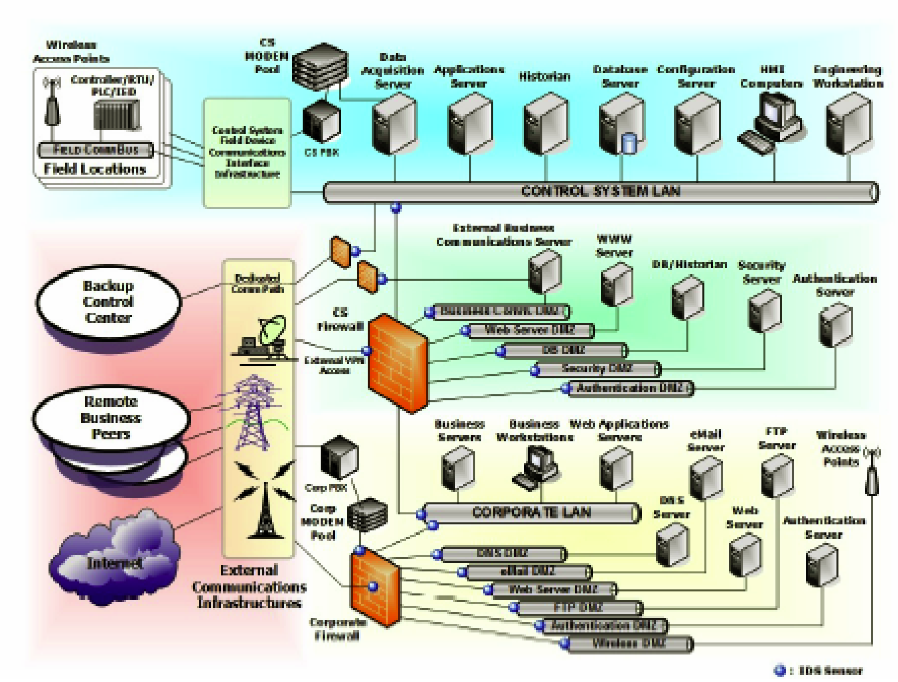


*Fig 2.1 Example of defence-in-depth strategy architecture (copyright © DHS)*

### 2.2.7 AstraZeneca Secure Network Isolation of Process Automation Computer Systems

The purpose of this AstraZeneca Operations document is to ensure the continuity of the process automation infrastructure in the event of a network-based security incident, by describing an approach and set of principles to the networking of process automation systems. The intention is to provide a high degree of protection against incidents in a specific automation system as well as against incidents in the AstraZeneca network infrastructure. The document consists of both mandatory and guiding principles for the implementation of process automation systems and networks.

The document uses a terminology that defines every kind of equipment that connects to, and communicates via, the local site network as a device. A device can be a server, workstation, and process automation or network equipment. The term segment is used for defining a set of devices that communicate with each other but connects to the rest of the network through a device that controls the communication in a desired way.

The fundamental part of the guideline is to divide the whole AstraZeneca network and devices into different classes according to the level of protection. The size and complexity of the AstraZeneca network makes it impractical to implement the same level of protection and IS security in all parts of the network.

*The devices are therefore divided into GOLD, SILVER and BRONZE classes. GOLD network segments contain only GOLD devices. SILVER network segments only contain devises with at least SILVER protection. All other segments are designated BRONZE.*

Devices connected to GOLD have in-support software versions, implement all AstraZeneca standards and have full and up-to-date patching of operating systems and up-to-date anti-virus protection. New patches are applied to GOLD devices as the highest priority within hours of release and through automated processes if possible. Devices that are critical to the operation of the corporate and internal networks are maintained as GOLD devices.

Devices connected to SILVER have in-support software versions, implement all AstraZeneca standards and have full and up-to-date patching and anti-virus protection. Application of new patches takes a longer time due to the number and diversity of devices involved.

BRONZE connected devices do not fully apply to global AstraZeneca IS security standards. Patching and anti-virus is not possible or not fully within AstraZeneca control mainly because of the need for vendor intervention and due to regulatory compliance problems.

Based on this definition the document presents recommendations and mandatory principles for architecture and hardening of process automation systems and networks. The guideline also presents a recommended IS architecture for the protection of process automation systems networks. [32]

The principles can be summarized as:

**a.**
When possible, process automation systems should run on up-to-date operating systems and have installed and up-to-date anti-virus software.

**b.**
Process automation systems should be hardened as much as possible.

**c.**
Effective control must be in place to prevent unauthorized electronic access, remote access and connection of portable computer equipment to process automation systems and networks.

**d.**
Risk assessment and understanding of network traffic flows to, from and within the process automation systems and networks must be performed.

**e.**
Mandatory network segmentation architecture for process automation systems network infrastructure.

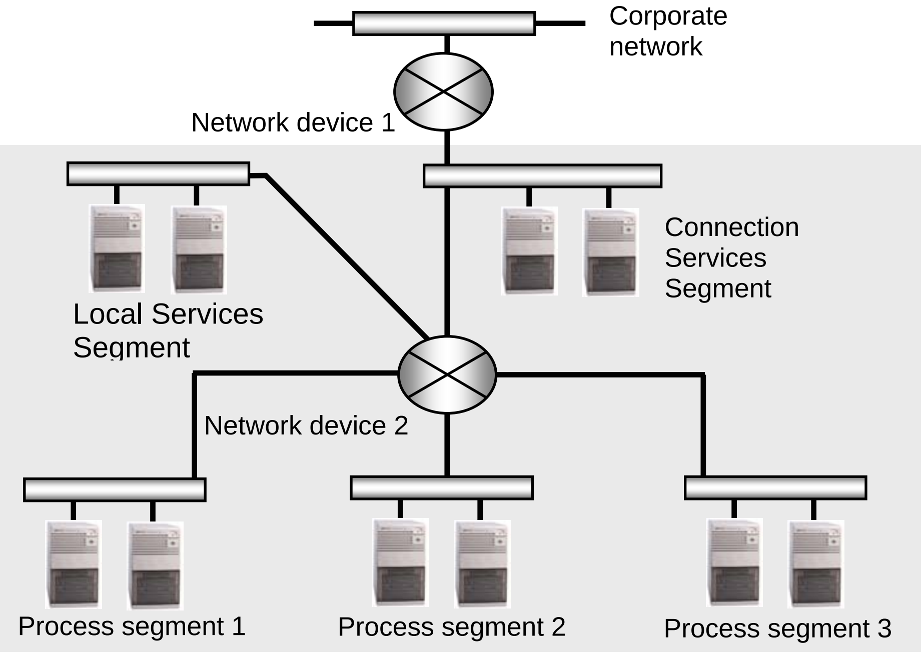


*Fig 2.2 AstraZeneca mandatory network segmentation*

**d.**
Ensuring that remote access to process automation systems meet AstraZeneca global network security standards.

## 2.2.8 AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services

This document defines an AstraZeneca Operations policy for the security and control of its process automation and associated laboratory-based systems. It is a document intended for AstraZeneca Operations globally. The document defines mandatory standards and good practice principles for protecting these systems from physical and electronic attacks.

Where possible process automation systems should be maintained and protected according to the rules and standards for corporate IT systems. As described in the introduction, process automation systems cannot always fulfil the IS security standards for corporate IT systems. Therefore the document defines the rules for protection based on how the different systems are connected to the corporate network. There are four different kinds of network connectivity for the different process automation devices:

- Devices connected directly to the corporate network (network connectivity scenario a)

- Devices within securely isolated networks with indirect connectivity to the corporate network as defined in [32]. (b)

- Groups of locally networked devices with no connection to the corporate network. (c)

- Devices with no network connection. (d)

Devices within (a) must meet all mandatory standards in the document. Devices in (b) must have local site approval for exceptions from mandatory aspects. Devices within (c, d) should meet all mandatory standards defined in the document where possible.

This is to be done through an implementation of a framework built on a background from industry process automation system and IS security. The framework focus on actions and aspects divided into seven themes:

- Establish ongoing governance

- Implement secure architecture and processes

- Understand the residual business risks

- Establish response capabilities

- Improve awareness and skills

- Manage third party risks

- Engage projects

*The different themes describe what is mandatory and what is good practice for systems depending on their network connectivity. Thus the document presents something of a generic program for IS security in process automation systems within AstraZeneca Operations. Deviations from compliance of mandatory aspects demand either global IS Security approval for exceptions or approval for local IS security for exceptions, depending on the severity of the deviations from the document.* [31]

## 2.3 ISA Hierarchical Reference Model

### 2.3.1 ISA 95 functional and equipment hierarchy modeling

The ISA 95 functional hierarchy model depends of defining the different activities within a manufacturing enterprise to certain specific levels. Activities on level 4 typically include plant production scheduling and operational management and the business-related activities needed to manage a manufacturing organization. Functions include enterprise or regional financial systems and other enterprise infrastructure components. [12]

Activities on level 3 include activities like detailed production scheduling, data collection and acquisition, quality management, process management and the functions involved in managing the work flows to produce the desired end products. [12]

Activities on level 2 include supervisory control. Activities on level 1 and 0 include direct control and the process. Functions here include batch control, continuous control and discrete control depending on the manufacturing processes. Pharmaceutical manufacturing is mainly performed through batch production. [12]

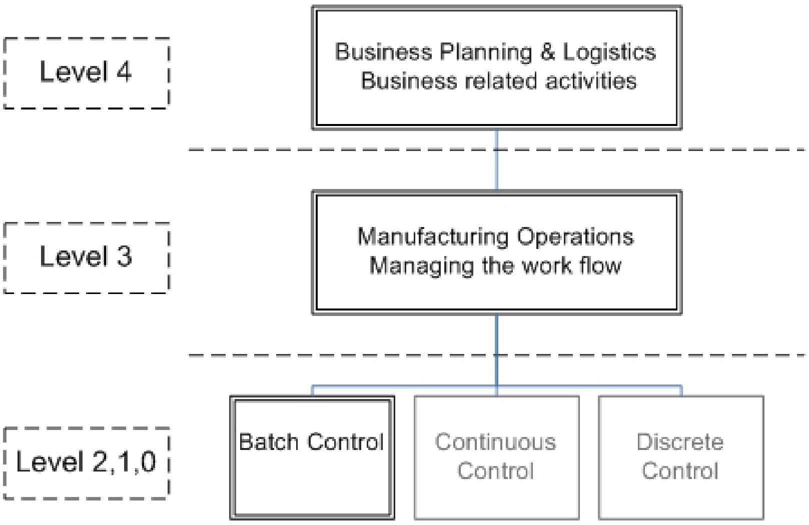


*Figure 2.3 ISA 95 functional hierarchy*

The equipment hierarchy model defines the areas of responsibility for the different functions in the hierarchy model. [12]

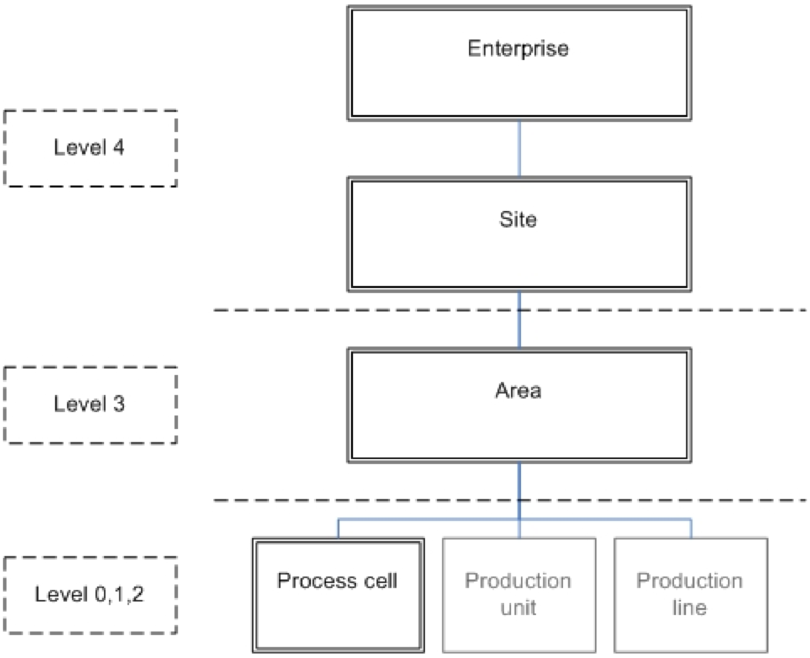


*Figure 2.4 ISA 95 equipment hierarchy*

An enterprise is a collection of one or more sites and may contain sites and areas. The enterprise is responsible for determining what products will be manufactured, at which sites they will be manufactured, and in general how they will be manufactured.

A site is a physical, geographical or logical grouping determined by the enterprise. It may contain areas and process cells. The level 4 functions at a site are involved in local site management and optimization. Site planning and scheduling may involve process cells within the areas.

An area is a physical, geographical or logical grouping determined by the site. It may contain process cells, production units and production lines. Most level 3 functions occur within the area. Areas generally have well-defined manufacturing capabilities and capacities that are made up of different process cells.

As mentioned above pharmaceutical manufacturing is mainly performed through batch production. Therefore level 0, 1, 2 are here considered as a process cell. This includes the process, the basic control equipment (a PLC or DCS system) and monitoring equipment (SCADA system). The process cell is the lowest element scheduled by operations on level 3 and 4. [12]

### 2.3.2 ISA hierarchical reference model

The ISA 99 standard use a hierarchical reference model for systems from level 0 (Process) to level 4 (Enterprise). The model is derived from the model in ISA 95. The reference model describes a generic view of an integrated manufacturing or production system, expressed as a series of logical levels. The model provides a map of for the various systems in the enterprise for increased understanding and visibility of the system activities and functions. [13]

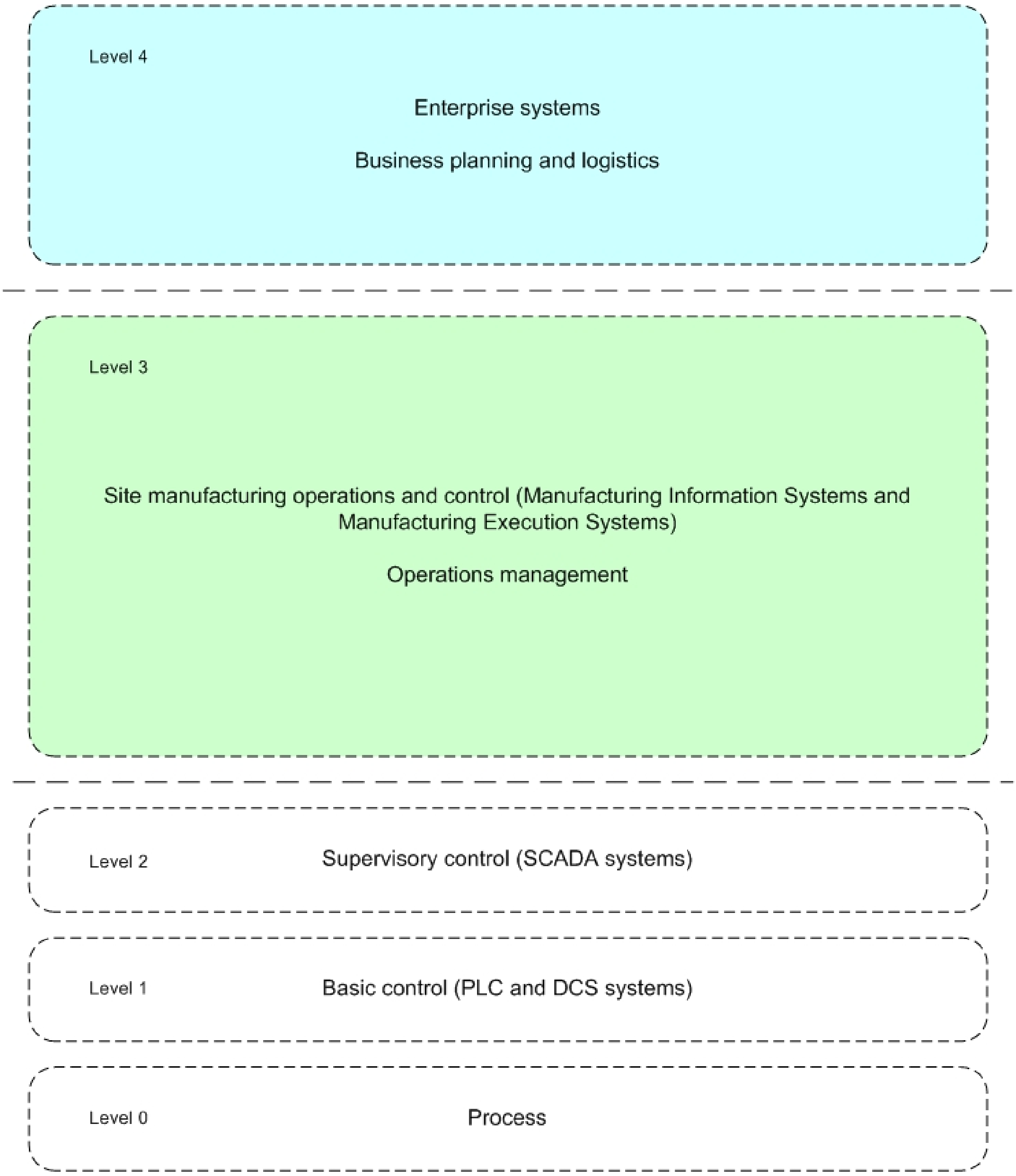

Level 4
Enterprise systems
Business planning and logistics
Level 3
Site manufacturing operations and control (Manufacturing Information Systems and Manufacturing Execution Systems)
Operations management
Level 2
Supervisory control (SCADA systems)
Level 1
Basic control (PLC and DCS systems)
Level 0
Process

*Fig. 2.5 ISA hierarchical reference model*

Computer systems used on the enterprise level are business systems. This includes for example accounting, logistics and production planning and business-to-business activities. MIS systems are systems for collecting information from the production and MES systems are used for executing the production. The data from production and corporate functions is used for optimization and detailed production scheduling.

SCADA systems typically consist of two PCs connected to the control equipment on level 1. The PCs are used for monitoring, collecting information and controlling the control equipment (PLC or DCS equipment and systems in this study). PLC and DCS are equipment that reads sensor values and if necessary executes control algorithms that change actuator and valve positions in the process (level 0). [13]

## 2.4 ISA 99 Zone and conduit model

The ISA 99 standard suggest the use of a key model for IS security analysis and implementation of IS security programs, the Zone and conduit model. By dividing the whole structure of the company network and computer systems into different zones and conduits, the security analysis can be improved. The intention with the use of the zone and conduit model in this study is to provide a tool for IS security analysis of Sweden Operations process automation systems and networks and to support the development of an IS security program.

The Zone and conduit model suggest a way to model the structure of the networks and systems in order to be able to identify assets and the risks connected to those assets. Therefore the first step in the model is an asset model that defines entities that are relevant to protect. Assets are systems and devices that are valuable and need protection against threats and disturbances. Assets can also be modelled in a hierarchical way where different assets contain sub-assets. [13]

The entities modelled in the asset model build up a reference architecture of the systems and networks. A reference architecture is specific to each situation under review and will be specific for that analysis. Each organization creates one or more reference architectures depending on the business functions performed, as well as the functions under review. According to the standard it would be common for an organization to have a single reference architecture for the general enterprise that has been generalized to cover all operating facilities. Each facility or type of facility may also have a more detailed reference network architecture that is used for expanding the model of the general enterprise model. [13]

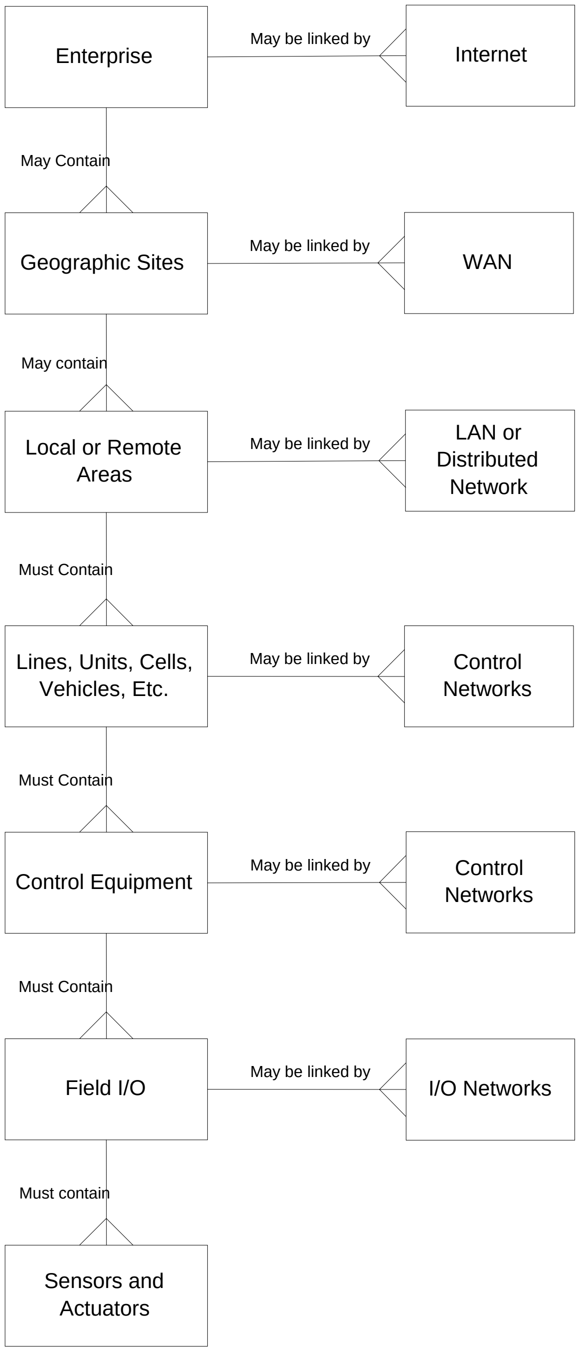


*Figure 2.6 Hierarchical asset model example (Copyright 2006 © ISA)*

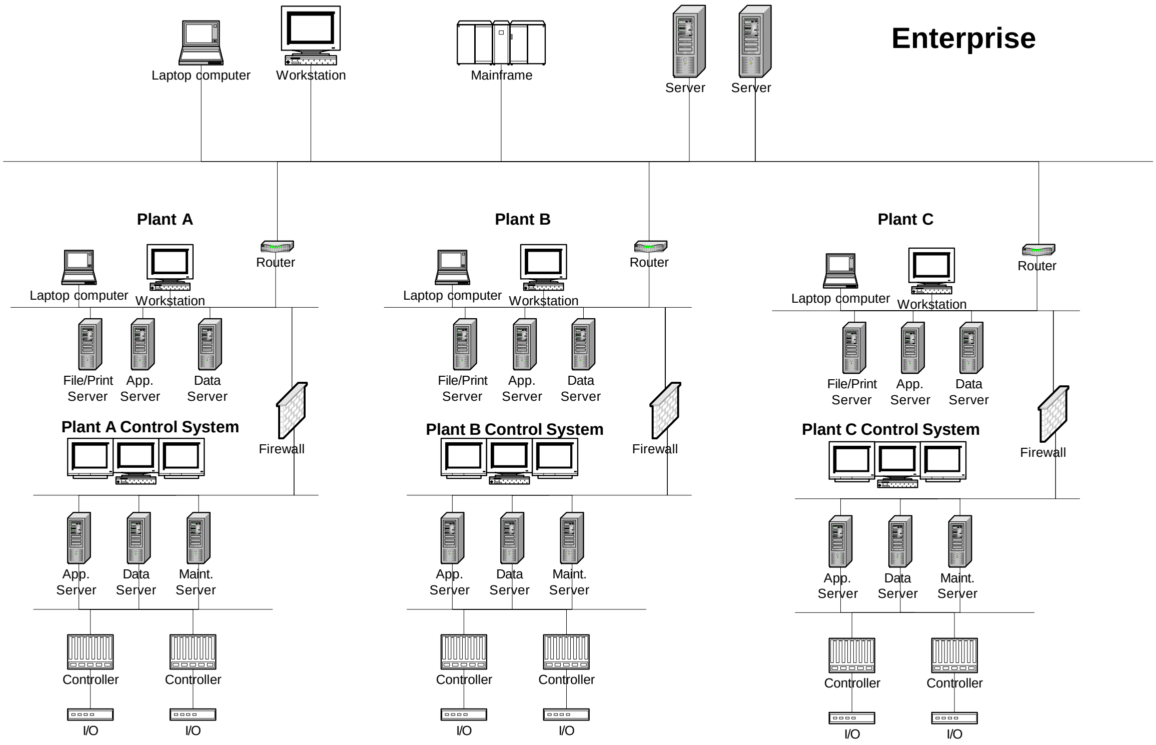


*Figure 2.7 Reference architecture example (Copyright 2006 © ISA)*

The reference architecture is then split up into defined security zones and conduits that interconnect the different zones. This model helps to assess common threats, vulnerabilities, and the corresponding countermeasures needed to attain the level of security required to protect the grouped assets. By grouping assets in this manner, a security policy can be defined for all assets that are members of a zone or a conduit. [13]

The security zones can contain other zones, assets or a combination of both. For every zone some characteristics or attributes are defined. Zone attributes that are relevant for this study are:

- Asset inventory

- Zone security policy

- Access requirement and controls

- Threat scenarios and vulnerabilities

Conduits are special security zones that apply to specific communication processes. That is, the conduit is the wiring, routers, switches, firewalls and other devices that are used for communication within and between different zones. The conduit can be seen as a pipe that connects the different zones and that are used for communication within zones. The conduit cannot be made up of other sub-conduits and has similar characteristics as the zones: [13]

- Asset inventory

- Conduit security policy

- Access requirement and controls

- Threats scenarios and vulnerabilities

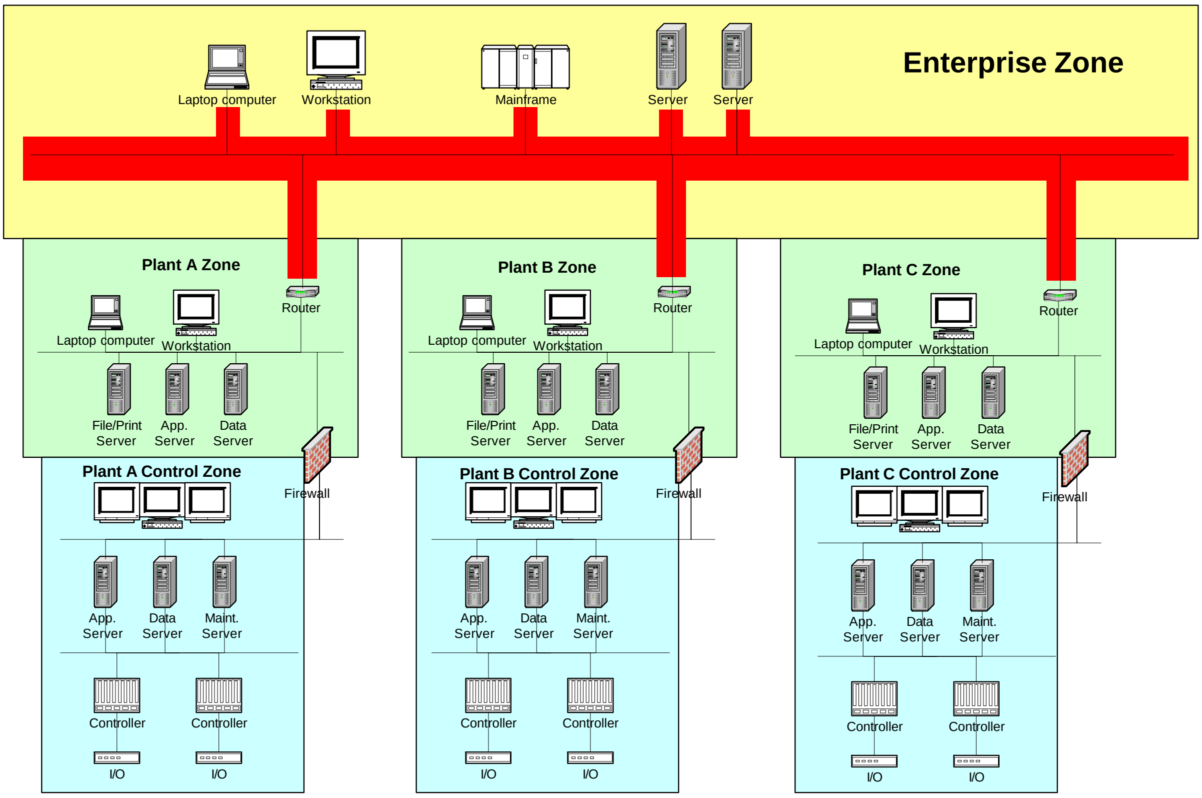


*Figure 2.8 Zones and conduit example (Copyright 2006 © ISA)*

The zone security policy and access requirement and controls here includes the security measures associated with the zone, activities permitted within the zone and the types of communication allowed access to and through the zone. The asset inventory includes assets that are valuable and worth protecting against threats inside the scope of this study. Assets can be both physical and abstract entities like servers, humans, the reputation of a company and valuable information. Threats and vulnerabilities represent possible identified threat scenarios based on the threats identified in section 2.7, which might harm or interfere with the identified assets. [13]

## 2.5 Development of an ISA 99 Security program

According to the ISA 99 Part 2: Establishing an Industrial Automation and Control Systems Security Program, the development of a cyber security program for process automation consists of at least 18 essential steps. The 18 steps provide 18 key elements of the IS security program. These elements are considered to be applicable on all different environments, conditions and situations for a manufacturing industry or site. The 18 key elements are: [14]

- Importance of cyber security in business

- Scope of the security program

- Organizational security

- Security policy

- Personnel security

- Physical and environmental security

- Incident planning and response (DRP)

- Access control

- Information and Document management

- System development and maintenance

- Staff training and security awareness

- Business continuity plan (BCP)

- Maintaining and implementing improvements

- Infrastructure-related operations and change management

- Risk identification, classification and assessment

- Risk management and implementation

- Monitoring and reviewing of the security program

- Compliance with policies and regulations

For a more detailed picture of the 18 elements and the suggested process for developing an IS security program, please refer to the ISA 99 standard Part 2. [14]

## 2.6 Criterions for evaluation of the architecture and IS security compliance

To evaluate the implemented network and system architecture for Sweden Operations it is important to connect the architecture to internal AstraZeneca standards and guidelines and to industrial standards and guidelines. IS security for industrial automation and control systems is an active research area. There are also a great variety of needs and threats for different industries. Therefore there is no universally adopted industry standard for recommended IS security safeguards implementation and suitable network architectures. The presented standards and guidelines represent international, national and industry references that are available today. This is considered to offer a good reference framework from both industry and AstraZeneca perspectives.

The criterions used for evaluation of the architecture and implemented security and the costs for implementing the security measures, are presented below. The criterions are mainly based on the criteria's used in the NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks document and on ISA 99 course material. [17] [20] [31]

### 2.6.1 Architecture security and IS security program implementation

The security criterion is maybe the most important criteria. It indicates the overall likely effectiveness of the architecture and implemented IS security measures to prevent possible attacks.

### 2.6.2 Architecture scalability and manageability

The overall ability of the architecture to be effectively deployed in both large and small systems or in large numbers. This also implies ability to expand the architecture. The overall manageability of the architecture indicates the ability of the architecture to be easily and effectively managed.

### 2.6.3 Architecture security versus cost

The last criteria can be seen as a summary of the criterions above. The probable cost of a security breach moves toward zero as the security level of the architecture and implemented security increases. At the same time the cost of security countermeasures increases with the security level, such as modeled in figure 2.9. Focus in this study is on the architectural aspects of IS security.

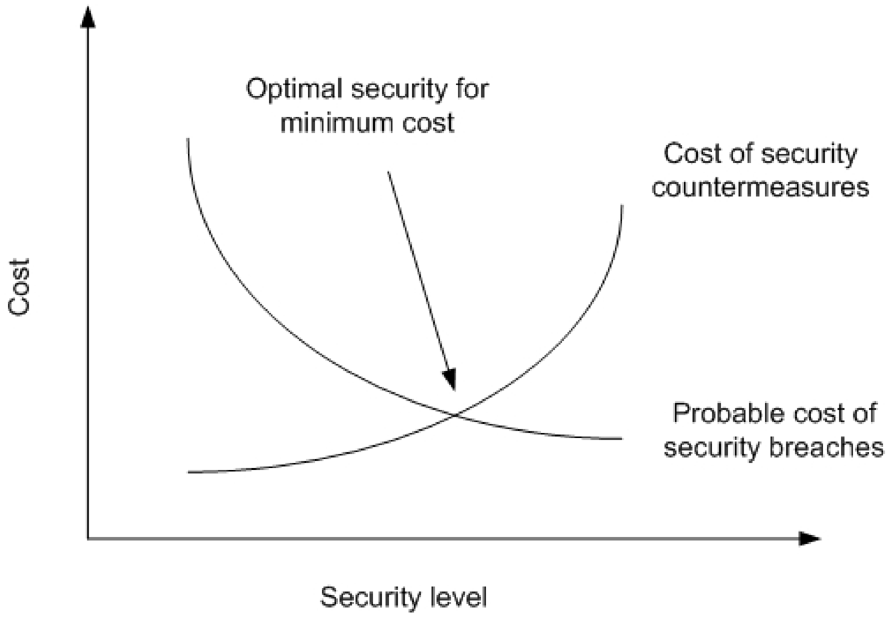


*Fig. 2.9 Cost versus security*

Thus there theoretically exists an optimal security level for minimal cost. In this criterion the architecture ability to use common hardware for applications must also be addressed. This means for example that applications used by different process automation systems might access the same database for process history collection. Therefore the possible use for sharing hardware for common applications also is weighted into the architecture and security versus cost criteria. [20]

## 2.7 ISA 99 IS security threats

To understand the possible IS security threats that endanger process automation systems it is important to understand the possible threat agents and the possible vulnerabilities to the systems. Common to all attackers or threat agents is the intentional or unintentional challenge to first gain access to the process automation networks and systems. Therefore it is important to understand the possible threat agents and second how they will gain access to process automation network and systems. [24]

ISA 99 defines threats as possible harmful actions that can be taken against a process automation system. Threats may be either passive or active. A passive threat is a threat that does not interfere with the affected system. A passive threat might include actions performed by the intruder to gather information that might be valuable or being useful in later performing an active attack. [13]

Active threats directly interfere with the affected system and come in various forms described in the standard. Active threats are here summarized as malicious code, human errors and interference of systems and communications. [13]

### 2.7.1 Threat agents

The ISA 99 standard present five forms of threat agents: [13]

**Insiders**
An insider is a ‘trusted’ person, employee, contractor, or supplier who has information that is not generally known to the public.

**Outsiders**
An outsider is a person or group not ‘trusted’ with inside access, which may or may not be known to the targeted organization. Outsiders may or may not have been insiders at one time.

**Natural**
Natural events include storms, earthquakes, floods, and tornadoes, and are generally considered a physical risk. Natural threats are considered as outside of the scope of the study.

**Accidental**
Someone unfamiliar with proper procedure and policy or an honest oversight causes an accidental risk. It is also likely that an organization does not know all the risks and may uncover them by accident as it operates complex industrial automation and control systems.

**Non-validated changes**
Updates, corrections, and other changes to operating systems, application programs, configurations, connectivity, and equipment can provide an unexpected security threat to the industrial automation and control systems.

### 2.7.2 Wire-tapping and scanning of networks

Wire-tapping and scanning of networks are passive threats. Wire-tapping means that the intruder gathers information that is transmitted on a network. The information can then be used for identifying business plans or valuable information. The intruder might also perform a scan of the network topology or scan for open ports in firewalls and systems. This information can later be used for performing an active attack against the system. [13] [20]

### 2.7.3 Malicious codes (Computer virus)

Malicious code is a program that might gather information about the system or process, destroy or falsify system data, halt the system with time-consuming operations or provide foothold for further intrusion in the system. Some viruses also replicate themselves and try to infect systems connected to the infested computer system.

Examples of malicious codes are computer viruses, worms and Trojan horses. Virus can be spread through networks, direct-dial up modems, e-mail and direct installation from connected memory devices like an USB memory sticks or by connection of a laptop computer. All malicious codes are manmade. [13]

### 2.7.4 Human errors

In this study, human errors represent mistakes, negligence or intentions to harm the system from a system operator or people with connection to process automation systems and networks. This also includes manipulation of operating systems and software connected to the control and monitoring program that is connected to the PLC or DCS equipment.

This also includes the threat of social engineering and insider attacks. Social engineering is performed through conning an individual to reveal secure information about architecture, networks and systems or even injecting hostile programs into a computer. The individual might be forced or tricked to reveal the information or to perform the hostile actions. Information can also later be used for conducting a more active IS attack against the process automation systems or sold to a hostile competitor or an organized criminal syndicate. Social engineering is a threat that has to be addressed seriously since it might provide an external attacker with valuable information or foothold for a more serious attack. [13]

An insider attack is an attack initiated by an entity inside the security perimeter (an ‘insider’). That is an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. [13]

### 2.7.5 Interference of systems and communications

One way of interfering with process automation systems is to perform a ‘denial of service attack’. The denial of service attack affects the availability of a network, operating system or application. An attack typically consists of the attacker sending multiple data packages to the attacked computer making it halt or become unavailable. Distributed denial of service attacks use multiple computers to send data packages towards the victim computer. [13]

The intruder might also try to connect directly to a specific system through a direct-dial up or a remote access connection. The direct-dial up connection is performed through a modem connection and the remote access connection through access from the Internet or through connection to a wireless network. System vendors of automation equipment often use modems for remote access to systems. In order to save money on travel and people the vendor can recode and modify parameters in the control equipment without being connected directly on site to the process. [13]

If to access the process automation network by a remote access connection the intruder faces the challenge of first locating the process automation systems networks. If successful the intruder must also succeed in gaining access to the process automation systems or networks. When connected, the intruder can then perform more serious activities on the infested system and against the computer devices that are connected to the network. This threat also includes man in-the middle attacks, database attacks, peer utility attacks and VPN hacking. [13] [25]

### 2.7.6 Summary

Possible IS security threats for different threat agents.

| Agent/Threat | Insider | Outsider | Accidental | Non-validated changes |
|---|---|---|---|---|
| Wiretapping and network scanning | | X | | |
| Malicious code | X | X | X | |
| Human errors | X | X (social engineering) | X | X |
| Interference of systems and communications | X | X | | |

*Table 2.1 IS security threats and threat agents*

## 2.8 Good Manufacturing Practice guide (GMP)

The GMP is a regulatory framework that provides guidance and rules for the manufacturing of pharmaceuticals. Most countries and the European Union today have their own GMP regulations. The American GMP is administrated by the Federal drug and food administration (FDA). The American GMP regulations are very important to the company due to that a large part of the AstraZeneca revenue comes from the American market. However the majority of the different GMP regulations follow the same principles. [21]

The GMP regulations are built on nine chapters:

- Quality management

- Personnel and education

- Facilities and equipment

- Documentation

- Manufacturing and packaging

- Quality control

- Production and analysis within outsourcing ventures

- Reclamations and withdrawal of products

- Internal inspections

If AstraZeneca violates the GMP regulations, the company face the risk of loosing its permission to manufacture and for marketing pharmaceuticals. This makes the GMP regulations very important to the company.

In this study, the most important part of the GMP regulations is the manufacturing, packaging and quality control directives. These directives demands that all production must be:

- Repeatable. All produced pharmaceuticals must be exactly the same (within a certain allowed deviation interval) irrespective of that they are manufactured in different batches.

- Traceable. There must be a possibility to trace all produced pharmaceuticals through the complete production process. This includes raw material, production processes and quality controls. All steps and deviations in the production process must be documented.

*Thus virus infections or changes to operating systems and the software on process automation and lab systems would jeopardize the compliance of the GMP regulations. This implies that all software on process automation systems and computerized quality control equipment (lab equipment) must always be approved and carefully maintained and supervised. This is known as the process automation system being in a validated state. Only process automation systems that are in a validated state can be used for manufacturing and quality assurance work.*

Within Sweden Operations there exist procedures for assuring that systems behave as intended after they have been updated or patched. These procedures are time consuming and costly since the production has to halt. Operating systems updates or changes to other software cannot be applied without assuring that the system works as intended. Therefore the computer systems within the manufacturing of pharmaceuticals must be protected in different ways than ordinary office computers. [2] [21] [53] [54]

# 3 Methodology

## 3.1 Overview

This chapter describes the methodology that was used for performing the study and the risk analysis method that was used for identifying and analyzing the most severe IS security risks. The chapter also provides some criticism and possible applicability of the study.

## 3.2 Performing the study

The work was continuously supported by the AstraZeneca supervisor through ideas, suggestions for personnel to contact for information and through sharing of knowledge. The work for performing the study can be divided into five major somewhat subsequent parts. All work was performed at the Södertälje site.

### 3.2.1 Understanding the production, systems and networks

To be able to perform the study the first step was to understand the context within Sweden Operations and the production at the Södertälje site. This work was mainly used for developing the reference architecture and to understand the IS security vulnerabilities and threats that are present to the process automation systems at the Södertälje site.

The work was performed through studying various AstraZeneca documents, performing observations and interviews with personnel in the production, lab, and system owners and managers and with OI personnel. Due to the size of the organization, complexity and structure of the networks and systems and the outsourcing agreement with IBM within Sweden Operations, this was a time consuming process.

In depth observations have been performed in the ALFA and BETA plant. The process for choosing ALFA and BETA production areas as reference was performed through evaluating different production areas as described in the introduction. Production areas at the Gärtuna and Snäckviken sub-sites were investigated during the process.

### 3.2.2 Evaluating the architecture and IS security compliance

The major effort was here spent on searching for current available IS security standards with a focus suitable for the study. The main focus was on finding IS security standards with suggestions for network segregations of manufacturing systems and networks. There are numerous IS security standards available for different environments and networks, but very few concerning process automation systems security. The topic is an active research area.

The industrial and national standards that are used in the study represent all relevant standards that are available today. Unfortunately the IEC 62443 standard is still being developed and therefore not available. The IEC 62443 ‘Security for industrial process measurement and control - Network and system security’ standards might have been useful for evaluation of the architecture and implemented security. The IEC 62443 work is connected to the work on the ISA 99 standards. The ISA 99 standard is considered to cover the relevant parts in the ISO/IEC 17779 and ISO/IEC 27001 standards. [13] [14] [27]

The available standards and AstraZeneca guidelines then formed a framework for evaluating the architecture and implemented IS security measures. The criterions used in the evaluation were chosen in cooperation with AstraZeneca supervisor. The NISCC Good Practice Guide on Firewall for SCADA and Process Control Networks document Deployment mainly inspired the criterions together with ISA course material. [17] [20]

The evaluation of the fulfillment of the AstraZeneca guidelines was mainly performed through interviews with responsible personnel and by review of relevant AstraZeneca documentation. Observations in the reference production areas in the study were also performed.

### 3.2.3 IS security risk identification and assessment

The IS security analysis work began with finding a suitable method for IS security risk analysis. The objective for the methodology in identifying and assessing the present IS security risks, was chosen to follow the Primatech Scenario-based approach for industrial cyber security analysis method (described below) and connect this to the ISA 99 Zone and conduit model. The ISA 99 Zone and conduit model is used for the work in the first step in the Primatech method.

Following the Primatech method, the first step was to define zones and conduits from the reference architecture (presented in chapter 4). After this, the work was focused on identifying all possible IS security threats and vulnerabilities within the zones and conduits. These scenarios were investigated in order to identify the assets that are threatened and to define the expected worst possible consequences. This also included work to identify which production areas that are connected to and affected by the operation of the DELTA conduit and the EPSILON and ZETA zones. The DELTA conduit (network) and the EPSILON and ZETA zones (networks) are described in chapter 4 and 6.

A lot of work was also spent on collecting information about implemented IS security measures through studying documentation, observations and interviews with responsible personnel. A test for hacker possibilities and virus infection from connected laptops in production was also performed. This test was performed through connection of an ‘external’ laptop to a BRONZE network (a production area or lab VLAN) (Appendix D).

The consequences were then connected to financial aspects defined by the delay in production that the worst-case scenario consequences would cause. The financial aspects of the consequences were transformed into a monetary loss with the help of the Sweden Operations Finance department (OF).

Finally the scenarios and their consequences were ranked in likelihood and impact. The likelihood rating is based on incident history, the threatening picture and the existing IS security measures. The likelihood and impacts was then summarized to provide the severity for the scenarios.

Based on the most severe risks, possible technical and administrative suggestions for security improvements were then suggested. These suggestions were inspired by the ISA 99 standard, AstraZeneca guidelines and the standards presented in the theory chapter. Input was also provided from the ISA 99 technical reports and personnel at the OIT department. [15] [16]

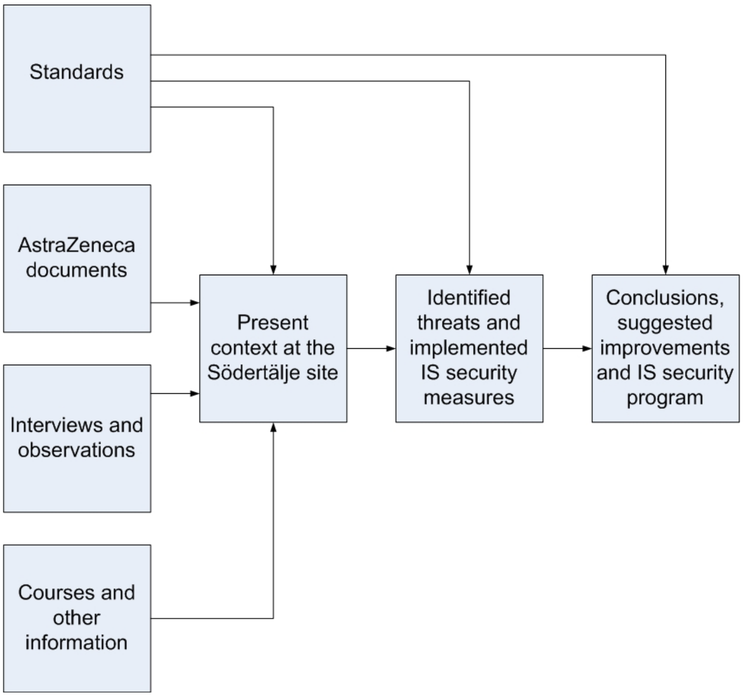

Standards
AstraZeneca documents
Interviews and observations
Courses and other information
Present context at the Södertälje site
Identified threats and implemented IS security measures
Conclusions, suggested improvements and IS security program

*Fig 3.1 Performing the study*

### 3.2.4 Development of an IS security program for the DELTA context

The first step in development of the security program was to define which of the 18 key elements presented in the ISA 99 Part 2, which was going to be included in the security program. Addition of a 'Defence-in-depth strategy' section was made. Sections were also added to expand the Production area and Lab environment IS security policy. This includes 'System hardening and anti-virus protection', 'System monitoring', 'Connection of portable computer equipment' and 'Reduction of third part risks'.

The remaining elements of the security program were then developed. The work is mainly based on the ISA 99 Part 2 but also includes input from the standards and guidelines in the theory chapter. The ISA 99 technical reports also provided input for technical suggestions. [14] [15] [16]

Finally a list of personnel and organizations responsible for the implementation of the italic paragraphs in the security program was developed (Appendix E).

### 3.2.5 Investigation of IS security risks in MES/EBR system implementation

This chapter evaluates the future implementation of a manufacturing execution system/electronic batch record system. Therefore the work was first spent on studying the possible structure of the system and interviewing personnel involved in the project. These interviews provided knowledge about the system and possible IS security risks that the system could create. Possible ways to implement the MES/EBR system in the reference architecture was then developed together with AstraZeneca supervisor. These models and their impact on the IS security level in the production were then briefly evaluated in a perspective of increased wireless network vulnerabilities, MES system availability and MES critical systems availability. Unfortunately there are no standards available concerning MES and IS security.

## 3.3 IS risk analysis methodology

To perform a successful IS risk analysis it is important to have a clear strategy in the process of identification, assessment and analysis of the risks that is inside the scope of the study. There are numerous methodologies available for IS risk analysis procedures. The methodologies are either asset or threat/scenario based. The final conclusion of both methods is the same but either starts by identifying assets worth protecting from threats/scenarios or threats/scenarios harmful to assets worth protecting. [14]

ISA 99 Part 2 present a suggested asset based method based on identification of assets worth protection and connecting them to possible threats and impacts. The method is applicable to process automation systems. The method is also applicable to the zone and conduit model. [14]

The intention with this study is to analyze the IS security on both a detailed level and with an overall perspective of the DELTA architecture. The awareness of IS security issues is also already present at AstraZeneca Sweden Operations. This combination makes a threat/scenario based analysis methodology more suitable than an asset based model like the one presented in ISA 99 Part 2. AstraZeneca supervisor also supported this decision.

In order to find suitable method for IS security analysis for a context in manufacturing of pharmaceuticals the CIDX document; Report on Cyber Security Vulnerability Assessment Methodologies, offers a good guideline for evaluating different risk analysis methods. With the help of attachment 2 (Technical criteria) the Primatech Scenario-based approach for industrial cyber security analysis, was chosen. [10] [19]

Primatech is an Ohio based consulting firm specialized in process safety, security and risk management. Primatech offers consulting, training and software for identifying and reducing consequences of risks. The company is also involved in the development of the ISA 99 standards.

### 3.3.1 Primatech Scenario-based approach for industrial cyber security analysis method

The Primatech ‘A Scenario-Based Approach for Industrial Cyber Security Vulnerability Analysis’ presents an IS security vulnerability analysis method that can be used to conduct IS security vulnerability analysis against present and future threats. The method can also be used on different levels of a reference architecture. The method is scenario based and is therefore suitable for the scope and context of this study.

The first step in the method is to divide the systems, processes, facilities and networks into different systems or subsystems. In this study this is done in accordance with the ISA 99 Zone and conduit model. The next step is to consider all credible threats within each zone or conduit.

Step three is to identify the vulnerabilities within each zone or conduit. Step four is to list worst possible consequences for the threat scenarios. Step five is to list existing security measures and measures within each zone and conduit. Step six is to risk rank all the different scenarios. The rating is in this study built upon a likelihood rating and a financial impact rating. The criterions for the rating are presented in appendix A.

The existing security measures decrease both the probability of a threat scenario and the consequences. The final seventh step is to identify possible recommendations for suggested security improvements based on the analysis in the first six steps.

To connect the different steps to the Zone and conduit model this provides the zone and conduit attributes; Asset inventory, Zone security policy, Access requirement and controls and Threat scenarios and vulnerabilities.

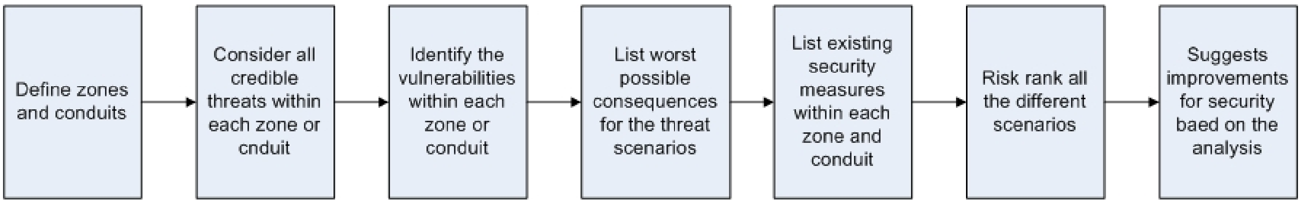

Define zones and conduits
Consider all credible threats within each zone or cnduit
Identify the vulnerabilities within each zone or conduit
List worst possible consequences for the threat scenarios
List existing security measures within each zone and conduit
Risk rank all the different scenarios
Suggests improvements for security baed on the analysis

*Fig. 3.2 Primatech Scenario-based approach for industrial cyber security analysis method combined with the ISA 99 Zone and conduit model*

### 3.3.2 Quantitative risk rating

Likelihood and impact consequences for different risks and assets can be rated in both qualitative and quantitative ways depending on the informational available.

Risks, likelihood or probabilities are usually treated as numbers and a value from zero to one respectively. In practice that kind of precise information is seldom available without extensive data collection. Hence a qualitative measure or quantitative scale is preferable.

The ISA 99 procedure above transforms qualitative ratings into quantitative measure scales. This is also the case with AstraZeneca guideline for risk analysis (also known as the AstraZeneca Integrated risk management tool (IRM)) and is also suggested in the Primatech method. Therefore the likelihood of a scenario is quantified as a number from one to five, corresponding to Very low, Low, Medium, High and Very high likelihood. [14] [19] [35]

An asset with quantitative valuation has a precise monetary loss associated with it. An asset with a qualitative valuation expresses a more abstract loss. In the case of loss of information and loss of time for production it is very hard to calculate exact values. Therefore the AstraZeneca quantification scale for impacts is used as measure for financial impacts. This provides a scale form one to five corresponding to the delay in production that a security incident causes.

Thus only the delay in time for production is transformed to a monetary value. The value of batches that have to be scrapped is also presented as a monetary loss.

The criterions are presented in appendix A. [29]

## 3.4 Criticism and applicability

### 3.4.1 Applicability

The result and conclusions of this study are only applicable at the AstraZeneca Sweden Operations context at the Södertälje site. The study might provide useful information for similar studies and IS security analysis at large manufacturing sites. Especially pharmaceutical and chemical substances manufacturing sites and companies might find the study useful. The study is less applicable on small manufacturing sites with process automation system that are less vulnerable to IS security threats.

The study also presents a good source for references of the current available and under development IS security standards for IS security in the process automation systems environments.

### 3.4.2 Criticism of the methodology

The methodology in the study has a strong touch of a management view of IS security and less technical foundation. More in depth study of the hardware and systems that are involved might have provided a deeper insight and a more accurate likelihood and impact rating in the IS security risk analysis.

There is also a possibility that the two production areas used in the study not represent the actual IS security context and conditions at the Södertälje site. They might have both a higher and a lower level of implemented IS security measures than the average production area at the site. Studying more production areas might therefore have been useful.

### 3.4.3 Criticism the information sources

Many of the IS security standards used in the study are closely related. Since the area is an active research topic there is no universally accepted standard for IS security in manufacturing and process automation systems. The ISA 99 standard is the standard that is most referred to today. Many standards are also intended for a variety of industry environments. There is also a possibility that there exist suitable standards within the IT industry.

The AstraZeneca documents used in the study are not publicly available and some information that is presented is also confidential. The AstraZeneca IS security standards are intended for the AstraZeneca environment and are therefore less applicable than industrial standards like IEC, ISA and ISO standards.

A possibility to review the BCPs, DRPs for DELTA and other confidential material has not been granted due to the outsourcing agreement with IBM or AstraZeneca restrictions. This information is therefore based on information from AstraZeneca supervisors.

A large part of the empirical material in the study is collected through interviews. There is a risk that the interviewed personnel at AstraZeneca have responded in a way that not is perfectly correct. The information might intend to emphasize the respondent in a good way. Some responses might also be incorrect due to guessing and assumptions from the respondents. Since the absence of a properly maintained IS security level probably will require more work for a system owner, there is a risk that they have tried to embellish the actual conditions.

# 4 A reference architecture for the DELTA context

## 4.1 Overview

To connect with the Zone and Conduit model from the ISA 99 standard this chapter provides a reference architecture that can be used in the subsequent chapters. The chapter describes the general process used for manufacturing of API and tablet pharmaceuticals (drug product pharmaceuticals), the systems used in the process and the overall architecture of the systems and the network that interconnects these systems – the DELTA context.

## 4.2 Manufacturing of pharmaceuticals

To provide a brief understanding of pharmaceutical manufacturing this section explains how tablets and active pharmaceutical ingredients (API) are manufactured. The basis of all pharmaceuticals is the API. The API is in general manufactured in a different production process than in the manufacturing process for the final product. The API is then used in different kinds of pharmaceuticals like tablets, capsules and Turbuhaler products. In this study, tablets are used as an example for the manufacturing process of the final product (or drug products pharmaceuticals). All manufacturing of pharmaceuticals at AstraZeneca in Södertälje is performed through batch manufacturing.

### 4.2.1 Manufacturing of API

The production in the ALFA plant is performed according to a gravimetric method. This means that the different equipment is placed on different floor plans. The raw materials are added at the top and the dried end product is delivered at the bottom floor. The Beta plant has three similar segments (Swedish: ‘skepp’) or production processes. The segments are called A, B and C.

The process for manufacturing of API in Beta consists of six steps. The first four steps use the same process equipment (reactor tanks) while the centrifugation and drying steps use separate process equipment. All equipment is controlled by DCS systems, which are operated by the operators in the factory. The production equipment and DCS systems used in the manufacturing process in segment A in Beta is pictured in appendix B and section 4.4.4. [58]

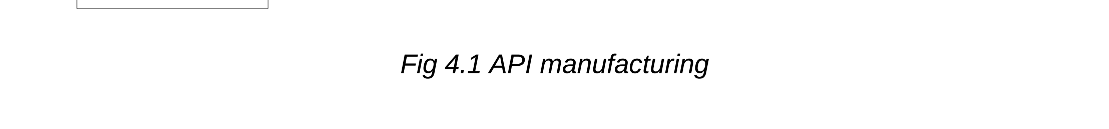


*Fig 4.1 API manufacturing*

The production process begins with mixing raw materials into chemical reactor tanks. Raw material is often dry material, liquid substances and different solvers. Solvers are added from the tank station (Swedish: ‘tankbar’) and liquid raw materials from the intake station (Swedish: ‘insugningsstation’).

Depending on produced substance, different reactions and adding of more substances produce the desired API in the reactor tanks. The API is now part of a solution that needs to be purified from liquid solvers and unwanted substances. The unwanted substances and solvers are fed into the receiving tanks. After some purification, the API substance is crystallized in the solution. This might be performed through cooling of the reactor tank or by adding other substances to the solution.

When the API substance has crystallized it is fed into the centrifugation equipment under the reactors and the receiving tanks. The centrifugation removes remaining solvers.

The last step in the manufacturing process is drying of the API substance. The final product consists of a dry powder of API granules.

### 4.2.2 Manufacturing of tablets

The manufacturing of tablets products consists of several production steps involving different processes and production equipment and the batch is physically moved between the different production equipments used in the different processes steps.

The process steps and the different process automation systems with operating systems used on SCADA systems for manufacturing of tablets in BETA are described in appendix B. Some equipment does not have SCADA systems and are controlled by manual control devices. The SCADA systems use PLC equipment for the control and monitoring of the process.

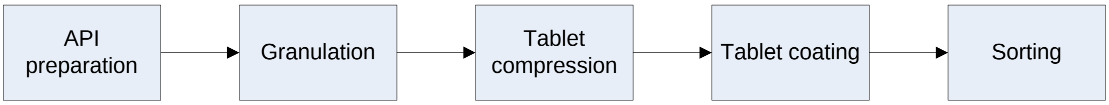


*Fig 4.2 Tablet formulation*

The first step in the production process of tablets is to prepare the API. The API is prepared into a mixture before the granulation starts. The granulation process involves building up several spherical layers starting with the API granules. The different layers are needed in order to make sure that the API is released at the right place in the human body. Different products have different layers depending on product group or tablet formulation.

After the granulation, the pharmaceuticals now consist of small granules. In the tablet compression phase, the granules are mixed with a material that binds together the granules, for example with cellulose. The cellulose granule mixture is then compressed into tablets in a tablet compression machine.

The next step is to provide the tablets with a proper coating. The coating is sprayed onto the tablets in a machine that resembles a tumble dryer. The coating is often dependent on the demands of the customers or on how the tablet needs to be protected. This might include providing the tablets with flavour, colour or lubrication.

The last step in the production process is to sort out defect tablets. This is done by machines that weights or sort the produced tablets and scrap tablets with a wrong weighing or defect form. A wrong weighing indicates that the number of granules not correspond to the intended potency of the produced pharmaceutical.

After the tablets are sorted they are sent to a packing area for packaging and distribution.

## 4.3 Systems in the manufacturing of pharmaceuticals at the Södertälje site

### 4.3.1 SCADA, PLC and DCS systems

The systems in production consist of process automation systems connected to one or more steps in the manufacturing of the pharmaceuticals. In this study a process automation system consists of a PLC or a DCS system connected to the process (level 1 and 0 in the hierarchical reference model) and PC clients.

PLC based production is mainly used for manufacturing of the final product (drug product pharmaceuticals) like tablets, Turbuhaler and capsule pharmaceuticals. The PLC (level 1) is connected to a SCADA (Supervisory control and data acquisition) system that consists of one or two PC clients (level 2) One PC is placed in a control room and the other PC is placed close to the process (level 0). The SCADA system is used for monitoring of the control equipment and for collecting data from the process.

DCS based production is mainly used for the manufacturing of API. The DCS (level 1) is connected to clients (level 2) and the manufacturing processes (level 0). One DCS can be used for monitoring of many different dispersed processes steps. The clients are used for monitoring the DCS and for collecting data from the processes.

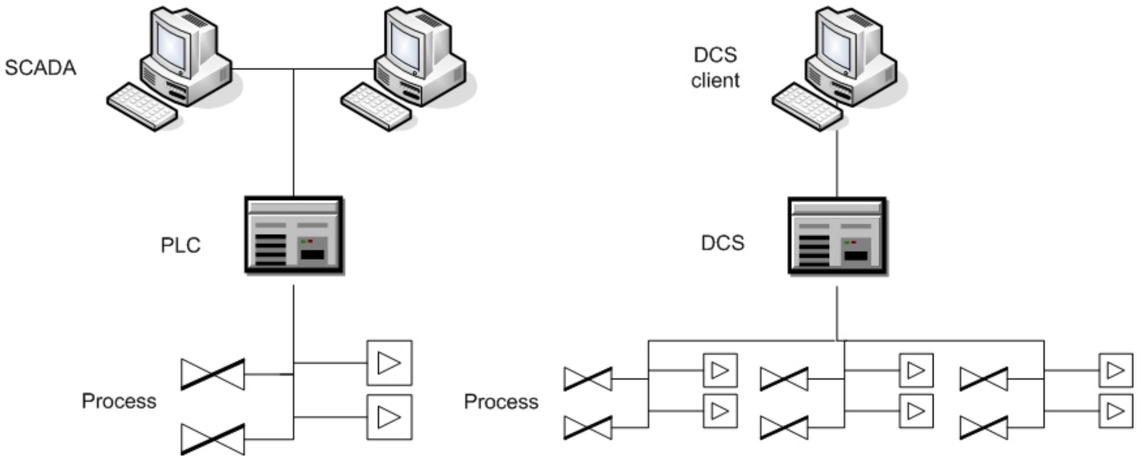


*Fig 4.3 SCADA + PLC and DCS*

### 4.3.2 Scheduling of production

The scheduling and planning of production is made with the help of a KANBAN system. KANBAN is a production-planning tool developed by Toyota that utilizes cards to keep track of items in manufacturing organizations. The KANBAN system is used for decreasing lead times in the production and to keep track of raw material and produced materials inventory. The system is partly computerized. All production planning and scheduling computer systems are operated from the corporate network (described below). Therefore they are not addressed in this study. [3]

### 4.3.3 Quality systems

All production is made in compliance with the GMP regulations that are described in the theory chapter.

**Recipes and Master recipes**
The DCS and PLC equipment uses predefined recipes in the manufacturing process. The recipe contains the procedure (program sequence), the formula (parameters), and the equipment requirements. The procedure defines the different steps the control equipment is supposed to perform, the formula defines the parameters to be used e.g., actuator values and equipment instructions. The equipment requirement specifies the equipment to be used. As a simple example, one step in the procedure might be filling, the equipment requirement specifies the name of the reactor to be used and the formula gives the amount of liquid the reactor should be filled with. When the recipe executes it is referred to as a control recipe. During execution, the control recipe collects relevant information such as the temperature of the liquid and the time for starting and ending of the filling step

A master recipe is the specification of how to produce a specific pharmaceutical, whereas the control recipe is the record of how a given quantity of a pharmaceutical was produced.

**Quality control and assurance – Lab systems**
Parallel to the production, special laboratory personnel run tests and analyze samples of both non-finished products and prepared products to assure the quality of the pharmaceuticals and that the production complies with the GMP regulations.

The lab personnel use special lab equipment systems like chromatographs and radiation analysis instruments. Most lab equipment is connected to PC clients and has separate JOTA (VLANs). Some lab systems are of client-server type and use server applications in the ZETA network segment (described below) for storing measurement data (here referred to as Eta systems).

The results from lab analyses are printed and used for quality assurance of manufactured batches (as described below) and for quality control. The systems used for this are called FI and OMEGA. These systems are operated from the corporate network and are therefore not addressed in this study.

**Batch protocols and quality control protocols**
The batch protocols are documents used by operators of the process equipment and lab personnel to provide reports from the production. For every process step there is a written protocol that connects to the recipe. For the step example above, this might include when the filling started and stopped, temperature of the liquid and if there

where any deviations from the defined recipe. When a step is completed the operator notes the required values and then signs the protocol to affirm that the step has been accomplished and performed in accurate ways that comply with the GMP regulations.

The lab personnel use similar quality control protocols for performing and reporting test results that assures the quality of produced batches.

**Batch reports**
The batch reports are information and data from the manufacturing processes of a batch. This might include audit trails and trend data with timestamps or other data and information collected from the process automation systems involved in the production of the batch.

**Batch files**
When the batch is manufactured, the batch protocols and quality control protocols from the batch are assembled together with the batch reports to a batch file. The batch files provide traceability for the manufactured batch. The batch files are critical for Sweden Operations in order to comply with the GMP requirements.

**Batch quality assurance**
Before the batch is approved and shipped it must undergo quality assurance before being released from manufacturing. This is performed by special quality personnel. The quality control process uses the batch file and confirms that the production has been made according to the master recipe and in compliance with the GMP regulations. This insures that the final product is suitable for the intended patients and not harmful to consume. [21]

**Validation of computer systems used in pharmaceutical manufacturing**
All equipment that have impact on the production processes of pharmaceuticals or impact on GMP requirements must be validated prior to being used in the production. The validation assures that the equipment behaves as intended and the production comply with the GMP regulations. The framework for this is called the Good automated manufacturing guide (GAMP). [2]

Since most equipment is computerized all changes of software or hardware or configurations on process automation systems must be revalidated. Thus applying updates to software or installing new software on process automation systems demands a new validation. The validation is performed through predefined SOPs and RUTs. [54]

### 4.3.4 Collecting and reporting of data from production – the THETA system

The Manufacturing information system (MIS) used within Sweden Operations for collecting and reporting of data from production is called THETA (Process Information System). All production areas on the Södertälje production site do not yet use the system.

The THETA system is based on central information collection of production data from the process automation systems used in the production and consists of three main parts: The central databases that the system uses, applications placed both centrally and locally on production clients and finally the services that the system provides.

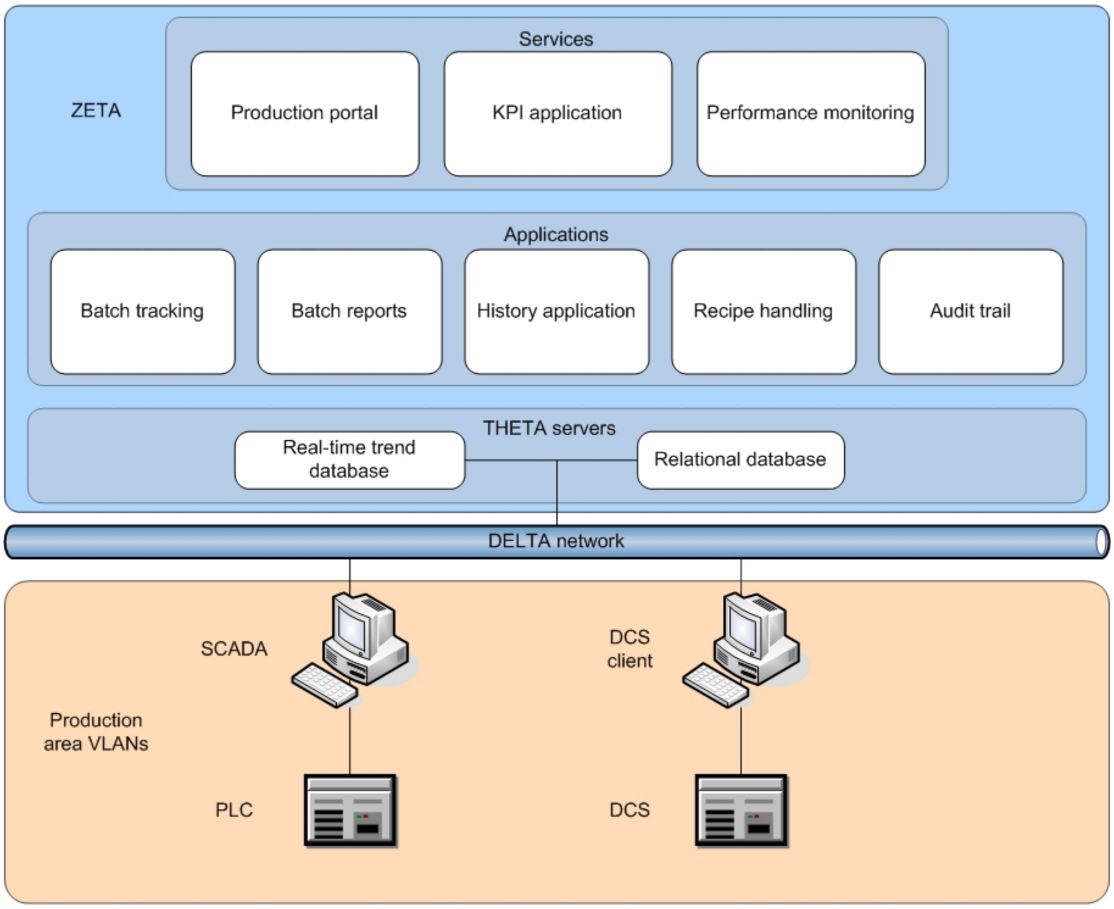


*Fig 4.4 THETA*

The central databases, applications and services use hardware that belongs to of the ZETA segment (described further down). There are two different databases:

The trend database is used for storing trend data. The trend database is a real-time process data historian as well as a special information platform with direct record access via a search tree technology. All process data from sensors on process automation systems in the production are stored along with a timestamp.

The relational database used for storing batch data, events from production and applications like recipe handling. Events include for example start time for starting manufacturing a batch, time for specific commands from operators and sensor alarms from the processes.

The central applications are used for providing batch data, batch reports, audit trails, trend history applications and recipe handling. The audit trail can be used to review who has been involved in manufacturing of a batch. The recipe handling application manages all manufacturing recipes (computer instruction recipes) for the connected process automation systems. When a recipe is updated it is downloaded to the specific process automation client and PLC or DCS system. This provides central storage and management of recipes. The history application is a graphical user interface that provides statistical tools for analysing trend data from production.

The central services provided are a production portal, KPI (key performance indicators) application and performance monitoring. The production portal is used to provide material to batch reports and provide information from the production to users in the corporate network and on the DELTA network (described below). The KPI application is used for optimization of the production and for finding bottlenecks in the supply chain. The performance-monitoring tool is used for reducing equipment and quality failures. With this tool the scrap and equipment breakdown costs in production are reduced. The services are presented to users on the corporate network through the DELTA application portal (described below) but can also be viewed from any web client inside DELTA.

THETA is an important and efficient tool for the manufacturing of pharmaceuticals at the Södertälje production site. [44] [64]

## 4.4 General model for systems involved in manufacturing of pharmaceuticals within Sweden Operations

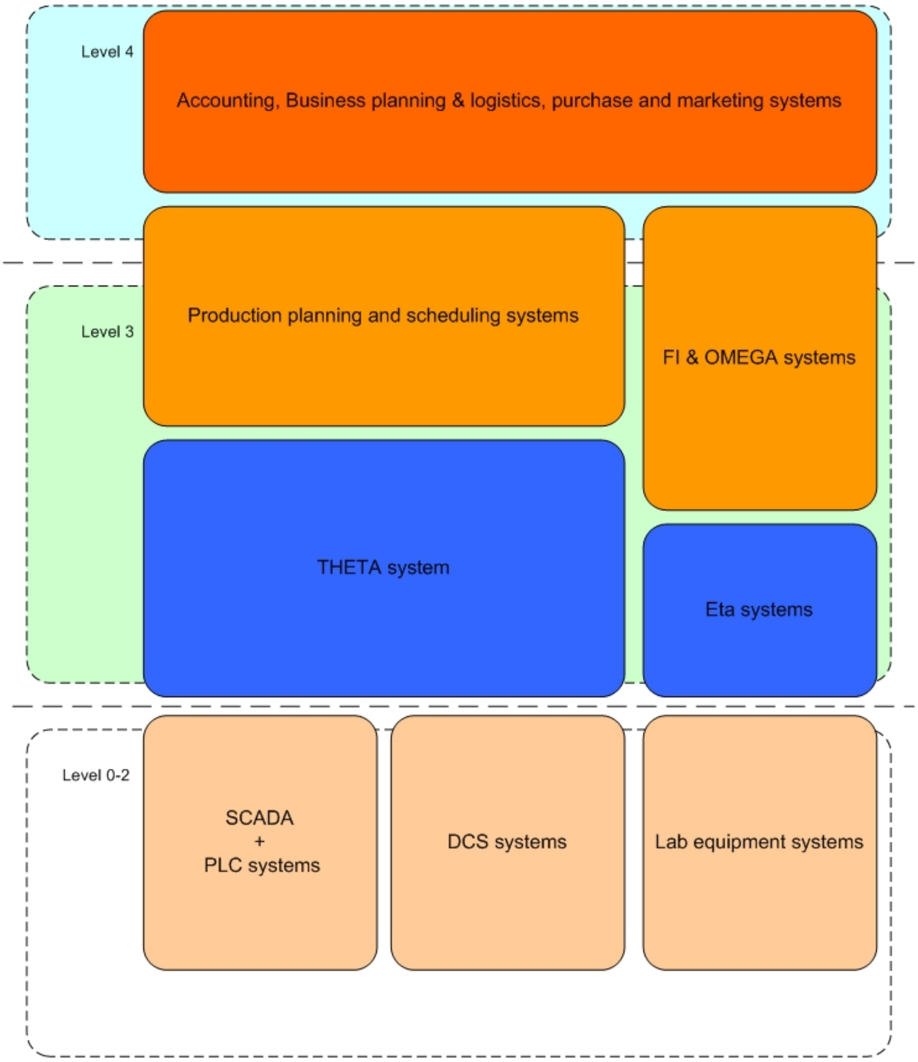

Level 4
Accounting, Business planning & logistics, purchase and marketing systems
Level 3
Production planning and scheduling systems
FI & OMEGA systems
THETA system
Eta systems
Level 0-2
SCADA
+
PLC systems
DCS systems
Lab equipment systems

*Fig 4.5 General model for systems involved in manufacturing of pharmaceuticals within Sweden Operations*

## 4.5 The DELTA architecture

The network structure or network solution that is used to connect the production with the corporate network within Sweden Operations is called the DELTA network service or the DELTA architecture.

DELTA was designed to provide both a high level of IS security and connectivity for the process automation system at the Södertälje site. The intention with DELTA is also to offer advantages of scale in forms of management and shared computer services. [44]

The architecture defines six major network or types of network segments:

- The corporate network

- The EPSILON segment

- The ZETA segment

- Production area networks

- Networks for the lab systems in production.

- The AstraZeneca corporate network is called GAMMA and is here modeled as a single entity. [44]

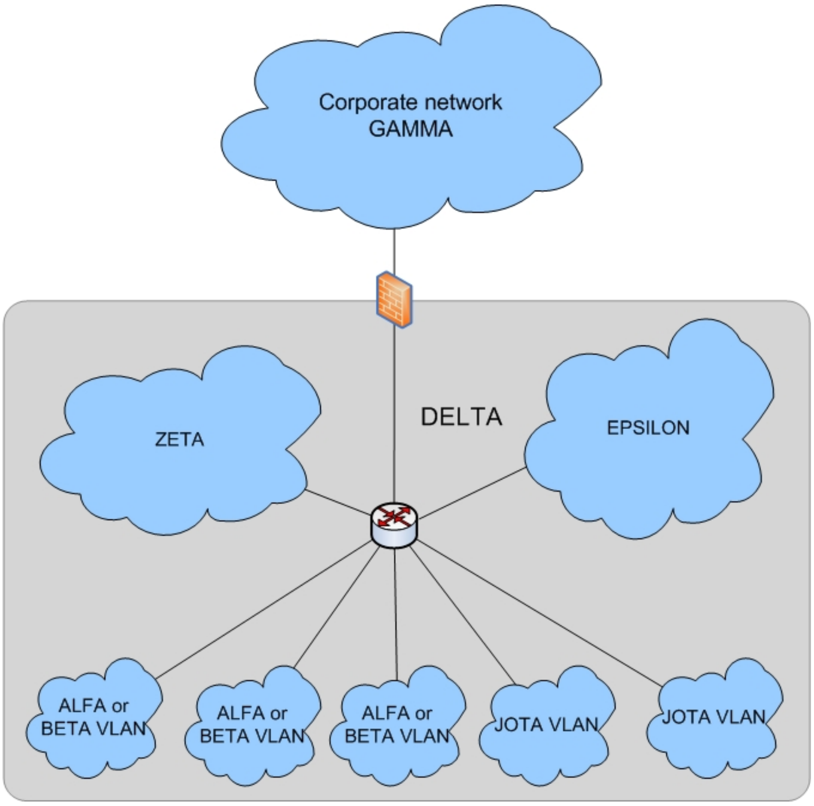


*Fig 4.6 The DELTA architecture*

Most of the production areas at the Södertälje site are today connected to the DELTA network. The production areas are geographically grouped at the Gärtuna and Snäckviken sub-sites into different factory buildings and have VLANs that are structured after the different factory buildings. [73]

No hardware is shared between the DELTA network and the corporate network. With this segmentation the production can be completely isolated from the corporate network. This segmentation also decreases the vulnerability to disturbances of communications and possible virus outbreaks in the corporate network.

The DELTA network service consists of the EPSILON and ZETA VLANs and the VLANs in the production areas and lab departments, a physical network that connects EPSILON and ZETA with the production areas and lab departments, and a physical firewall-protected connection between the corporate network and the central router. All communication with the corporate network is logically defined to be performed from EPSILON. The EPSILON segment is the DMZ in DELTA and also provides central infrastructure services. ZETA provides a network for different services and applications that are used by more than one of the production or lab VLANs. [44]

Included in the services provided by the DELTA network service are also client PC platforms (computer and operating system) for production (SESO-PRD client) and laboratory systems in production (SESO-LAB client). The intention with standard clients is to decrease cost for process automation and lab systems. The clients are provided with Microsoft Windows 2000 and anti-virus software. [44]

Process automation systems that use non-standardized computers have clients that might run on different operating systems software or is a special client that is needed by some specific automation equipment.

The DELTA administration is responsible for the DELTA network, the network, servers and systems in EPSILON and for maintaining the ZETA segment network. The DELTA administration is also responsible for the hardware and operating systems on the systems that operate from the ZETA segment. The information stored or used in the services and software applications provided from EPSILON and ZETA is owned by the consumer of the service. The DELTA administration is also responsible for maintaining the networks in the DELTA connected production and lab buildings, and finally for the hardware and operating systems on the standard clients. [44]

For example, the information and systems in THETA belongs to the system owner of the THETA system. At same time, the THETA system has servers in the ZETA segment, which falls under DELTA administration supervision. Therefore the DELTA administration is responsible for the hardware and operating systems on the servers that THETA uses but not for the special THETA software applications. For EPSILON the DELTA administration is responsible for network, hardware, and operating systems and for providing the service but not for the data stored and used by the service. This belongs to the consumer of the service. [44]

### 4.5.1 The DELTA network, servers and databases

The DELTA network consists of a physically separated network with access points in the connected production and lab buildings, the EPSILON and ZETA segments and a firewall-protected connection to GAMMA. The primary function of the network is to deliver a communication service (the DELTA network service). Hardware in DELTA also consists of servers and databases in EPSILON and ZETA, that offer different applications and services (EPSILON central infrastructure services and ZETA applications) for users in production and lab. Thus the hardware that DELTA consists of is a physical network, network equipment and servers and databases. [44]

Systems in the different production areas and JOTA VLANs are only allowed to communicate with applications and services in ZETA and EPSILON. No communication is permitted between different production area VLANs and JOTA VLANs. Applications in ZETA are only allowed to communicate with the different production areas, JOTA VLANs and with EPSILON. The corporate network is only allowed to communicate with EPSILON through the firewall. All this is physically and logically defined in the network. [44]

### 4.5.2 The EPSILON segment

EPSILON is a separate VLAN and the demilitarized zone (DMZ) of the DELTA architecture. A DMZ is network zone that provides an extra protective layer between two other zones. In the DELTA context EPSILON works as a DMZ between the corporate network and ZETA, the production area VLANs or the JOTA VLANs.

The servers that EPSILON uses are stored in protected server rooms on the site. The servers are used for managing the network and to provide the central infrastructure services. [44]

Central infrastructure services included in EPSILON are:

**Fileservers**
This service provides data storage for different applications and systems in production and lab.

**Databases**
This service provides different databases for different systems and systems in production and lab.

**DELTA application portal**
This service provides a secure access for applications and users in the corporate network to systems and applications inside DELTA (systems in ZETA, production and lab). The service provides indirect access to the systems inside DELTA.

**Print service**
Central print management and printers for users in production and lab.

**Time synchronization**
A central service for synchronization of correct time configurations on the systems and applications used in ZETA, EPSILON, production and lab.

**Active directory**
This service provides access to AstraZeneca login accounts. This is more efficient and secure than to provide special login and account management for authentication and login on clients in the different production areas and on the lab systems.

**Antivirus**
This service is used to provide antivirus updates to systems inside DELTA and in the production area networks. The service uses the global AstraZeneca antivirus infrastructure.

**Backup for central services**
This service offers backups to the systems used for the EPSILON central services described above.

**Inventory and configuration database**
A system that keeps track of and stores information about installed hardware and software on clients in production and lab.

**Backup for local systems**
A backup service for clients and systems in production and lab. Provides a possibility to make ‘disc-images’ or hard drive copies. The service is not intended to be used for backup of data from production and lab but to be used as way for quick reinstallation of operating systems and other software on process automation systems. The service is mainly intended for the clients in production and lab.

The IS security level in EPSILON is maintained as AstraZeneca GOLD standard or as ‘other critical devices’. [32] [50]

### 4.5.3 The ZETA segment

The ZETA is a separate VLAN for applications that are used for collecting, assembling and reporting information from processes and equipment in the different production areas and lab systems. The intention with ZETA is to provide advantages of scale and increase the IS security level by placing all systems in ZETA that are used by more than one production or JOTA network. The use of a ZETA segment also enables IBM support for hardware and operating systems of the systems that have servers in ZETA.

The most important part of ZETA is the THETA system. The information stored in THETA is used for batch reports and for optimization and tuning of processes and equipment used in the production (described above). There are also Eta systems in ZETA. These systems are used for storing data from lab equipment in production. [44]

The DELTA administration is responsible for the network and the hardware and the operating systems on servers in ZETA. The servers are stored in protected server rooms on the site. IS security on Servers are maintained as AstraZeneca SILVER standard.

### 4.5.4 Production area VLAN

In this study there is considered to exist two main different variants of production area networks or VLANs. PLC based production or DCS based production area VLANs.

In BETA almost all of the PLC + SCADA system are connected to the production area VLAN. Some SCADA systems are operated by one client but the majority use two clients. The execution of commands to the control equipment is performed from the clients. The clients communicate with THETA in ZETA and the DELTA infrastructure through scanning node servers. The scanning node servers assure that all communication is transformed into communication protocols that are suitable for the systems in THETA. [68]

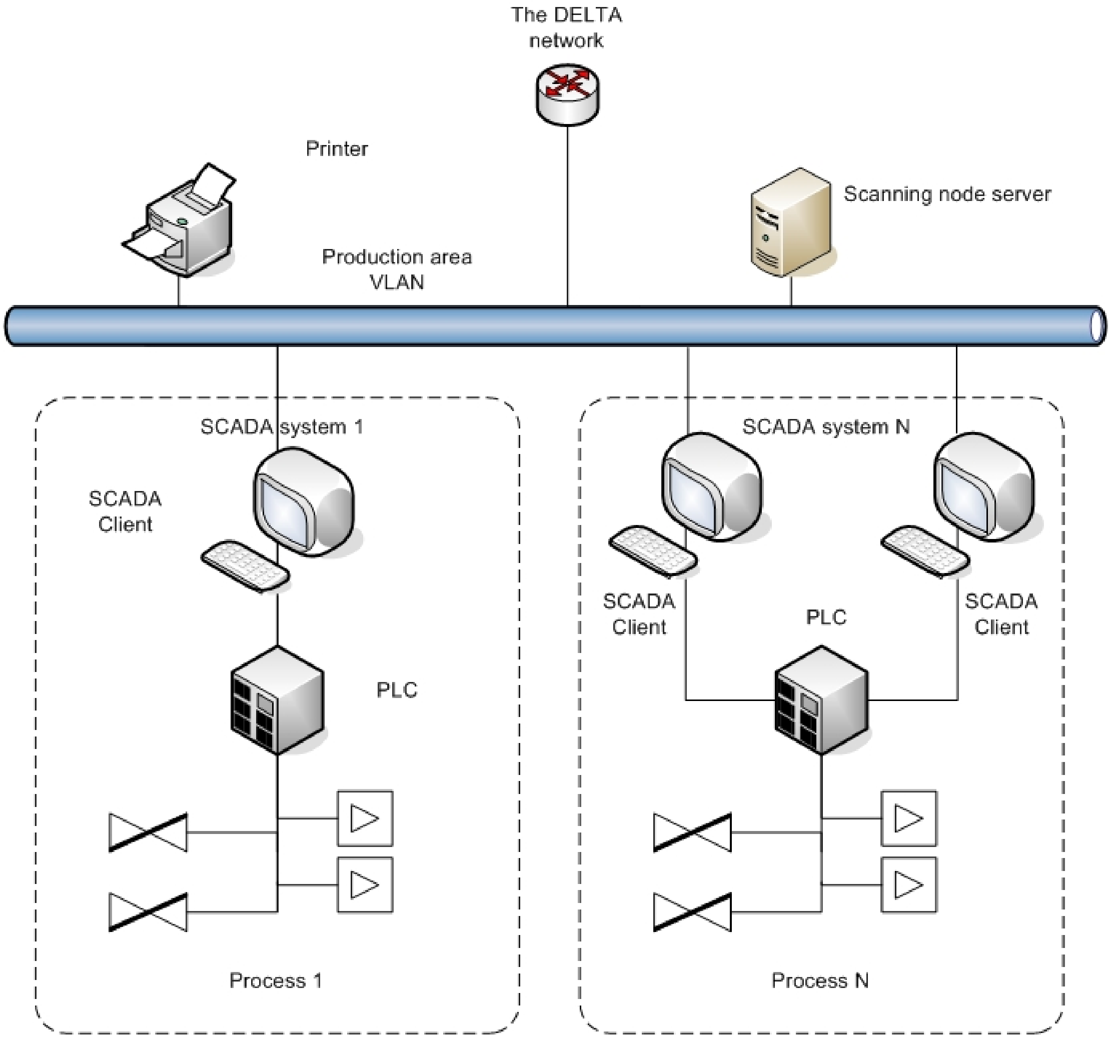


*Fig 4.7 General model for PLC based production area VLAN (BETA)*

DCS based production is mainly used in the manufacturing of API. In the ALFA plant, the DCS equipment is stored in a separate room under an operator control room. Clients are placed in the operator room and in direct connection to the centrifugation and drying equipment. Every segment in the ALFA plant has two clients assigned in the operator room. This assignment is only for practical reasons and the different segments and DCS systems can be operated from any client on the network in the building. [45] [58]

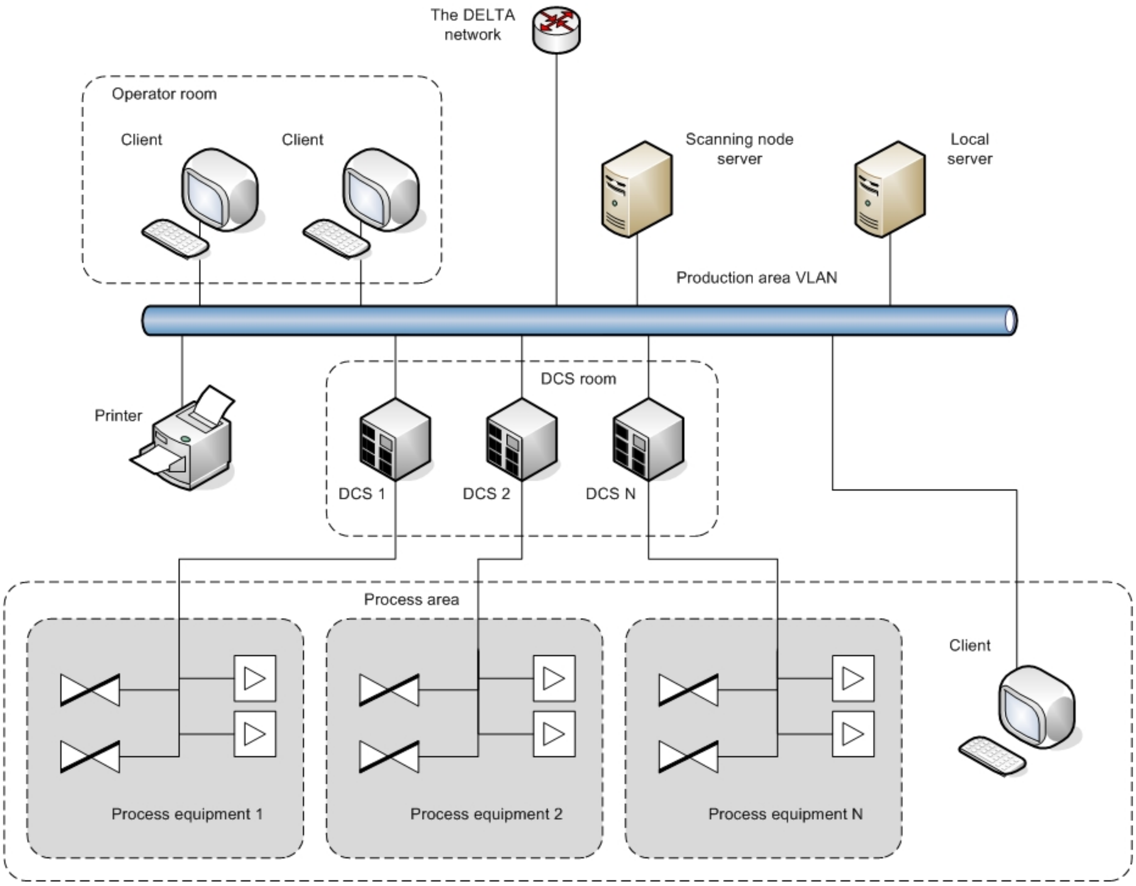


*Fig 4.8 General model for DCS based production area VLAN (ALFA)*

The scanning node server is used to translate information from production equipment prior to sending it to the THETA system. The local server is used for storing process history and recipes (program instructions) for the DCS system.

The DELTA administration is responsible for the network and the hardware and operating systems on the standard clients. Local system owners and managers are responsible for the control system applications and other software on the clients.

Today mostly non-standard clients are used in ALFA and BETA. Responsible for hardware, operating systems and applications on non-standard clients are local system owners and managers. [58] [57] [62] [81]

The IS Security level in production area VLANs is maintained as BRONZE or 'Securely isolated devices'. [32] [50]

### 4.5.5 Jota VLAN

The Jota VLANs are networks used for connection of the lab systems (that are used in manufacturing) to the DELTA network. The Jota VLAN basically provides a network service for the lab clients and the connected lab equipment and systems. As described above, the lab personnel perform lab tests and measurements with support of the lab equipment and systems. The results of these tests are printed and then manually typed into the FI and OMEGA systems. These systems are operated from the corporate network and are therefore not addressed in this study. [59]

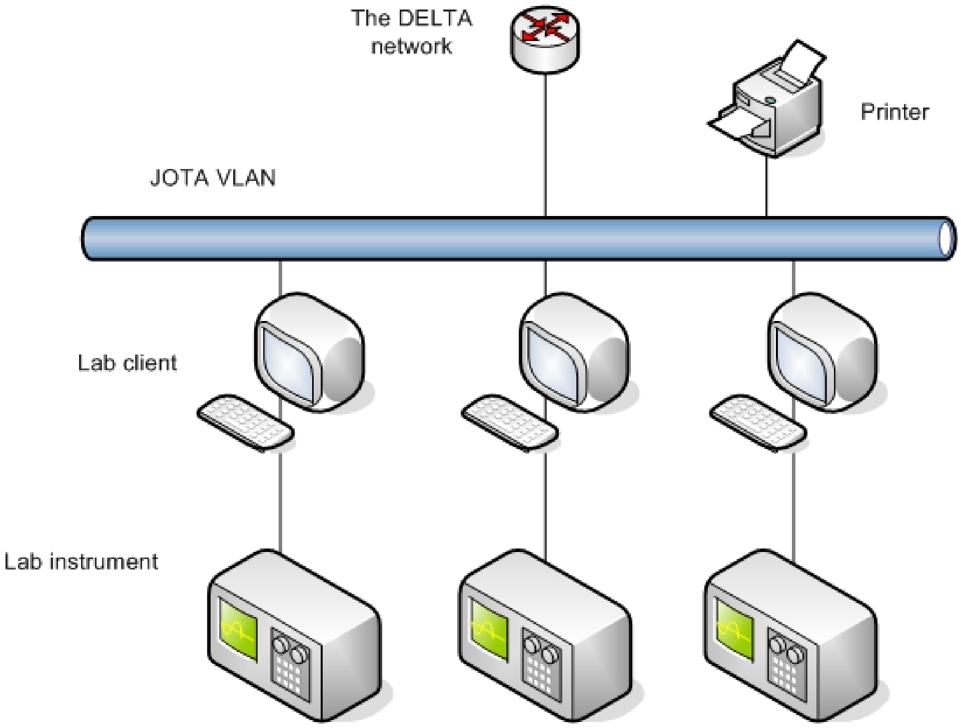


*Fig 4.9 General model for a Jota VLAN*

Some lab systems are of client-server type as described above. These systems have clients in the JOTA VLANs and servers in the Eta systems in ZETA.

The DELTA administration is responsible for the network and the hardware and operating systems of the clients. Local system owners and managers are responsible for the applications on the clients.

The IS Security level in JOTA VLANs is maintained as AstraZeneca BRONZE standard or ‘Securely isolated devices’. [32] [50].

### 4.5.6 The corporate network (GAMMA)

The corporate network (a WAN) is not deeply analyzed in this study. The corporate network is called GAMMA and is divided into local campus networks for the different AstraZeneca sites. It consists of network equipment, PCs and servers. Systems involved here are concerned with activities on level 3 and 4 in the ISA hierarchical model and other activities like research and marketing. The campus network is connected to DELTA, the Internet and other campus networks.

The IS Security level is maintained as AstraZeneca SILVER standard in the corporate network. [32]

## 4.6 A reference architecture for the DELTA context

To connect with the ISA 99 standard, this section summarizes this chapter into a reference architecture for the systems and networks within the DELTA context. The reference architecture is suitable for the scope of this study and for a management view of the IS security work in the production networks within Sweden Operations.

This reference architecture is used for evaluation of the DELTA architecture and implemented IS security (chapter 5), identification and analysis of IS security risks (chapter 6) and for developing an ISA 99 IS security program for DELTA (chapter 7). The reference architecture also provides a background for analysis of IS security issues due to the implementation of an MES/EBR system (chapter 8).

| Network | Maintained AstraZeneca IS security standard level |
|---|---|
| GAMMA | SILVER |
| EPSILON | GOLD |
| ZETA | Servers are maintained as SILVER |
| Production area VLAN | BRONZE |
| JOTA VLAN | BRONZE |

*Table 4.1 AstraZeneca IS security levels*

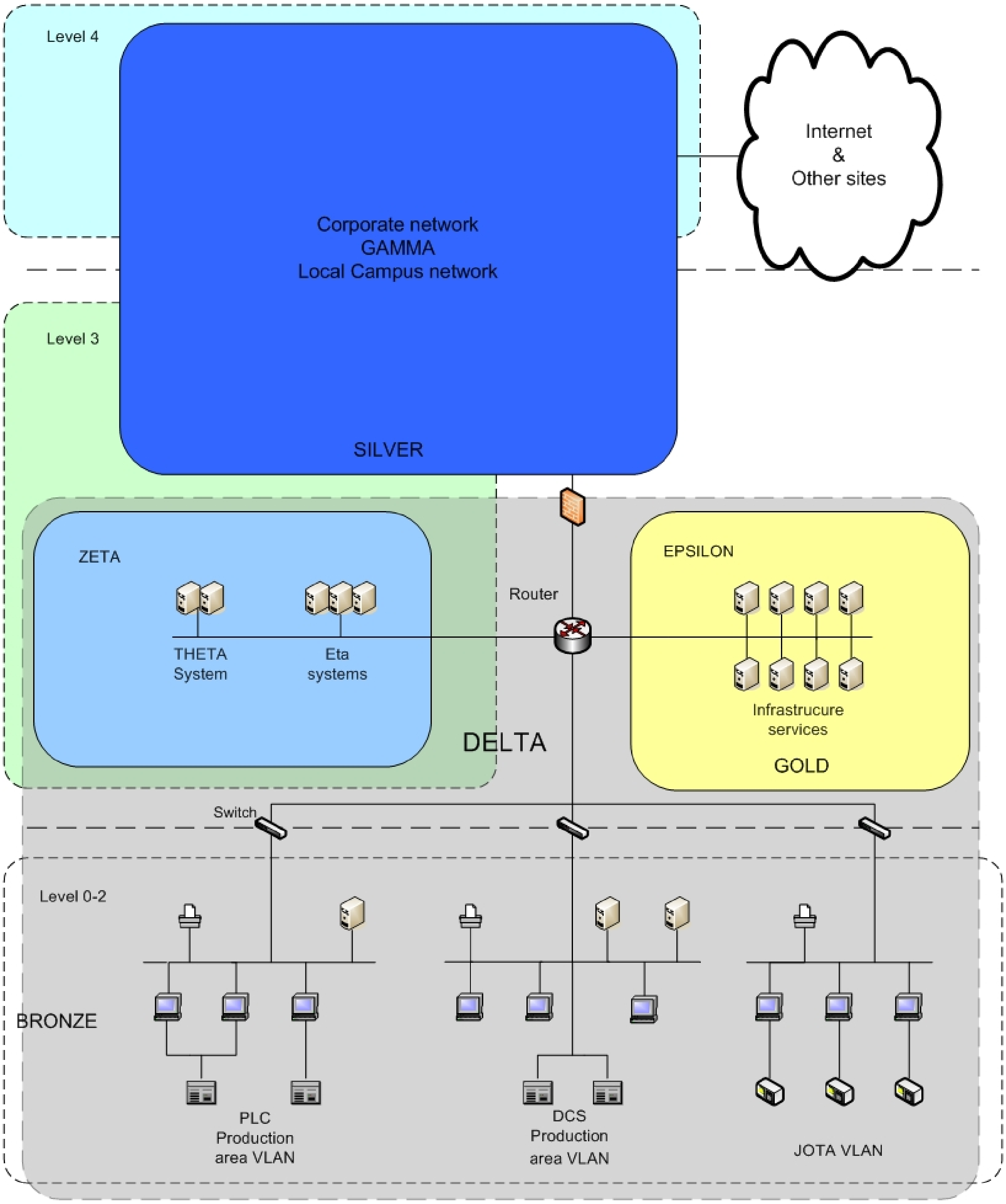


*Fig 4.10 A reference architecture for systems and networks within the DELTA context*

# 5 Evaluation of the architecture and IS security level compliance

## 5.1 Overview

This chapter analyse the implemented DELTA architecture and IS security measures through the three criterions specified in the theory section; Architecture security and IS security program implementation, Architecture scalability and manageability and Architecture security versus cost.

*The analysis is made through connection of current available IS security standards concerning network architecture in connection to production systems (presented in the theory chapter). It is strongly recommended that the reader of this chapter study the theory chapter and preferably also the involved standards, prior to reading this chapter.*

Standards used in the Architecture security and IS security program implementation criteria are:

- AstraZeneca Secure network Isolation of process automation computer systems.

- AstraZeneca Mandatory standards and good practice for the security of process automation systems.

- NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.

- NIST Guide to Supervisory Control and Data Acquisition (SCADA) and industrial Control Systems Security.

- Department of Homeland Security Control Systems Cyber Security: Defence-in-depth strategies.

- ISA 99 part 2.

Standards used in the Architecture scalability and manageability criteria are:

- NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Network.

- NIST Guide to Supervisory Control and Data Acquisition (SCADA) and industrial Control Systems Security.

Standards used in the Architecture security versus cost criteria are mainly the NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.

The architecture and all systems in process automation networks are not empirically investigated due to the limitations of the study. The empirical foundation of the study is built on AstraZeneca policies, AstraZeneca SOP, RUT, BaDS and system documentations and observations and interviews.

The analysis is conducted with a perspective that emphasizes an architecture that will offer a cost effective and secure environment for process automation systems. Where effective or necessary it also demands cooperation from process automation system operators, system owners and managers as well as senior management. The architecture is not the solution for all security problems. According to ISA 99, IS security is an organizational challenge that affects all levels of the ISA hierarchical reference model. [14]

## 5.2 Architecture security and IS security program implementation

### 5.2.1 AstraZeneca Secure network isolation of process automation computer systems

Compliance of the overall principles for IS security protection of process automation systems.

**a.**
Overall security policy available for IS security levels, operating systems and the use of anti-virus on process automation systems. [31] [32] [81]

**b.**
Security policy and initiatives exist for hardening of process automation system. The implementations of the policies differ within the different production areas. Standard client platforms are considered to be more secure than non-standard clients. [31] [32] [78] [81]

**c.**
There are routines and SOPs available for control of local unauthorized access and connection of portable computer equipment.

The DELTA architecture prevents unauthorized remote access to process automation systems and networks from the Internet. However, vendors of automation process equipment might install modems that are left behind and can be used for direct dial-up access or war-dialing attacks on process automation equipment.

There exists a security policy for remote access control from trusted computers within the AstraZeneca networks. All computer equipment must be checked for virus and approved before being connected to a production area or JOTA VLAN. [49] [52] [73]

**d.**
Not fully fulfilled. All traffic flows to, from and within process automation networks and all dependencies on external systems are identified. A risk assessment on the impact of loss or disruption of the traffic flows to the dependent systems is not performed. The suggestion is that the result of this study might be important input for a future risk assessment analysis. [44]

**e.**
*The DELTA reference architecture presented in chapter 4 is considered to comply with the requirements in the document.*

According to the document the firewall between GAMMA and DELTA should be maintained as fully open during normal operations. The firewall is today configured to during normal operations only allow communication between predefined systems in GAMMA and within DELTA. Thus the document is not fully implemented in order to increase the IS security level in the DELTA network and process automation systems. [32] [50] [73]

**f.**
A global policy for remote access to the process automation systems exists.  How well this is communicated through the organization is unknown. Remote access from outside AstraZeneca to process automation systems at the Södertälje site must always be approved by LISSM. [38] [73]

### 5.2.2 AstraZeneca Mandatory standards and good practice for the security of process automation systems

Compliance of the mandatory standards and good practices for IS security protection of process automation systems.

**Establish ongoing governance**
There exists AstraZeneca policies, SOP and RUT for roles and responsibilities for IS security in process automation systems. Those documents cover most areas of IS security but are intended for system owners and users. The impression is that the DELTA IS security level would benefit from having a clear program for IS security and also a policy towards senior management. The policy for senior management should explain the benefits and costs with the implemented architecture and IS security protection measures.

**Implement secure architecture and processes**
This document provides a clear policy for how to implement a secure architecture and IS security environment for process automation systems.

*The DELTA architecture is considered to comply with the secure isolation aspects (except for the firewall configuration). There are process automation systems that require approval of exceptions from AstraZeneca Global IS Security and many exceptions that will require approval from site LISSM.*

Knowledge about exceptions is collected by the site LISSM through the AstraZeneca ‘Traffic light’ compliance process. [44] [65] [81]

**Understand the residual business risk**
This is in principally fulfilled. No document for IRM (Integrated Risk Management. AstraZeneca procedure for risk assessment) document for DELTA exists. This study can be seen as input for a future IRM process for the DELTA context. [56]

### Establish response capabilities

There exist documents for responsibilities for DELTA, the systems in production and the systems in the ZETA segment. Documents and responsibilities for incident management exist for the campus network on the Södertälje site. This includes the DELTA network. IBM is responsible for maintaining this. [73]

### Improve awareness and skills

Currently there are no major efforts for increasing awareness and skills about IS security in the production. There exist training frameworks for computer users in general. This includes a computer user's code of conduct and a small course, before access to the Internet is granted. A suggestion is to provide operators and personnel that work with process automation systems with training or information in order to raise the skills and awareness about IS security threats.

There is currently no clear document available for senior management to explain the usefulness, benefits and risks with the DELTA architecture. This might be included in a business case for a DELTA security program

### Manage third party risks

AstraZeneca Engineering and local production and lab project managers and system managers handles the risks from vendors and support organizations of process automation systems. The IS security risk is only one of many risks involved in the projects for purchasing and implementation of process automation systems. Depending on various factors, all requirements in projects are sometimes not possible to meet. IS security risks are in general addressed, but not always. This means that hardening of process automation systems, patching of operating systems or the use of anti-virus software not always is possible. [61]

All connection of computerized equipment (that belongs to external support personnel or vendors of process automation systems) in production areas is controlled through local SOPs. There exist routines for virus scanning of third part computer equipment prior to being connected to the DELTA network. If needed, AstraZeneca will provide data from Internet but not through directly connecting the process automation systems to the Internet. [52] [66]

### Engage projects

When AstraZeneca Engineering manages projects for purchasing of automation equipment there is no clear document or routine for including IS security in the project specifications. The common practice is to work in cooperation with the system vendor and future system owners to implement IS security measures.

Projects for increasing IS security within the DELTA context are initiated continuously. Examples are ongoing hardening of process automation systems and use of modern and more secure operating systems on clients for process automation systems. Currently this document is being implemented in the production within Sweden Operations. [61] [73]

### 5.2.3 NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks

**Architecture security**
The DELTA architecture match the firewall deployment design (nr 8 Firewall and VLAN-based Process Network Combination) presented last in the document. This design is rated as 4.5 of 5 in the security aspect. According to the document this design is very secure provided that a demilitarized zone (DMZ) is used. Since this is the case for the DELTA architecture it can be concluded as a good solution in the security perspective. The drawback with the design is the scenario where the DMZ security is compromised. This will lead to possible infections and security problems in a majority of the control systems networks. Thus the applications and hardware in the DMZ must be hardened as much as possible.

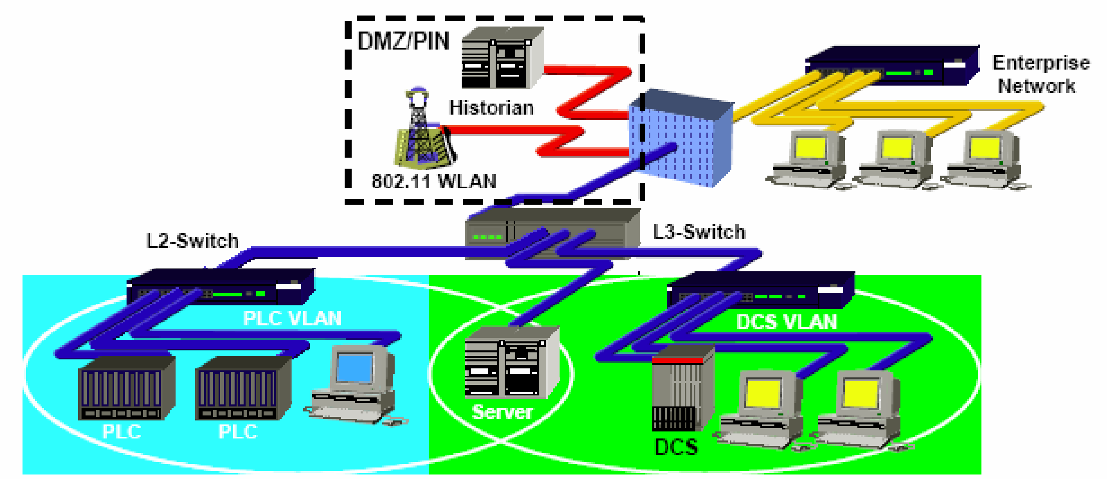


*Figure 5.1 Design nr 8, Firewall and VLAN-based Process Network Combination (copyright NISCC)*

The only solution presented in the document that provides a more secure design is the Paired Firewalls between Process Control network and Enterprise network (design nr 7, 5 out of 5 in the security aspect).

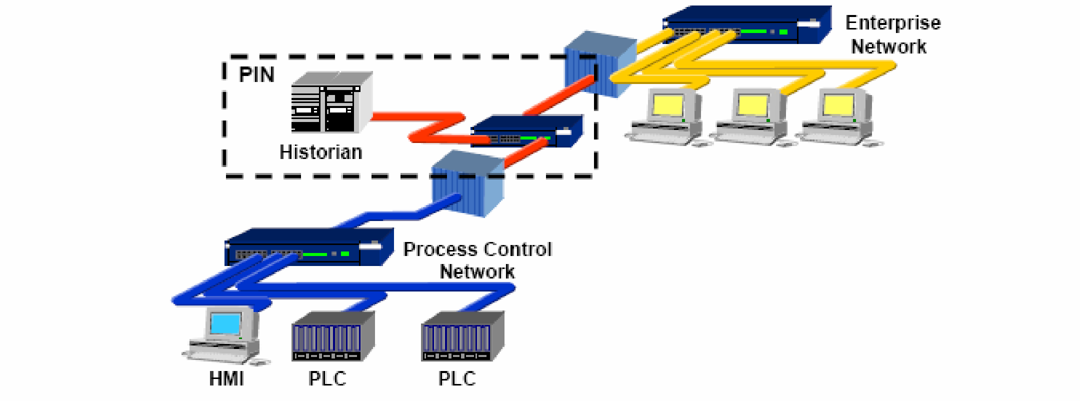


*Figure 5.2 Design nr 7, Paired Firewalls between Process Control network and Enterprise network (copyright NISCC)*

### 5.2.4 NIST Guide to Supervisory Control and Data Acquisition (SCADA) and industrial Control Systems Security

**Architecture security**
This document recommends an architecture or network segregation that at least implements three different zones, where one is a demilitarized zone. The DELTA architecture matches something between network segregation model 4 and 5 that are presented in the document (Firewall with DMZ between Corporate Network and Control Network or Paired Firewalls between Corporate Network and Control network). Both models are concluded as a secure way of segregating the production network from the corporate network. Model 5 provides more in-depth protection but increases complexity and cost. The services and applications provided from EPSILON and ZETA match recommendations for services and applications that are to be placed in a DMZ.

Thus DELTA can be concluded to comply with security recommendations in the document. The document also concludes that the primary security risk is that if systems in the DMZ are compromised or infected. Then systems in the DMZ can be used for attacks on control networks through permitted communications. Thus the applications and hardware in the DMZ must be hardened as much as possible. The document also recommends the use of different antivirus software for DMZ than used in the corporate network to decrease the likelihood of this scenario.

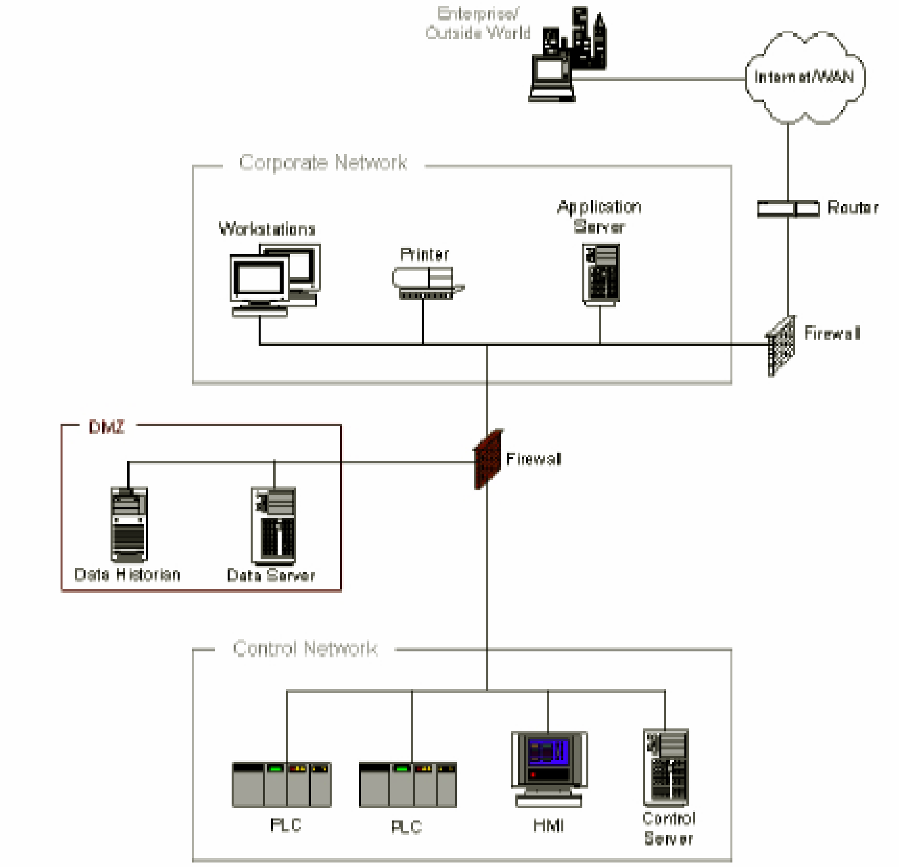


*Fig 5.3 Firewall with DMZ between Corporate Network and Control Network (copyright NIST)*

### 5.2.5 Department of Homeland Security Control Systems Cyber Security: Defence in depth strategies

**Architecture security and defence-in-depth strategy implementation**
The Department of Homeland Security Control Systems Cyber Security: Defence-in-depth Strategies, recommends the deployment of firewalls in combination with DMZs in order to protect the control systems LAN. Thus the DELTA architecture provides a good solution in aspects of security.

Intrusion detection systems are used in GAMMA and there exists overall security policies. The security might benefit from more detailed policies and a more clear communication of the security policies towards process automation system owners and production management. There exist no special IS security training initiatives for operators of process automation systems. There exist BCPs and DCPs for incident responses. Thus the IS security level and implemented architecture provides a depth in defence protection (except for the training initiatives) for the process automation systems at the site.

### 5.2.6 ISA 99

**Security program implementation**
There exists no clear security program for the networks and systems used in the production at the Södertälje site. There exists a variety of global and local policies, documents, SOPs and RUTs for security in production. Some documents are intended for specific systems or networks. Some documents are very generic and address systems on a variety of the different levels in the hierarchical reference model.

According to ISA 99 a common error in addressing cyber security (IS security) is to break down the problem to specific systems and networks. Cyber security is a much larger challenge that must be addressed in a holistic manner. Cyber security can also be seen as more of a cultural and organizational task that must be addressed in multiple ways. ISA 99 therefore recommends the implementation of a cyber security management system (here referred to as an IS security program) in order to reduce IS security risks and to sustain risk reduction over time. [14]

The conclusion here is that the DELTA architecture and the IS security measures at the site lack a clear IS security program. Thus the implemented IS security measures within the DELTA network does not comply fully with the ISA 99 standard.

### 5.2.7 Compliance conclusions

| Standard | IS Security compliance | Comments |
|---|---|---|
| AstraZeneca Secure network Isolation of process automation computer systems | Mainly compliant | The DELTA architecture and implemented security in general fulfils the document. Risk assessment and configuration of the firewall deviates from the document. |
| AstraZeneca Mandatory standards and good practice for the security of process automation systems | Mainly compliant | The DELTA architecture and implemented security in general fulfils the document. There is also no clear policy for control of how the document is implemented in the operations. Many process automation systems must be further hardened and protected with anti-virus or require global or local exceptions. |
| NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks | Yes | DELTA corresponds to design 8. Security 4.5 out of 5. DMZ must be hardened as much as possible. |
| NIST Guide to Supervisory Control and Data Acquisition (SCADA) and industrial Control Systems Security | Yes | DELTA corresponds to model 4 and 5. DMZ must be hardened as much as possible. Should use different antivirus software in DMZ than on corporate network. |
| Department of Homeland Security Control Systems Cyber Security: Defence-in-depth strategies | Yes | With the connection to GAMMA the architecture and IS security measures provides a defence-in-depth strategy. There should be some sort of training initiatives for operators of process automation systems. |
| ISA 99 | No clear IS security program. | Clear view on IS security as important. No clear security program. |

*Table 4.1 IS security standards compliance*

## 5.3 Architecture scalability and manageability

### 5.3.1 NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks

According to the NISCC document, the design model (nr 8) that DELTA can be compared with, offers excellent scalability (5 out of 5). Several production area networks and VLANs can be added without significant problems. Thus extra production areas can easily be added to a site.

The drawback of design model nr 8 is the added management complexity and cost (manageability 3 out of 5). However for a large manufacturing site there is a lot of complexity in computer systems and networks incorporated anyway. Thus the drawback of manageability more applies to smaller manufacturing sites.

The outsourcing agreement with IBM also implies that the possible manageability problems with the architecture will be addressed by IBM and therefore not should be a major problem for AstraZeneca and Sweden Operations. It is very important that IBM fulfils its part of the agreement, considering especially incident management and availability and accessibility of the DELTA network,

### 5.3.2 NIST Guide to Supervisory Control and Data Acquisition (SCADA) and industrial Control Systems Security

The most scalable control network and corporate network segregation architecture is the implementation of at least 3 zones where one is DMZ, according to the NIST document. Therefore it is concluded that the DELTA architecture offers a good solution in terms of scalability. Placing patch management, antivirus servers and other security services in EPSILON and ZETA offers advantages of scale and more controlled updates of software on process automation systems.

The DMZ architecture adds cost in terms of manageability and complexity according to the document.

## 5.4 Architecture security versus cost

The DELTA architecture offers a solution that according to the standards and guidelines provides a secure environment in terms of IS security. Comparing with a higher level of security (replacing the router with firewalls between the DMZ and the different production areas or increased segmentation) this will add some extra security but also most likely a lot of problems in terms of manageability. Comparing with a lower level of security (no DMZ) this will create an architecture that permits direct connectivity between the corporate network and process control networks. Considering the high vulnerability in process automation systems used for pharmaceutical manufacturing this is not a satisfying level of IS security. This will also violate global AstraZeneca IS security standards. [17] [31]

The main drawbacks with the architecture are the complexity and potential problems with manageability that is created. Big manufacturing sites with lots of different systems and production processes involve a lot of complexity in implementation and manageability of computer systems and networks. Since DELTA is intended to be applied on a large site involved in pharmaceutical manufacturing the manageability issue is not seen as a big problem if compared to the security and scalability level that the architecture adds. If the architecture is to be implemented on a smaller site there might be more inexpensive solutions for the same security and scalability level. Due to the outsourcing of the infrastructure service, this problem will also have to be addressed by IBM.

Advantages with the architecture are the security level, ability to use large-scale advantages and the ability to expand the architecture. Large-scale advantages include placing applications for security and production (that are used by more than one production area or system in the production) in ZETA and EPSILON segments.

## 5.5 Summary

According to current available standards the DELTA architecture is suitable for a large manufacturing site within Sweden Operations. It is considered as almost a best practice solution for a large manufacturing site with highly vulnerable process automation systems that demands a high level of IS security protection. It is less suitable for a small manufacturing site.

The architecture and implemented IS security safeguards in general comply with global AstraZeneca IS security standards. The security level and the effectiveness of the DELTA architecture would benefit from a clear security policy or security program. There exist policies, documents and SOPs for how to secure process automation systems and networks. Theses AstraZeneca policies aim for systems and networks on different levels or are in general intended for a specific system or a special kind of systems.

*DELTA provides a suitable architecture for a large manufacturing site within Sweden Operations, but would benefit from a clear and complementing IS security program.*

# 6 Identification and analysis of IS security risks

## 6.1 Overview

This chapter presents an IS security risk analysis of the systems and networks within the DELTA context. The objective is to identify the main risks and assess these risks in order to provide a background and a business case for the DELTA IS security program (chapter 7), find possible areas of improvements for IS security for the DELTA network and context.

The risk analysis uses the ISA 99 Zone and conduit model and is performed according to the Primatech Scenario-based approach for cyber security vulnerability analysis method.

## 6.2 Zone and conduit model definition

To connect with the ISA 99 standard, the first step in the risk analysis is to define zones and conduits from the reference architecture presented in section 4.5.

The idea here is to view the DELTA network as a conduit, the DELTA conduit. The different production area networks are divided into two different security zones based on if they use PLC or DCS automation systems.

ZETA and EPSILON are defined as separate security zones. The corporate network (GAMMA) is mapped as a separate security zone. The corporate network is here only viewed as a protection layer and a way for threats to enter. Therefore the GAMMA zone does only have attributes in the form of a security policy. Finally the JOTA VLANs are also defined as a separate security zone.

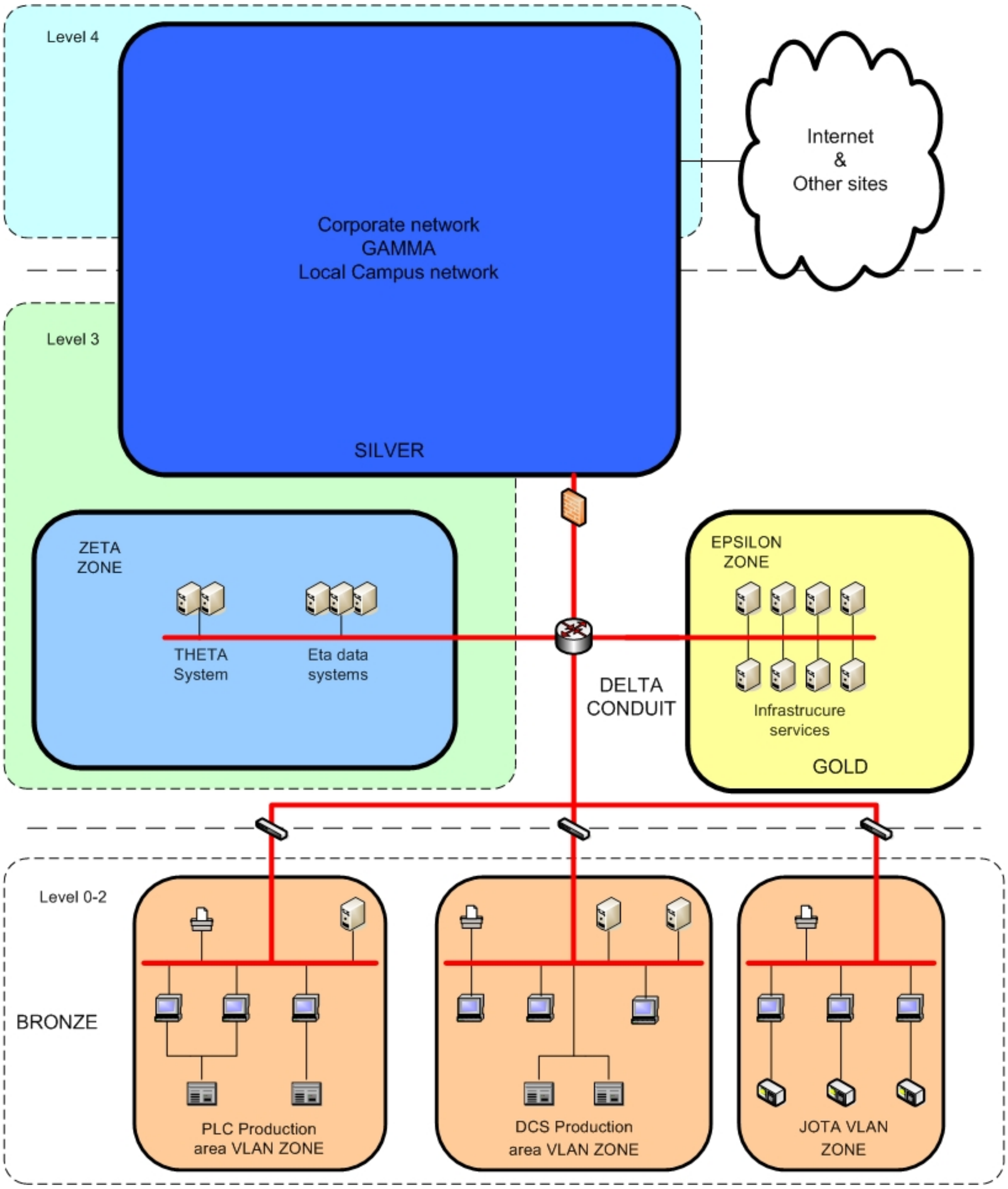


*Fig 6.1 Zone and conduit model*

## 6.3 Asset inventory

This section describes the assets that are considered being valuable for Sweden Operations within the DELTA context. The costs for loss of assets are estimated as loss of manufactured batches or the time that the production in the different production areas is forced to stop due to IS security incidents. The cost of loss reflects the worst possible consequences of the threat scenarios presented in appendix C. Only the lost production capacity or time is transformed into the financial impact rating criteria as described in chapter 3 and appendix A.

Costs for production areas being out of order are based on the refinement value (Swedish: Förädlingsvärdet) per day. This includes both direct and indirect costs. The refinement value is based on the assumptions that production is performed 46 weeks per year, five days a week, in three shifts per day and includes overheads and depreciations.

It is also assumed that if a production area is infected, then the packaging area that belongs to the production area is also affected by the stop. It is also assumable that work for restoring the process automation systems from an IS security incident, will be performed on both weekends and regular working days. This means that the cost for impacts only affect regular working days. [67] [72]

Information assets that is used and transmitted within the DELTA context is classified as confidential or internal depending on the estimated value for a competitor to AstraZeneca. The information is described in section 4.3.3. Confidential information is in general assumed to be of value for a competitor to AstraZeneca. The different information that is communicated, used or stored within the zones or the DELTA conduit is presented in table 6.2. [63] [70] [71]

### 6.3.1 DELTA CONDUIT

The DELTA conduit provides the communication between the different zones, thus the network and communication is viewed as an asset. The infrastructure services provided by DELTA (like login, data storage, backup services) are needed for the operation of the other zones. A loss of the DELTA conduit will cause the communication between connected production areas and the ZETA zone to halt.

The production areas connected to the DELTA conduit are:

- Gärtuna sub-site: Kappa, Lambda, BETA, My, Ny

- Snäckviken sub-site: ALFA, Xi, Pi, San, Koppa, Rho, Sigma, Tau

It is very difficult to estimate exact monetary numbers for the loss of production in all production areas. Therefore the total cost for the DELTA conduit being out of order for one day is estimated to the same as for Sweden Operations production ‘being out of order’ for one day. Today almost all production areas are connected to the DELTA network. Thus this figure is a slight over exaggeration of the present costs. [67] [73]

Information sent over the DELTA conduit is also considered as an asset. Information transmitted on the DELTA conduit is considered confidential or internal within Sweden Operations. The information is considered confidential to external organizations. The loss of information is considered to be costly for AstraZeneca but very hard to estimate in a monetary value. A lot of the information is also available in paper format (batch protocols and quality control protocols) in the production and lab environments. [60] [70] [71] [81]

Knowledge of the network architecture is assumed not to be of significant value since the network is built according to AstraZeneca standards and is protected by the GAMMA zone from direct attacks. The relevant standards are not confidential. [31] [32]

### 6.3.2 EPSILON ZONE

Assets in EPSILON are the servers that are used for the services that EPSILON provides. Examples of this include login services, web portals and communication services. This means that production area zones connected to the DELTA conduit are in general dependent on that EPSILON is working as intended. Thus the cost for EPSILON being out of order is the same as for the DELTA conduit. [44]

The information stored, used or communicated in the EPSILON zone is the same as for the DELTA conduit.

### 6.3.3 ZETA ZONE

Assets in ZETA are mainly the applications used by THETA and the Eta systems and the servers for these applications.

THETA has connected production areas at the Gärtuna sub-site and at the Snäckviken sub-site. [64]

Information stored in THETA is considered confidential. Assets here also include information from production for optimization and information for performing production. The loss of information is considered to be costly for AstraZeneca but very hard to estimate in a monetary value. [60] [70] [71]

### 6.3.4 Production area VLAN ZONE

Assets in the production area zone are:

- The processes and production equipment

- Clients (both standard and non-standard clients)

- PLC or DCS equipment

- Control systems software on clients and PLC or DCS equipment

- Information about pharmaceutical recipes or product formulation processes that are considered providing AstraZeneca with a competitive advantage. Electronic recipes and batch protocols.

- Quality of produced pharmaceuticals or batches. Batches manufactured in ALFA and BETA are valuable. [76] [77]

Under the assumptions described in section 6.3, the cost for BETA and ALFA being out of order one day is estimated to a significant cost. [67] [72]
[74]

Loss of information used in the production (i.e. electronic work instructions or product recipes) is considered not being confidential within Sweden Operations. The loss of information is considered to be costly for AstraZeneca but very hard to estimate in a monetary value. The information is also available in paper format (batch protocols and quality control protocols) in the production and lab environments. These are considered confidential.

Knowledge of the network architecture is assumed not to be of significant value since it is considered as standard network architecture.

### 6.3.5 JOTA VLAN ZONE

Assets in the JOTA VLAN zone are the clients, lab equipment and lab equipment software. There is no significant risk that manufactured batches that have to be scrapped because of malfunctions in lab clients.

Quality control protocols are available in paper format. These are confidential.

### 6.3.6 Summary of assets

Assets are the networks, process automation systems, servers, confidential and internal information and process automation systems and lab equipment. The cost per day for lost production and cost for loss of batches are presented in table 6.1. This only includes costs for loss of production capacity and scrapped batches as described above.

| | Cost per day for lost production | Cost for loss of batches |
|---|---|---|
| DELTA conduit | | |
| EPSILON zone | | |
| ZETA zone | | |
| PLC based zone (BETA) | | |
| DCS based zone (ALFA) | | |
| JOTA VLAN zone | | |

*Table 6.1 Cost for lost production and batches*

| Information | Confidential | Internal | Stored, used or communicated within |
|---|---|---|---|
| Master batch recipe material | | | - |
| Batch and quality control protocols | | | Production and Laboratory environments (in paper format) |
| Batch recipes (electronic work instructions) | | | ZETA, production area VLAN and the DELTA conduit |
| Batch report material | | | ZETA and the DELTA conduit |

*Table 6.2 Classification of information*

## 6.4 Zone and conduit security policies

### 6.4.1 DELTA CONDUIT

The traffic control of communication on the DELTA conduit is performed through the internal firewall, the use of anti-virus and predefined rules for allowed communication. The anti-virus is updated according to the rules of the EPSILON zone.

Traffic is not permitted between different production areas, between production areas and the corporate network and between ZETA and the corporate network (GAMMA). Traffic is allowed between ZETA and production areas and between EPSILON and all other zones. Traffic is permitted between JOTA VLANs and EPSILON and ZETA. No communication is permitted between different JOTA VLANs or between JOTA VLAN and production area VLAN. [44]

Communication between the zones inside DELTA and users in GAMMA is permitted through the DELTA Application Portal service. Thus users in GAMMA can indirectly communicate with the different production areas and ZETA. [44]

In the event of a 'Day zero attack' (GAMMA, DELTA, EPSILON and production severely infected by a virus that the anti-virus software not have been updated against) the firewall can be used for completely closing the communication to the corporate network. This can also be done as a preventive action. [73]

This paragraph presents the estimated recovery time for the DELTA conduit for different IS security incidents. [73]

### 6.4.2 EPSILON ZONE

Communication with the corporate network through the firewall is permitted. The firewall can be closed in the scenario of a virus threat. Communications with ZETA, production area VLAN zones and JOTA VLAN are allowed. [44]

IS security is maintained as AstraZeneca GOLD standard in EPSILON. All servers must run up-to-date antivirus software according to AstraZeneca corporate standards. [32]

Since EPSILON consists of servers there is no large demand for the use of e-mail. Thus no e-mail is used within EPSILON. The reason for this is also to reduce the IS security risks. [73]

Servers and computer equipment are protected in locked server rooms on the site.

This paragraph presents the estimated recovery time for the EPSILON zone for different IS security incidents. [73]

### 6.4.3 ZETA ZONE

Communication with EPSILON, production area VLAN zones and JOTA VLAN is permitted. [44]

Security is maintained as AstraZeneca SILVER standard on servers. All systems must run up-to-date antivirus software according to AstraZeneca standards. [32]

No e-mail is used on ZETA applications.

This paragraph explains the impact on THETA connected production areas if the THETA system is being disabled due to an IS security incident. [64]

The lab systems in the JOTA VLAN are not dependent on incidents in the ZETA segment. [59]

This section describes the estimated recovery time for the THETA system due to a severe IS security incident in the ZETA zone. A manufactured batch that is validated and approved is not affected by IS security incidents in the THETA zone. This means that AstraZeneca do not face the risk of having to recall distributed batches due to THETA zone malfunctions. There exist recovery plans in case of an infection or breakdown. [48] [60] [69]

### 6.4.4 Production area VLAN ZONE

Rules for communication permit traffic between production area zones and ZETA or EPSILON. No communication between different production area VLAN zones and with JOTA VLAN zones is permitted. [44]

IS Security in production area zones is maintained according to AstraZeneca BRONZE standard. Updates of operating systems and software on the clients in the production are made irregularly. Every time operating systems are patched the process automation systems have to be validated before the production of pharmaceuticals is allowed to continue.

Mostly non-standard clients are used today in BETA and ALFA. [83]

If standard clients are used they are provided with anti-virus software. Updates of antivirus software are performed regularly and patches to operating systems are applied on a non-regular time scale. [44] [50]

If non-standard clients are used there is no guarantee that the system is provided with anti-virus or protection against malicious codes or unauthorized access. There is also no guarantee that the clients are updated and patched. There exists a routine for this but it is not fully implemented or used. The different production areas maintain the security on the non-standard clients and the local servers in production. Thus there is no guarantee that non-standard clients are provided with anti-virus software or hardened against unauthorized operator manipulations. [58] [78] [44]

E-mail use and Internet access is prohibited on the clients in the production area zones. [73]

AstraZeneca security policies demands that all use of modems for vendor installation and support of process automation systems through remote access must be approved by the site Local Infrastructure Security managers (LISSM).

This section describes the current situation in the production areas (BETA and ALFA) used as references in the study. This includes estimated recovery time from IS security incidents and the IS security measures that are implemented to prevent incidents. [46] [52] [57] [58] [62] [66]

### 6.4.5 JOTA VLAN ZONE

Communication is permitted between the JOTA VLAN zone to the ZETA and EPSILON zones. Communication between different JOTA VLANs is prohibited.

IS Security in JOTA VLANs is maintained according to AstraZeneca BRONZE standard. The lab clients have anti-virus software. Patches to operating systems are applied on a non-regular time scale. Due to that the lab equipment not have to run continuously it is easier to apply patches and updates on lab clients than on production connected clients. Operating systems and anti-virus software updates are applied regularly. [32] [59]

E-mail use and Internet access is prohibited on the clients in the JOTA VLAN zones. [73]

This paragraph describes the possible impacts of IS security incidents and IS security measures that are present on the lab systems. [47]

### 6.4.6 GAMMA

GAMMA and connects to the Internet and internal AstraZeneca networks (including DELTA). Since GAMMA includes a great variety of systems that not are relevant for this study, only the connection to Internet and DELTA will is described here. This section also describes how virus and hackers possible will reach the DELTA conduit.

Antivirus updating and operating systems patching is performed regularly. GAMMA firewalls and infrastructure are considered to provide protection to DELTA against Denial-of-service attacks. [50] [32] [73]

To summarize; GAMMA provides both protection and a threat with the connection to the Internet and corporate office computers.

## 6.5 Access requirements and controls

### 6.5.1 DELTA CONDUIT

To be able to access systems in ZETA and production via the DELTA application portal, AstraZeneca personnel must apply for and be granted permission. The DELTA manager approves administrator access. The manager that is responsible for the personnel grants other access. [73]

IBM is responsible for the network and the services that are provided and thus also for the access requirements and controls.

DELTA services comply with current corporate standards for passwords. [36]

### 6.5.2 EPSILON ZONE

Servers used in EPSILON are stored in locked server rooms. The different services do not share hardware (different servers for different services). [73]

Access to systems in EPSILON is controlled by the DELTA manager and managed by IBM. Users with administration status authority are strictly controlled. Normal users are less controlled. [73]

### 6.5.3 ZETA ZONE

ZETA servers are stored in locked server rooms on the site. [81]

To be able to access THETA applications in ZETA through the DELTA application portal, AstraZeneca personnel must apply for and be granted permission. Access is approved by OITP and managed by IBM. Personnel that are granted access have in general very limited access rights. The access is regularly revised. [54] [64]

External personnel (for example consultants) use the same procedure and routines for applying for access to THETA systems. Duration of the access is always limited. System providers and support are also controlled by various business contracts. [54] [64]

### 6.5.4 Production area VLAN ZONE

To access the process automation systems, AstraZeneca personnel must first have access to the plant building. Access to the process automation system clients is protected by login and passwords. Operators and personnel that operate the clients are assigned different authority levels depending on the level of responsibility and education. This authority applies for the process-control computer system. [55] [81]

AstraZeneca policy demands that unnecessary ports (like USB or CD-ROM) on clients are closed and that operating systems are hardened to prevent manipulation.

This does not guarantee that all ports are closed and the systems are properly hardened. [31]

For standard clients there exist implementations for hardening and access constrains in the operating systems. Sometimes this is also included in the control system software. [78[

For non-standard clients there are only operating systems hardening if it is included in the control system software or installed by the local CTS department. Thus the standard clients in general have a higher level of security. [78] [81]

The networks in production area zones permit connections of portable computer devices like laptops. AstraZeneca laptops cannot be assigned IP-addresses via DHCP and are therefore not considered to posses a major virus infection threat. For 'external' laptops it is possible to assign an IP address. Telnet, FTP and http communication protocols are enabled after defining an IP address. All communication protocols require login for access to ZETA applications or EPSILON devices. [82]

### 6.5.5 JOTA VLAN ZONE

To access the lab clients, lab personnel must have physical access to the clients and proper login rights. Since the lab client is a standard client there exists work implemented for hardening and constrains for access in the operating system to prevent undesired manipulation.

There exist no special initiatives for hardening of USB, floppy drive and CD-ROM ports on lab clients.

The JOTA VLANs permits connections of portable computer devices like laptops. AstraZeneca laptops cannot assigned IP-addresses and are therefore not considered to posses a major virus infection threat. For 'external' laptops it is possible to assign an IP address. Telnet, FTP and http communication protocols are enabled after defining an IP address. All communication protocols require login for access to ZETA applications or EPSILON devices. [82]

## 6.6 Analysis of threatening picture for the DELTA context

This section describes the current threatening picture that is present to the DELTA context. The threatening picture is based on theoretical likelihood for possibility incidents due to malicious code, human errors and hostile intrusion threats and IS security incident history. This section also analyse the hacker possibilities for intrusion into the DELTA conduit. [4] [14] [26] [33] [66] [73]

## 6.7 Identified threat scenarios and vulnerabilities

Please refer to appendix C for the identified credible IS security scenarios that threatens the DELTA conduit and the different zones. The threats are assembled through observations, interviews, and system and network descriptions and based on the threats that are presented in the theory chapter.

The consequences represent the consequences of worst-case scenarios. The costs of the consequences are transformed into the financial impact scale (appendix A). Costs of halted production less than one day, cost for destroyed equipment, cost for lost batched or costs by loss of potentially important information are not transformed.

The likelihood of the different scenarios is derived in cooperation with AstraZeneca Local IS security managers and the Local IT infrastructure manager at the Södertälje site. The likelihoods are based on incident history, IS security threatening picture and the existing security measures that is presented in the Zone and conduit Security policy and Access requirement and control sections. The existing security measures affect the likelihood. [73] [79]

As a function of the likelihood and financial impact, the severity rating associated with each threat is summarized.

The conclusion is that the main IS security risks are:

- An unknown virus from GAMMA and the Internet, with major impact on all the different zones and the DELTA conduit (a Day zero scenario).

- IBM error that have major effects on both the DELTA conduit and the production area VLAN zones.

- Non-validated update or patching of the DELTA conduit and infrastructure prevent communications or network services.

- Major virus infection from a system provider in a PLC based production area zone.

- Major virus infection from direct-dial up access in a PLC based production area zone.

- Major incident due to remote access through a direct-dial up connection in a PLC based production area zone.

- Major incident due to virus outbreak from a non-standard client in a PLC based production area zone.

## 6.8 Evaluation of the DELTA architecture and implemented IS security measures from a risk perspective

An infection with a virus that is unknown to the DMZ (a Day zero attack) is the greatest threat to this network architecture. The network architecture provides good protection against external virus attacks where the antivirus software in the DMZ is updated. When connected to the Internet through the corporate network, the architecture also provides excellent protection against undesired remote access and denial of service attacks.

The network would be more vulnerable if connected directly to the Internet since GAMMA provides protection against denial service attacks and hostile intrusion (hacking). The firewall is a good way to almost eliminate possible intrusion from the Internet and GAMMA into the DELTA network. The firewall also provides virus protection.

The present internal security measures and policies including rules for no communication between different production area zones, hardening of clients and security policies for remote access, provides a fairly secure environment for local process automation and lab systems in the DELTA connected production areas and lab departments.

The DCS based production zone, the ZETA zone and the JOTA VLAN are the most secure zones.

## 6.9 Suggested improvements

This section present suggested improvements for increasing the IS security level in the DELTA context. Suggestions are mainly inspired by the ISA 99 Technical reports and possibilities for hacking derived in section 6.6. [4] [15]

## 6.10 Summary

According to the risk analysis there are threat scenarios with consequences and impacts that might be very costly for Sweden Operations. A Day zero scenario (Major virus outbreak in the production due to that the anti-virus in the DELTA network not is updated in time) might cost Sweden Operations as much as -  . The built in architecture and IS security measures address all identified threat scenarios, except for the Day zero scenario. The Day zero scenario potential is well known to the site Local IS security managers.

The most severe IS risk that endangers DELTA and the production of pharmaceuticals at the Södertälje site is:

- A virus that is unknown to the antivirus used in the demilitarized zone of DELTA, with origin from GAMMA and the Internet (A Day zero scenario) and with major outbreak in the DELTA connected production area networks.

- A major error executed by IBM that affects critical infrastructure equipment and systems within DELTA.

- Applying of a non-validated patching on critical infrastructure equipment or systems within DELTA that cause a major malfunction in the DELTA network.

- Major virus infection from a process automation systems vendor or support organization in a PLC based production area network.

- Major virus infection from an unauthorized direct-dial up access in a PLC based production area network.

- Unauthorized remote access through direct-dial up into a PLC based production area network.

- Major incident due to virus outbreak from a non-standard client in a PLC based production area network.

This section also summarize the most important and cost effective IS security improvements that could be realized in order to increase the IS security level in the DELTA context.

# 7 DELTA ISA 99 security program

## 7.1 Overview

This chapter presents a suggested IS security program for the DELTA network and the systems that are connected to the network. The IS security program is based on the suggested 18 key elements (section 2.5) of a cyber security management system presented in the ISA 99 Part 2 standard, 'Establishing an Industrial Automation and Control Systems Security Program'. According to the standard this represents the essential parts of a security program for all different conditions and organizations. The documents used in the chapter for evaluating the architecture and IS security compliance (chapter 5) together with the ISA 99 technical reports provides further input to the program. The AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services document provides compliance through mandatory IS security aspects for process automation systems. [14] [15] [16] [32]

*The security program uses a network segmentation of the DELTA architecture into two defined IS security zones. The intention with the network segmentation is to increase the visibility and the efficiency of the security policies and the risk management within the program. The defined zones are a DELTA network zone, including the DELTA network, ZETA and EPSILON, and a zone for production area and JOTA VLANs. The two zones have separate security policies (Section 7.6 and 7.7).*

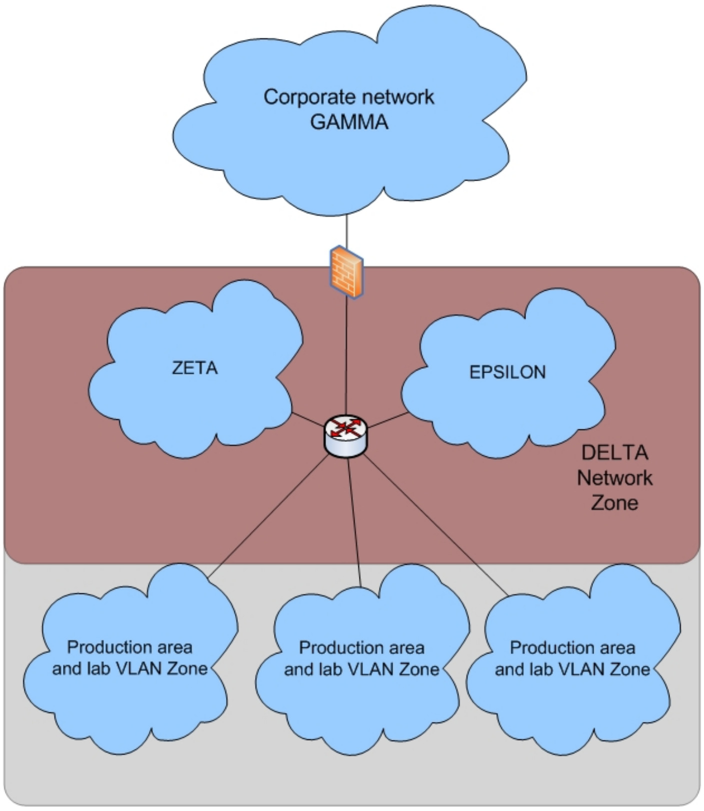


*Fig 7.1 DELTA zone and production area and lab VLAN zones*

***Text in italics presents important information and suggestions or mandatory aspects.***

***Paragraphs in bold text represent mandatory AstraZeneca Operations aspects that must be implemented or demand global or local IS security approval for exceptions. Both global and local exceptions are to be documented and reported for approval.*** [31]

***Text sections that begin with a star (*) represent sections that provide improvements that are implemented today and need to be confirmed or evaluated to assure that an effective level of IS security is implemented.***

***Text sections that begin with two stars (**) represent sections that provide improvements that will increase the IS security level and should be considered in a longer timetable.***

***Text sections that begin with three stars (***) represent sections that provide high priority improvements that is needed in order to increase the IS security level and can be realized in a near future to a cost that is assumed to be justified by the increased IS security level***.

## 7.2 Business case for a DELTA ISA 99 security program

*Objective: Make sure that Sweden Operations understands the importance of IS security in the context of process automation systems. Develop a business case for the IS security program that includes analysis of the loss of integrity, availability or confidentiality of process automation systems due to an IS security incident.*

A majority of the production areas at the Södertälje site are today connected to the DELTA network. Due to regulatory requirements, technical possibilities and business aspects, most of the process automation systems used in the manufacturing of pharmaceuticals cannot maintain a satisfying level of Information systems (IS) security, in order to be connected directly to the corporate network (GAMMA). There is also no great need for the use of Internet access and e-mail on process automation systems that would justify such direct connection to GAMMA.

The main idea with the DELTA network architecture is therefore to provide a secure IS security environment for process automation systems and at the same time provide a communication link between the operations and FREIA. Thus DELTA is a critical part in the ongoing work for increased integration and effectiveness within Sweden Operations.

The impact of the loss of availability and integrity of the process automation systems used at the Södertälje site could be very costly for Sweden Operations. Risk analysis performed on the networks and production systems connected to DELTA indicates that a major virus incident (A day zero scenario) might halt almost all production in Södertälje.

This worst-case scenario is estimated to cost Sweden Operations - for loss of production capacity. This might possibly also affect the delivery capacity for AstraZeneca globally and in the long run the company’s global reputation.

A severe virus infection of the THETA system would halt the tablet production within Sweden Operations. This worst-case scenario is estimated to cost Sweden Operations - for loss of production capacity.

A major virus infection in a production area network in a plant used for tablet manufacturing (BETA here used as an example) might possibly stop the production. This is estimated to cost – for loss of production capacity plus the cost for batches that have to be scrapped.

Inside the DELTA network there is also stored and communicated a lot of information that is considered to provide AstraZeneca with a competitive advantage. The loss of confidentiality of such information due to wiretapping of the DELTA network might reduce demand and profit for Sweden Operations.

For a more detailed picture of possible IS security incident scenarios, please refer to the risk analysis chapter (chapter six).

At present, various AstraZeneca standards, policies and SOPs defines the rules for how to protect process automation systems and connected networks from IS security threats. These documents are often very generic or intended for a special kind of system. The different production areas at the Södertälje site today also have different standards and rules for IS security on process automation systems. Therefore there is need for an overall strategy or program for the IS security activities in the manufacturing.

According to the ISA 99 standard, a common error when addressing IS security is to deal with one system at a time. According to the standard, IS security is a much larger challenge that must be addressed in a holistic manner on a company–wide basis. IS security can be viewed as more of a cultural and organizational issue that must be addressed in multiple ways. A satisfying level of IS security cannot be achieved through one project. IS security work is an evolutionary process that demands both long term planning and continuous efforts and measures. Therefore the ISA 99 standard suggests the implementation of an IS security program as the best way to reduce IS security risks to process automation systems and to sustain risk reduction over time.

An IS security program that is integrated in management, implementation and ongoing operations and maintenance of process automation systems will in the long run be more cost effective than selective measures to prevent IS security incidents. The intention with the program is also to reduce the bureaucracy in the IS security work and to simplify the communication and cooperation among departments like OIT, CTS, the operations, IT Services and IBM. Many of these departments today have different views on possible IS security threats and risks that threatens process automation systems.

Comparing costs for planning and implementation of an DELTA ISA 99 security program with the worst-case scenario costs described above, this gives an indication of that an IS security program is an efficient way to maintain and increase the IS security level within DELTA and the connected process automation systems.

The benefits of the DELTA ISA 99 security program will also increase as more and more local networks are being connected to DELTA. The costs for maintaining the DELTA ISA 99 security program will decrease, as it becomes an integral part in the operation of DELTA and process automation systems at the Södertälje site.

The ISA 99 standard represents a broad international industrial framework for IS security within automation and control systems. The DELTA ISA 99 security program is intended to comply with and supplement GAMP regulations and global AstraZeneca IS security standards for process automation systems. [2] [31] [32]

## 7.3 Scope of the DELTA ISA 99 security program

*Objective: Establish a framework to initiate and control the implementation and ongoing operations of IS security within the DELTA context. The scope is recommended to include all IS security aspects for process automation systems within the DELTA network and production and laboratory environments in the production areas.*

The reader of this document should be aware of that it is intended for the DELTA network and not intended for the GAMMA corporate campus network. Thus the suggested recommendations only apply for DELTA and connected internal networks and systems. This is referred to as the DELTA context in this document.

### 7.3.1 Responsibilities

A suggested scope of management responsibility for the IS security within DELTA and the connected production areas at the Södertälje site is:

*- Responsible for overall IS security in the DELTA context and for defining and maintaining the DELTA ISA 99 security program is the DELTA security group (DSG, section 7.4.1).*

*- Responsible for the implementation of all mandatory and suggested security measures presented in this document, in the DELTA network and the EPSILON segment are the DELTA governing group (Swedish: 'DELTA styrgrupp'). This also includes ensuring the availability and integrity of the ZETA segment.*

*- Responsible for the implementation of all mandatory and suggested security measures presented in this document, are the system owners for the different process automation and lab systems. This also includes the THETA system and the Eta systems.*

*- IT Services are operationally responsible for hardware and operating systems for standard clients. Operationally responsible for process automation and lab systems applications and all non-standard clients are the system owners of these applications and clients.*

*- Responsible for the training and education of operators and lab personnel and the operation of process automation and lab systems are managers of the concerned production areas and connected lab departments.*

*- Responsible for the implementation of IS security in process automation purchasing and implementation projects are suggested to be the AstraZeneca Engineering department. Where appropriate this responsibility is shared with CTS project managers and Lab systems project managers.*

This makes it possible to use the current responsibility hierarchy. IT Services are operationally responsible for networks, systems and hardware on central infrastructure services in EPSILON and the DELTA network. IT Services are responsible for hardware and operating systems for applications and services in ZETA and on standard clients. System owners of THETA and the Eta systems and application software on standard clients are responsible for these applications. Local system owners are responsible for all software and hardware on non-standard clients. [44]

***Please refer to Appendix E for full picture of implementation responsibilities of sections in italics.***

***Please refer to the DELTA- BaDS for a full picture of responsibilities concerning DELTA.*** [44]

## 7.4 Organizational security

*Objective: Establish an organization or network of people with responsibility for overall security within the DELTA network and context and for managing the DELTA ISA 99 security program, recognizing that there are operational and IS as well as organizational components that should be addressed.*

### 7.4.1 Establishment of a DELTA Security Group (DSG)

Establish a special DELTA security group (DSG) responsible for providing clear direction and oversight of the overall IS security in the DELTA network and context. A suggestion is that the group is formed of the site Local IS security managers (LISSM) (OITI) and the site Local IT infrastructure manager/DELTA manager (OITI) together with representatives from:

- DELTA governing group (DELTA styrgrupp)

- The OITP department (Production information systems, responsible for THETA)

- Process automation system operators and system owners (both PLC and DCS based production)

- Lab personnel and lab system owners

- The CTS department (process automation system managers)

- Lab system managers

- Process technicians and production support

- AZ Engineering (automation projects group) and project managers from CTS and Lab systems

- The IT Services department

- IBM Security

By involving personnel from outside OITI, the chance for understanding and integration of IS security in DELTA and the operations will increase. Cooperation will increase and communication and sharing of knowledge will be simplified between the different organizations

The DSG will be responsible for reviewing and maintaining the DELTA ISA 99 security program and to communicate it towards the representative's respective department. A suggestion is also that one of the site LISSM or the Local IT infrastructure manager/DELTA manager is appointed as chairman of DSG. This person should also, as a suggestion based on the importance of the work being performed by DSG, report to Sweden Operations OIT Director (SWEOPS IS IT Director).

DSG must in cooperation and with the support of Sweden Operations senior management ensure that the DELTA IS security program is implemented into the responsible organizations within the Södertälje site. The implementation should be made in consideration with the needs of the operational departments to minimize economic loss due to IS security measures interference with the operations. The goal is to implement an IS security level that in the long run is optimal in terms of both IS security and business perspectives.

A suggestion is that the DSG group meets on a monthly basis. The frequency of the meetings could also be adapted to the needs in terms of reviewing the program and responding to IS security incidents.

Use balanced scorecards to provide members of DSG with incitements to strive for increased cooperation and efforts in the work for reducing the likelihood for IS security incidents.

DSG must actively invite new member representatives from new networks and systems that are connected to the DELTA network. DSG should also suggest that systems and networks that would benefit from being connected to DELTA, becomes connected to the DELTA network.

## 7.5 Defence-in-depth strategy for the DELTA context

*Objective: Create a defence-in-depth strategy that adds several layers of IS security protection within the DELTA network and production and lab environments.*

According to the AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services and the DHS Control Systems Cyber Security: Defence in depth strategies, it is important to endorse a defence-in-depth strategy to provide a high level IS security level to the DELTA context. A defence-in-depth strategy can be summarized as adding several layers of protection or measures against IS security threats. A suggested defence-in-depth strategy for IS security in the DELTA context at the Södertälje site is: [11] [32]

- **** (1) Firewalls and wireless networks. There should be a firewall between the corporate network and the DELTA network. If a wireless access point is added to the DELTA network, there should be a firewall between the DELTA network and the access point. Firewalls should be properly patched and maintained.***

***Efficient firewalls will make it very difficult for an intruder on the Internet or a wireless network to access systems within the DELTA network. The wireless networks must also be configured and secured in a way that maintain the level of security and comply with AstraZeneca global IS security standards.*** [37]

- **** (2) Secure architecture and demilitarized zones. Maintain a high level of security in EPSILON. Use EPSILON as a DMZ between a wireless network access point and ZETA and production and JOTA VLANs (if possible). Take advantage of the security level in the DELTA architecture and actively suggest that added systems are constructed and operated in a way that increase the security level in the DELTA network. Safeguard that the implementation of new systems and networks on a minimum maintains the current level of IS security.***

- **** (3)*** *Intrusion detection and prevention systems.*

- Change control. Implement a centralized change control software system for all connected systems (where possible) in ZETA, production and lab.

- IP address control. Implement a network configuration that couple IP addresses with MAC addresses. This will decrease the likelihood of unauthorized connection of portable equipment to production networks.

- **** (4) E-mail and Internet access. No e-mail should be used on process automation systems or systems within the DELTA network. No Internet access should be possible in ZETA, EPSILON and on process automation and lab systems.***

- ***** (5)*** *Standard clients and systems. Cooperate with AstraZeneca Engineering and other appropriate AstraZeneca departments to decrease the number of systems that use non-standard clients. IS security is easier to maintain on standard clients. Since many process automation systems have a long lifetime, standard clients with standard operating systems increase the chance of being supported by operating and security systems vendors (Please refer to section 7.7.5 - 7.7.7 for more information). Ensure that the standard clients meet the requirements from production and lab.*

- ****** (6)*** *Hardening of process automation and lab systems as described in section 7.7.6.*

- ***** (7)*** *Security organization. Install a DSG group as described in section 7.4.*

- ***** (8)*** *Security policies. Implement clear security policies. This document provides a framework for a security policy for the DELTA network and a security policy for the production area and JOTA environments (Section 7.6 and 7.7). Communicate the policies towards the departments or personnel defined in section 7.3.*

- ***** (9)*** *Security training. Provide users in production and lab with a 'Production and lab computer user code of conduct' for IS security expectations and responsibilities (as suggested in section 7.7.2). Involve IS security training in courses for operation of process automation and lab systems. Evaluate how personnel from contractors and consultant firms and third part organizations maintain security.*

- **** (10)*** *Incident response capacity. Actively work with system and network owners to ensure that they have updated and tested BCPs and DRPs (Section 7.6 and 7.7).*

- ***(11) Remote access. Avoid remote access to networks and systems within the DELTA network. Assure the implementation of this. If remote access is used it must be carefully supervised of the site LISSM and comply with AstraZeneca global IS security standards. Only temporary and strictly controlled modem connections are to be used. Evaluate the suggestions in section 7.7.11.***

## 7.6 IS security policy for DELTA network, services and applications

*Objective: Identify how Sweden Operations defines and operates IS security within the DELTA network context.*

This section presents a suggested IS Security policy for the DELTA network, services and applications.

Most of the management of networks, systems, services and applications within the DELTA network and the ZETA and EPSILON zones, is performed by IT Services, IBM and Omikron (Consulting firm that provides the applications and services in THETA). This means that most suggested requirements under this section must be controlled through reviews and updates of the business agreements with IT Services, IBM and Omikron. Clear responsibilities for security incidents for external companies should be stated in order to increase the awareness of those companies so that they deliver their services with the agreed level of IS security.

Together with the AstraZeneca document Mandatory Standards and Good Practice for the Security of Process Automation Services, the security policy should be communicated towards the departments and personnel as defined in section 7.3 and appendix E. [31]

### 7.6.1 Physical and environmental IS security

*Objective: Create a secure environment for protecting critical DELTA network and server equipment from damage, loss, unauthorized access and misuse.*

The security perimeter at the Gärtuna and Snäckviken sub-sites and security perimeters to production area facilities, functions as the main security barrier against unauthorized access to networks, equipment and systems.

***(12)** There is need for extra control of physical access to and protection of server rooms with critical servers and network equipment for both AstraZeneca personnel and external personnel. There should be a clear policy that defines who authorized AstraZeneca and authorized external personnel are.*

These facilities must also be protected against environmental damage such as fire, water, smoke, dust, radiation and impact. Ensure that all external connections (power and communications) are adequately protected and maintained. This must be properly agreed with and communicated towards internal and external contractors.

***(13)** Ensure that external and AstraZeneca personnel are following the physical security procedures that have been established. Ensure that procedures are* *established for monitoring and alarming when physical or environmental security of the DELTA network, hardware, services and applications are compromised.*

**** (14)** Ensure that all new process automation systems equipment (including the THETA and Eta data systems) and central infrastructure devices are checked for computer virus and malicious code prior to being connected to a network within DELTA. Ensure that all software, which might be of potential value for a competitor or dubious organization outside AstraZeneca, is erased prior to removing and disposing process automation systems and servers used within DELTA. Ensure that all possible negative impacts on ongoing production due to disconnection of process automation system equipment, network equipment and other critical computer equipment are eliminated prior to removal.*

## 7.6.2 Personnel IS security

*Objective: Evaluate new and current external and AstraZeneca personnel to determine if they will maintain the defined IS security level within the DELTA context.*

***** (15)** Ensure that there is a security policy established for responsible personnel from IBM, ZETA system application providers and other appropriate organizations that install, operate, support or maintain networks and systems within DELTA. The policy should clearly state the expectations and responsibilities in terms of IS security. A suggestion is that this policy includes:*

*- Agreements with contractor to ensure appropriate communication of the policy towards personnel that performs consulting services within DELTA.*

*- Agreements with contractor to ensure reviewing of external personnel prior to sensitive work assignments within DELTA and the production area and JOTA VLANs.*

*- Insurance that no external personnel have total control over all networks and systems in the DELTA network, ZETA and EPSILON.*

*- Clear responsibility for IS security incidents for the responsible company if external personnel fails to fulfill business agreements and this leads to a security incident.*

*- A clear process for shutting off misbehaving or suspicious external personnel.*

*- A statement that insures that the policy apply on external personnel for a reasonable time after their employment and/or work for AstraZeneca ceases.*

All stated above must also apply for all AstraZeneca personnel that perform tasks similar to those of the external personnel.

## 7.6.3 Access control

*Objective: Address the administrative process of account administration, authentication and authorization of users in the corporate network to specific resources within the DELTA network.*

This section applies to both AstraZeneca personnel and external personnel.

**Account administration**
**** (16) There must be clear rules for authority and access to systems inside the DELTA network. All users must be individually identifiable with separate accounts. Access should be granted, changed or terminated by the user's respective manager.***

***Administrator authority should be granted from the DELTA manager. There should be a clear record on authorized user access accounts including, individual attributes, their permissions, extension of access authority and the authorizing manager. The record should regularly be updated and reviewed in order to remove accounts no longer needed and to ensure that the users only have the minimum required permissions.***

***No default passwords should be used. Ensure that a password protected screen saver is activated when leaving a system. Ensure that all passwords meet global AstraZeneca corporate standards.*** [36]

**Authentication**
***** (17) The standard AstraZeneca accounts are suggested to be used as authentication.***

*There should be a SOP for managers that is granting authority, to support the manager in the evaluation of that the person is considered to not pose an IS security threat. There should also be a SOP for the DELTA manager to be followed prior to granting administrator authority to support evaluation of that the person is considered to not pose an IS security threat.*

***All systems should provide an audit trail or a log that stores information about all access to systems on the DELTA network and failed log-on attempts.***

***There must be a function that disables the users account for a certain amount of time after some number of failed login attempts. There should also be a function that ensures that the user has to login again after some length of inactive time.***

**Authorization**
***** (18) All authenticated personnel should be provided with a security policy that clearly states the rules that the granted authority expects. User accounts should be role based to manage access to appropriate information and systems.***

### 7.6.4 Staff IS security training and awareness

*Objective: Provide personnel with necessary information to identify and address IS security vulnerabilities and to ensure their work practices are using effective risk mitigation solutions.*

There are already SOPs (that must be read and confirmed before access is granted) available for both AstraZeneca and external personnel that is approved access to THETA and other systems inside DELTA. To expand this initiative, in accordance with the ISA 99 standard, there should be a small test prior to granting access for evaluating that the person has acknowledged the SOP information. This test and the SOPs concerned should be reviewed in an appropriate time interval.

**** (19)*** *Personnel with connection to critical systems like THETA and EPSILON central infrastructure services should be educated in the threat of social engineering to reduce the likelihood and impact of insider induced IS security incidents and loss of confidential information.*

### *7.6.5* System development and maintenance

*Objective: Build IS security into the THETA system and where possible other applications in the EPSILON and ZETA zones.*

**** (20) All software on devices in EPSILON and ZETA must be maintained at release levels supported by the vendor of the software. This also includes the operating systems on standard clients. All systems should have a documented life cycle plan for software and hardware components.***

Where possible, demand that systems and applications within ZETA and EPSILON (mainly THETA) include features that ensures a proper built-in level of IS security. For THETA this could include a THETA system architecture that enables the use of an automatic recovery system, backup of all involved data and possibility for quick execution of BCP and DRP.

Ensure that all systems and applications that have impact on the production of pharmaceuticals have a clear established routine for patching and updating of operating systems and software applications, which insures minimal negative influence on the production. This is to reduce the likelihood of a scenario where an upgrade to systems causes the production to halt. The SOP 016054 defines when systems in ZETA and EPSILON must be patched. [50]

***** (21) IS Security requirements must be considered and addressed during all maintenance and support of production critical systems in EPSILON and ZETA*.**

**** *(22)*** *Work actively in cooperation with project managers that are responsible for implementation of new systems inside DELTA. Examples are possibilities for quick execution of BCP and DRP, high level of built-in system security and use of secure operating systems that are easy to maintain. Examples include the upcoming MES/EBR system implementation.*

### 7.6.6 Incident planning and response (DRP)

*Objective: Deter and detect IS security incidents and respond promptly if an incident occurs in the DELTA network and in EPSILON or ZETA applications.*

Due to the outsourcing contract with IBM, most of the content in this section must be agreed (and ensured that it is implemented) with IBM. For THETA, there is room for initiatives from OITP in cooperation with Omikron and IT Services to develop satisfying incident planning and response.

***** *(23)*** *Review the DRP for DELTA.*

*It is important that there exists a clear DRP for servers in ZETA and for THETA and the Eta systems. There should be some sort of regular testing and drills of the DRPs for DELTA, EPSILON and ZETA to ensure that if an incident is identified there is a proper response. Review that all of this is implemented in a satisfying way.*

**** (24)*** *Ensure and review periodically (suggestion on a yearly basis) with IT Services, IBM, Omikron and OITP that proper DRPs exists for DELTA networks and systems in EPSILON and ZETA. This includes responses to possible worst-case scenarios and review of the time that the responses are assumed to require.*

***** (25)*** *There should be an established routine for IBM for reporting of incidents and unusual events and experiences within the DELTA network and the applications used in the EPSILON and ZETA zones and production and JOTA VLANs. The incidents and experiences should be documented to record the incident, the response, the lessons learned and the course of action to prevent it from occurring again. Preferably this could be manifested as a SOP for the DSG group. This document should then be communicated to the appropriate departments and personnel as defined in section 7.3 and appendix E.*

### 7.6.7 Business continuity plan (BCP)

*Objective: Identify procedures for sustaining essential business operations while recovering from a significant disruption in DELTA or THETA.*

****** (26)*** *Review the BCP for DELTA.*

*OITP should in cooperation with IT Services, Omikron and IBM develop a satisfying BCP for THETA. Make sure that all of this is implemented in a satisfying way. This includes how to restore locally (SCADA and DCS systems) saved data to the system (if the THETA system becomes unavailable and the SCADA and DCS systems have to store data locally) and loss of infrastructure services. The plans should be tested and updated regularly.*

According to the ISA 99 standard, the first step in the procedure for developing a BCP is to specify the recovery objectives for the involved systems based on the business needs. Based on these objectives, there should be development of a BCP that ensures that the production can be restored in a timely fashion. A major source for contribution to this area is the impact analysis of IS security incidents to specific systems and networks performed in the IRM process (section 7.9).

***** (27)*** *A formal business continuity team should be formed including IT Services, IBM, Omikron and system managers of the THETA and Eta systems. This team should in the event of a significant disruption determine the priority of critical systems to reestablish normal operations. The BCP should also define and communicate the specific roles and responsibilities for each part of the plan.*

The ISA 99 standard also states that the organization must make and protect system backups to support the BCP. Today there is a backup for all involved systems in EPSILON and ZETA. A suggestion is therefore to evaluate the existence and functionally of automatic recovery system for THETA and Eta systems and to ensure that the procedure for restoring all systems from automatic recovery is established in detail in the BCPs for DELTA, THETA and Eta systems.

A suggestion is to review and update the agreements with IBM concerning the implementation and preparedness of the BCP for DELTA (based on input from an IRM process and impact analysis of different IS security incidents). It is also suggested to review and update the BCP for THETA in cooperation with OITP, Omikron, IT Services and IBM. Finally there should be some sort of regular testing and drills of the BCPs for DELTA and ZETA applications.

### 7.6.8 Information and document management

*Objective: Safeguard information and make appropriately available the information associated with operating the DELTA network and the ZETA and EPSILON zones.*

OITP should in cooperation with IT Services, IBM and Omikron ensure that THETA complies with the objectives of this section. This mainly includes ensuring long-term storing of data and possible retrieving of long-term stored data. This must also be implemented on a satisfying level for the Eta systems.

**** (28)** Disposal of servers from EPSILON and ZETA requires removal of data that might be of value to a competitor to AstraZeneca.*

There should also be a policy defining which documents that are considered to be confidential for the operation of the DELTA network. Thus all information about the DELTA network should be classified as either ‘confidential’ or ‘internal’ information. This is to reduce the information for a possible external or internal attacker.

**** (29) Most information that is communicated in the DELTA network is considered confidential to organizations outside Sweden Operations. Therefore it must be assured that no part of the network admits possibilities for wiretapping. This includes all wireless networks.*** [63] [71] [72]

## 7.7 IS security policy for Production area and Lab environments

*Objective: Identify how Sweden Operations defines and operates IS security within the process automation and lab systems environment.*

This section presents a suggested IS security policy for the production area and lab environments. Together with the Mandatory Standards and Good Practice for the Security of Process Automation Services document, the security policy should be communicated towards the departments and personnel as defined in section 7.3 and appendix E. [31]

### 7.7.1 Physical and environmental IS security

*Objective: Create a secure environment for protecting critical process automation and lab system from damage, loss, unauthorized access and misuse.*

For all production areas there should be a security policy and procedure for physical protection of process automation. Current security perimeters at the Snäckviken and

Gärtuna sub-sites comply with the requirements in the ISA 99 standard. The process automation and lab systems must also be protected against environmental threats such as fire, water, smoke, dust, radiation and impact.

### 7.7.2 Personnel IS security

*Objective: Evaluate new and current external and AstraZeneca personnel to determine if they will maintain the defined IS security level within the process automation and lab environments.*

***** (30)** *There should be a clear policy for all personnel that operate process automation and lab systems. The policy should state the IS security responsibilities of personnel.*

*A suggestion is therefore that there should be a document or a 'Production and lab computer users code of conduct' or equivalent for IS security expectations and responsibilities of the personnel defined above. This document should be regularly communicated and include IS security expectations, responsibilities and disciplinary actions that might be the result for personnel that violate the regulations. The document should also state the reason why the rules are necessary with focus on the GMP regulations and not with focus on the potential business effects IS security incidents might cause (please refer to chapter 6 for a more detailed view about IS security incident impacts). The document is intended to complement the standard AstraZeneca global 'Computer Users Code of Conduct'.* [30]

*Thus the document could include rules and information about:*

*- A GMP background to the rules.*

*- That the process automation or lab system only is to be used for the purpose intended.*

*- No connection of computer equipment or media is allowed, including USB and CD-ROM.*

*- Installation of programs on clients is not permitted.*

*- E-mail or Internet use is never permitted.*

*- The user must also follow the corporate Computer Users Code of Conduct when operating process automation and lab systems.*

*- What the user is expected to do if other personnel violates the document.*

*- The disciplinary consequences that might be the result of violation of the rules. This could range from warnings to dismissals*

*The disciplinary consequences must match with AstraZeneca employee terms and conditions. The responsibilities should also extend for a reasonable time after employment ceases.*

***** (31)** *It must also be agreed with third part and contract employees (consultants and contractors (Swedish: 'bemanningspersonal' ) to follow the document prior to* *performing process automation systems related work in production and lab environments.*

### 7.7.3 Access control

*Objective: Address the administrative process of account administration, authentication and authorization of users on process automation and lab systems.*

**** (32) Ensure that passwords and accounts comply with AstraZeneca corporate standards. Use standard AstraZeneca accounts for login on process automation and lab systems to provide central account administration. Access should be granted, changed or terminated by the authority of the manager for the production area, lab or appropriate. A SOP could be created for this task, to support the manager in the evaluation of the employee. All access accounts should be recorded with information about the individual, their permissions and the authorizing manager. Access accounts shall be removed as soon as they are no longer needed. Users shall have minimum required permissions.*** [36]

*No group accounts or default passwords should be used. Ensure that a password protected screen saver is activated when leaving the system.*

***All access should be logged. Access accounts should be disabled for a certain amount of time after some number of failed login attempts. Access accounts should be role based to ensure that a required minimum of resources is granted****.*

### 7.7.4 Staff training and IS security awareness

*Objective: Provide personnel with necessary information to identify and address IS security vulnerabilities and to ensure their work practices are using effective risk mitigation solutions.*

***** (33)*** *Newly employed operators are educated in the operation of process automation systems. This education should also include IS security training, implementation of section 7.7.2 and information about the social engineering threat. This should regularly be tested and updated.*

****** (34)*** *CTS and other technical automation support organizations must be carefully informed that modem connection of and to process automation systems never is permitted without a clear permission from LISSM.*

### 7.7.5 System development, maintenance and disposal

*Objective: Build IS security into the process automation and lab systems.*

***** (35)*** *Perform work for developing a standard client that meet the demands and requirements in terms of both IS security and production usability. Update the client continuously.*

***** (36)** Cooperate with AstraZeneca Engineering and other relevant AstraZeneca departments to decrease the number of systems that use non-standard clients. IS security is easier to maintain on standard clients. Since many process automation systems have a long lifetime, standard clients with standard operating systems increase the chance of being supported by operating, control and security systems vendors. There is a clear business case for the use of standard clients.*

**(*37) All software on process automation and lab systems must be maintained at release levels supported by the vendor as defined in the Mandatory Standards and Good Practice for the Security of Process Automation Services document. All systems should have a documented life cycle plan for software and hardware components.*** [31]

****** (38) All remote access to process automation and lab systems must meet Global corporate IS security standards and be reported to LISSM, OIT. No modems or modem connections is to be used by process automation and lab systems during installation, operations or maintenance, without a clear and documented permission from LISSM.*** [31]

**** (39) There must be proper procedures established and audited with respect to the addition, removal and disposal of process automation and lab systems. All data that might be considered as confidential or of value to a competitor to AstraZeneca must be erased prior to disposal of all process automation systems. Establish a SOP for the process for adding and connecting of process for process automation and lab systems. Include virus scanning in the SOP. Investigate the suggestions for use of EPSILON central services as described in section 7.7.11.***

### 7.7.6 System hardening and anti-virus protection

*Objective: Provide process automation and lab systems with proper protection to combat misuse and virus infections.*

****** (40) All (including also process automation systems without any network connection) clients should be provided with locked cabinet or alternatively equivalent software to prevent physical intrusion and connection of memory devices. This includes disabling USB, floppy drives and CD-ROM ports and equivalent ports and vulnerabilities. Safeguard keys to cabinet lock.***

***Provide all clients (including unconnected process automation systems) with software that disables all vulnerabilities in the operating system. This includes disabling command prompt and Microsoft Windows Explorer and equivalent vulnerabilities. A suggestion is that administrator access enables this.***

***Always undertake further hardening of process automation systems where defined by the automation vendor.***

***It is desired to provide all process automation and lab systems with standard clients. Include the software and hardening as described in section 7.7.6 on standard clients. Make sure that the standard clients meet the requirements that the production and lab departments demand.***

A suggestion is that the site LISSM should approve all use of non-standard clients.

****** (41) All process automation and lab systems should be equipped with antivirus software. Updates should preferably be made with the help of the DELTA antivirus service. Updates should be made regularly.***

***** (42) Operating system should be updated or patched when administratively and technically possible, without interfering with the production or laboratory tests performed. Minimum requirement is that updates shall be made once a year.***

***** (43) Ensure that all servers and control systems equipment (like scanning node and local servers and PLC and DCS hardware or equivalent) are properly hardened according to the AstraZeneca document Mandatory Standards and Good Practice for the Security of Process Automation Services. This includes use of anti-virus software, physical protection (locked cabinets) against unauthorized connection and abuse and proper patching of operating systems. This section also applies where appropriate to lab equipment and systems. Safeguard the keys to cabinet locks.*** [31]

Implement change control software as described in section 7.5.

Where patching of operating systems and the use of antivirus software not is possible on process automation systems, evaluation and assessment of the use of other equivalent security measures should be performed. A suggested alternative solution is the combination of:

- Physical protection of clients and other computerized equipment belonging to the process automation system. The protection must prevent connection of any computer or memory device to the system.

- Let the whole process automation system connect to the production area network through a system-included firewall. Firewall should be dedicated (not host-based) and only allow communication to predefined addresses and on a minimal number of predefined protocols. The firewall might include packet filtering, stateful inspection and application proxy filtering, depending on security and manageability issues. Some firewalls also have inbuilt antivirus. [15]

- No email or Internet access on the process automation system.

- No modem or remote access to the process automation system.

Include this as a new ‘process automation system firewall’ service in the services offered by DELTA (see section 4.5).

For production areas that use DCS process automation systems that cannot be patched or use of antivirus, there should be analysis for which firewall solution is the most suitable depending on the DCS network connectivity to the production area network.

This suggestion does not apply for servers in production.

### 7.7.7 System monitoring

*Objective: Ensure traceability of all systems with impact on the production and identify threat agents.*

***(44) Install and operate monitoring software on all systems that have impact on the production. Ensure that logs are recorded from logon attempts, external attempts to access or modify data, use of user accounts on the system and all changes to the system and platform parameters (As defined in the Mandatory Standards and Good Practice for the Security of Process Automation Services document).*** [31]

***All systems should generate an audit trail. Investigate if there is possibility for a central service in EPSILON to support this task*.**

### 7.7.8 Incident planning and response (DRP)

*Objective: Deter and detect IS security incidents and respond promptly if an incident occurs in a process automation or lab VLAN*

**** *(45)*** *There shall be a DRP for every production area unit or lab department. The DRP should state responsible personnel and define the actions to be performed to restore systems. The plan should be tested, drilled and updated regularly. Plans should also include responses to loss of infrastructure services or contact with critical systems like THETA.*

*All incidents should be documented and reported to the DSG. Which personnel that are responsible for this should also be stated in the DRP.*

Responsible for development of the DRP document should be the affected system owners in cooperation with management in the production area unit or lab department.

A suggestion is that the DRP should have supplementary CD-ROM or USB memory devices that contains software for restoring different systems in the scenario of an IS security incident. This would decrease the recovery time.

A suggestion is also that the DSG is responsible for approving DRPs.

Ensure that DRP also contains plans for local servers in production.

### 7.7.9 Business continuity plan (BCP)

*Objective: Identify procedures for sustaining essential business operations while recovering from a significant disruption in process automation and lab systems.*

**** *(46)*** *Develop a BCP for every production area unit and lab department. The BCP shall state recovery objectives based on business needs and define the specific roles and responsibilities for each part of the plan. The plans need to be tested and updated regularly. Plans should also include responses to loss of infrastructure services or contact with critical systems like THETA.*

DSG shall determine the impact and consequences that is associated with loss of systems to provide input for recovery priorities in the scenario of a major incident.

***** (47)** Form a special Sweden Operations DRP and BCP team of responsible system managers, IT Services, IBM, CTS personnel, OITP personnel and managers for Sweden Operations production area units and lab departments. The group is responsible for restoring systems and operations with the help of local DRP and BCP. This might be more effective in terms of both costs and recovery time. In the scenario of a major incident in several process automation and lab VLANs the group should determine the priority order for restoring critical systems.*

Ensure that BCPs also contains plans for local servers in production.

### 7.7.10 Information and document management

*Objective: Safeguard and make appropriately available the information associated with operating the process automation and lab systems.*

**** (48)** Provide a policy for CTS and system owners of process automation systems that demand that all information on systems must be erased prior to disposal of equipment and systems.*

### 7.7.11 Connection of portable computer equipment

*Objective: Combat unauthorized connection of portable computer equipment in production and lab environments and prevent possible virus injection.*

***(49) Avoid connection of portable computers to process automation and lab VLAN. If portable computer equipment has to be used and connected, it must be cleaned from malicious codes prior to connection according to applicable SOP that is in place.*** [52] [46]

Investigate the possibility to develop a special central service in EPSILON for easy cleaning of virus on portable computer equipment or portable media devices.

This service could consist of a physically isolated server that is updated with the latest antivirus software. By connecting to the server, the connected computer or media device is scanned and cleaned.

Alternatively an individual SILVER standard VLAN could be created for this task. This VLAN should have a network connection in all DELTA connected buildings. The VLAN should be able to communicate with BRONZE networks but with EPSILON as DMZ. Alternatively a wireless router could be connected to the new VLAN and increase the mobility for the owner of the portable computer equipment in the production areas. This VLAN could also be used if a wireless access point is added to DELTA. This VLAN is then used for connection of the portable computer equipment.

### 7.7.12 Reduction of third party risks

*Objective: Reduce IS security risks from third part organization to an acceptable level.*

**Manage risks from vendors**
***** (50)*** *Ensure that AstraZeneca Engineering actively take notice to the Mandatory Standards and Good Practice for the Security of Process Automation Services document (mainly section 8.3.2) when choosing vendors and purchasing new process automation and lab systems. To ensure this establish a SOP for AstraZeneca Engineering personnel which states that all purchase projects must consider this and preferably state that process automation systems must be able to use standard clients. The SOP shall (as a suggestion) include mandatory reporting to DSG of all cases that deviates from this to increase the incentive for AstraZeneca Engineering to contribute to the IS security work.* [31]

*There should also be one specialized SOPs for project managers from all different production areas (CTS) and LAB.*

**Manage risks from support organizations**
***** (51) Develop a SOP according to section 8.3.3 in the Mandatory Standards and Good Practice for the Security of Process Automation Services document, which is to be followed by all support organizations of process automation and lab systems. Include anti-virus scanning in the SOP.*** [31]

## 7.8 Infrastructure operations and change management

*Objective: Address the procedure requirements for changes and updates of systems to IS security.*

This area is addressed in the SOP 016054 and the AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services and the AstraZeneca guideline Secure Network Isolation of Process Automation Computer Systems. There also exist policies for validation of systems due to all sorts of changes of process automation systems, [31] [32] [50] [54]

### 7.8.1 Update and patch management strategy

Deployment of operating systems software patches is regulated in the SOP 016054. This means that the patch deployment for the DELTA network and the EPSILON and ZETA applications already has a working and mandatory procedure. [50]

For process automation systems in production area networks (BRONZE) there is room for deployment of patches on a local decision based non-regular time interval. Based on this it is suggested that there should be a well documented procedure that includes:

- Maximal time length that is allowed to pass without applying security patches to systems in BRONZE class networks.

- Forming of a special process automation systems patching group. This group should work continuously throughout the year with patching of process automation systems (where there is greatest need for patching, based on IRM work and upcoming threats). This work should be conducted in cooperation with appropriate CTS departments and system owners. The intention with this suggestion is to provide a way for patch deployment that provide security patches and at the same time minimal interference with the production. For example all systems could be patched during the summer brake and the group responsible for all other security patching throughout the rest of the year. The group could be formed of IBM, IT Services and CTS personnel and directed by the DSG.

### 7.8.2 Backup management

A procedure for backing up and restoring computer systems within DELTA should be established, used and verified by appropriate testing. This should apply as mandatory (where possible) for all involved systems and system owners. This connects to section 7.7.8 and 7.7.9.

## 7.9 Integrated risk management (IRM)

*Objective: Recognize where IS security vulnerabilities and risks exist in the DELTA context and implement security measures that commensurate with the identified risks.*

### 7.9.1 IRM

To recognize where IS security vulnerabilities exist and the potential impact and consequences that could occur as a result of an IS security incident, it is important to identify, assess and manage all IS security risks. The ISA 99 standard suggests that risk management is based on two parts. All risks must first be identified, classified and assessed. The identified risks should then be managed through risk mitigation implementations. AstraZeneca have developed a framework for risk management called the Integrated risk management (IRM). Therefore the suggestion is that the DELTA ISA 99 security program takes advantage of the IRM tool for risk management.

** ***(52)*** *In order to follow AstraZeneca standard procedures for IRM the DSG should perform a yearly IRM process. The result of the IRM process will then form the basis for further reviewing of the IS security program and for implementing improvements. The risk criterions presented in appendix A should be used in the IRM process. Please refer to relevant IRM documentation for more information about the IRM tool.* [35] [56]

Use IBM or other external part to provide expert knowledge about new threats and vulnerabilities during yearly IRM work.

## 7.10 Maintaining and implementing improvements for IS security

*Objective: Implement, measure, track and improve security efforts continually to keep process automation systems and the production of pharmaceuticals more secure.*

### 7.10.1 Identify new threats and opportunities

The procedure to identify new threats is integrated in the IRM process. In order to identify possible improvements for IS security; the process should also include work on identifying opportunities. Since the IRM process is performed once a year, DSG could discuss and respond to new threats on a monthly basis. If necessary, emergency cases should be taken care of immediately.

### 7.10.2 Identify and implement corrective and preventive actions

Based on the identified threats and opportunities in section 7.9.1 and 7.10.1, the DSG group must on an appropriate time interval or on yearly basis identify corrective and preventive actions. By integrating changes continually, there is less need for significant amounts of time to be spent on updating the entire DELTA IS security.

When actions are approved, action plans and areas of improvement need to be communicated towards key stakeholders and the affected personnel.

### 7.10.3 Evaluate personnel feedback on IS security measures

When implementing IS security measures it is important to seek personnel feedback on performance shortcomings and production interference due to the IS security measures. The idea with the DSG group composition is to increase the efficiency of communication of action plans to stakeholders and gathering of stakeholder and personnel feedback. The feedback could be collected when appropriate or on a yearly basis. The feedback could also be selectively addressed or based on free responses for suggestions of improvements. For example could a structured questionnaire be used for collecting feedback in important areas.

## 7.11 Monitoring and reviewing of the DELTA ISA 99 security program

*Objective: Monitor and review the DELTA ISA 99 security program continually.*

### 7.11.1 Review the business case for the DELTA ISA 99 security program

As a part of the yearly based Sweden Operations budget planning work, the DSG chairman shall update the business case for the IS security program. The business case and a summary of the work conducted during the year within the DSG should be presented for the management responsible for DSG. This will provide a basis for management review of the work and the efficiency and effectiveness of the security program.

### 7.11.2 Continuously review the IS security activities within the DELTA network and the operations

***** (53)*** *To assure that the IS security activities in the network are performing as expected, the DSG need a process for collecting information about the performance of manual and automatic (computerized) IS security activities. The manual part of the process could be based on audits in production and lab areas, server rooms and review of system maintenance and operations. Audit of the automatic IS security activities must be performed in cooperation with IBM and IT Services. This creates a dilemma since then IBM would both provide and review the IS security level. A suggestion is to solve this issue with the help of IT Services.*

The audits could be performed as monthly random inspections in critical areas and on a yearly random basis for less critical areas. The suggestion is that areas identified as the most severe in the risk analysis in section 7.9 above are inspected more frequently.

### 7.11.3 Report IS security incidents in a timely manner

***** (54)*** *IBM and the IT Services department should have procedures in place to identify failed and successful IS security breaches. The DSG should establish a connection to IBM and IT Services for collection of the information that is produced as a result of this procedure (in a timely manner). There should also be an initiative for educating operators and relevant personnel on reporting IS security incidents to the DSG in a timely manner.*

Information provides data for incident response and reviewing the risk level. IBM and the IT Services department should execute this process. The information also provides data for IRM work and for business case background.

The system owner and information owners of the systems that is affected by the incidents should also be informed.

### 7.11.4 Review the risk level with changes to the environment and address issues discovered

When there are changes in the IS security environment or within the DELTA context, that demands urgent risk level assessment, the members of DSG shall consult with the local LISSM to evaluate if there is need for immediate actions.

**** (55) IBM and IT Services should have a procedure for closing the firewall between GAMMA and the DELTA network when there is risk for virus infection or a possible Day zero scenario.***

## 7.12 DELTA ISA 99 security program compliance

*Objective: Assess the IS security program policies and procedures to affirm that they meet legal, regulatory and company security requirements.*

The DELTA ISA 99 security program complies with the ISA 99 Part 2 standard.

The program is intended to comply with and complement the SOP 016054 and the AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services documents. When changes are made to the program there must be a compliance audit to ensure compliance to these documents. The suggested firewall configuration deviates from Mandatory Standards and Good Practice for the Security of Process Automation Services. [31]

The program complies with AstraZeneca IRM requirements. [56]

The program complies with the GAMP 4 Guide, appendix O3: Guideline for Automated System Security. This includes system classification, Employee awareness, and Incident management and Information security policy. [2]

## 7.13 Summary

This chapter presents a suggested IS security program for DELTA context. The intention with the program is to address IS security within the DELTA network and in the production and lab environments in an overall solution manner with respect to both IS security and business requirements.

***Sections with priority (***) are 7.5, 7.6.6, 7.6.7, 7.6.2, 7.7.4, 7.7.5, 7.7.6***

***Responsibilities for implementation of all italic sections are presented in Appendix E.***

# 8 MES/EBR system implementation and IS security

## 8.1 Overview

This chapter briefly discusses the implementation of a MES/EBR system and the IS security risks that this implementation potentially creates. The chapter also provides some IS security conclusions that is of interest for the MES/EBR system implementation.

In order to follow the scope of the study the focus in this chapter is on how the EBR system implementation affects the IS security within the DELTA context and the production at the Södertälje site.

## 8.2 Implementation of a MES/EBR system

Sweden Operations is looking at the possibility to implement a computerized Manufacturing execution system (MES). A MES is a system that companies can use to measure and control critical production activities. Activities include prodcution recource management, prodeuction definition management, production tracking, production performance analysis, production dispatching, prodcution data collection and production execution management. Some of the benefits with regards to MES solutions are increased traceability, productivity, and quality. The MES system connects the systems used in the production (level 0-2 in the ISA hierarchy) with Enterprise resource and planning systems (ERP systems) (level 4). Today there are many different ERP system used by Sweden Operations. All ERP systems are today operated from GAMMA. [23] [73] [80]

Current plans for a computerized MES system within Sweden Opertions consists of an Electronic batch record (EBR) system and a system for manufacturing operations that also connects the EBR system to the ERP systems. Current MIS systems (mainly THETA) and systems in production areas and JOTA VLANs will provide production data to the MES system. [75]

### 8.2.1 Electronic batch records (EBR)

A crucial part of the MES system is the EBR system. The EBR system provides most of the MES functions except for production scheduling and performance analysis. Benefits of the EBR system is paperless production and includes electronic batch recipes, protocols and reports, equipment management, process documentation, electronic work instructions (program recipes), lab analysis results and most of all the electronic batch record. The batch record contains all data about the manufactured batch (including audit trails, critical sensor and equipment values, and electronic signatures with timestamps) and founds the basis for the validation process before the batch is approved to be shipped to the ISMO department. The system enforces that all values corresponds to the master batch recipe. This makes the validation of manufactured batches almost automatic since only the production and quality control deviations from the master batch protocol have to be approved by validation personal. Hence the EBR system has a great potential to reduce costs for administration, validation and documentation within the production of pharmaceuticals. [28]

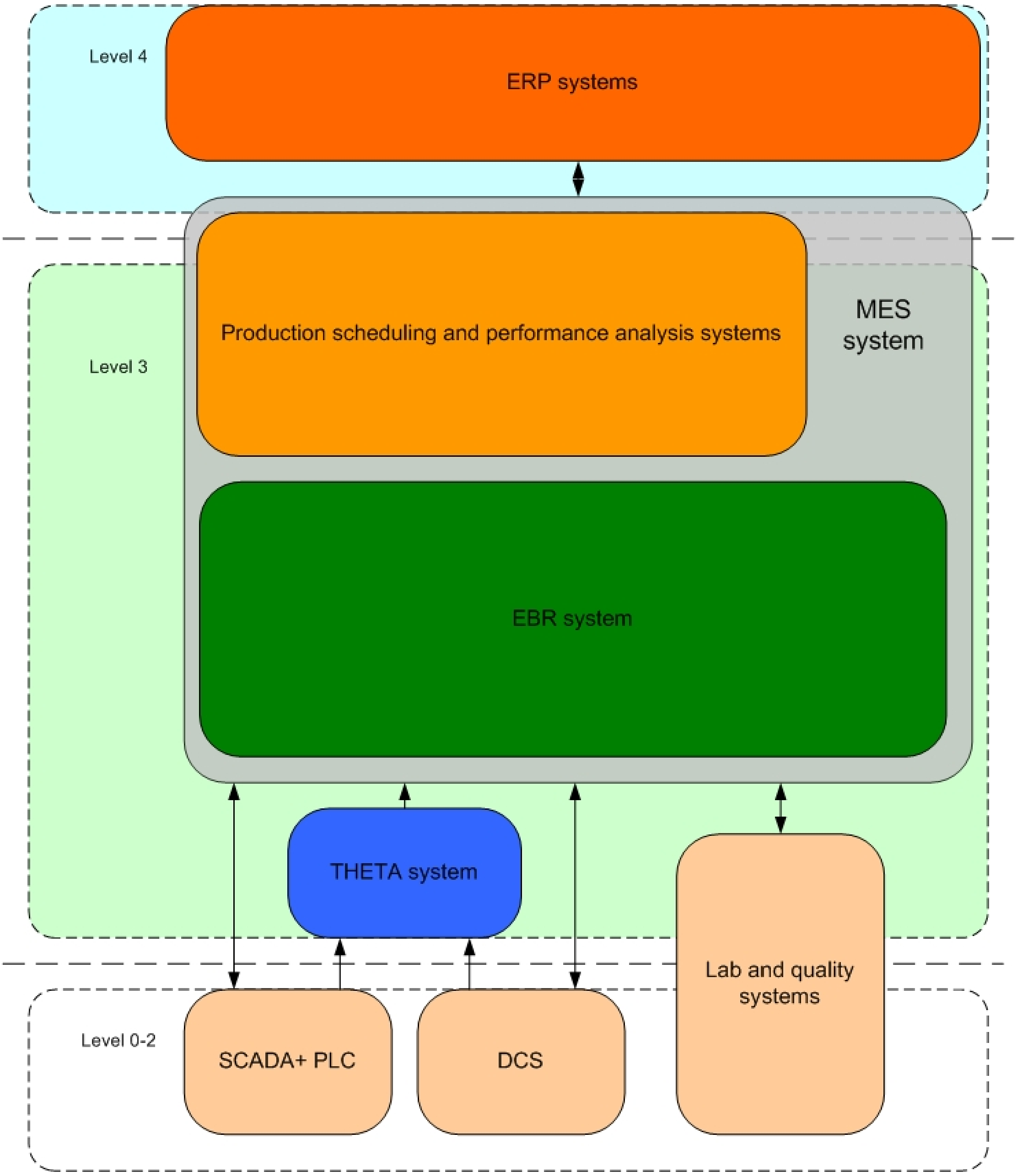


*Fig 8.1 Structure of MES system*

### 8.2.2 MES and EBR system functionality

The production scheduling and performance analysis part of the system will mainly keep track of what is produced and report Key performance indicators (KPI) from the production. Connecting to IS security, the loss of such a system due to an IS security incident will not cause the production to stop immediately. If the system becomes unavailable for a long time, the scheduling of batches and material in production will have to be made manually.

The EBR part of the system in principal consist of databases and software that connects the databases with the production scheduling and performance analysis system, production systems and operator HMI, SCADA and DCS, lab systems and the THETA system. The databases store batch record contents and keep track of the equipment recipes and batch record templates. [28]

Thus the availability of the EBR system becomes very important for the production since no production can be performed without that the production equipment is connected to the EBR system. The data transmitted to and from the EBR system is also of potential value to a competitor to AstraZeneca since it contains a lot of information about the production processes.

Furthermore there is also likely to be increased demands for the use of wireless networks to be able to connect all production equipment and personnel to the EBR/MES system.

Finally to comply with the GMP regulations and provide traceability, the batch reports and electronic batch and lab protocols or batch files have to be electronically long term stored. The technical solution for this task is not yet decided.

### 8.2.3 Suggested network solutions for the implementation of an MES system

It is today not yet decided where the MES system will be placed in the network architecture within Sweden Operations. Probable locations for the system are in the GAMMA network or inside the DELTA network (in the ZETA zone). [73 [75]

Irrespective of if the system is operated from GAMMA or the ZETA segment, there is need for a communication bus server that translates information between, ERP, MES, MIS and process automation and lab systems. Such bus-server will most likely be operated from the EPSILON segment. This means that communication through the communication bus and communications between GAMMA and DELTA can utilize EPSILON as a DMZ. [73]

The increased need for wireless connectivity and access to the MES/EBR system also requires the use of wireless access points. In GAMMA there are already wireless networks and access points available. Today there are no access points available in DELTA. If such access points are needed it will most likely be added as a separate AstraZeneca ‘BRONZE’ standard network. [32] [73]

This creates three possible architectures for the DELTA context with the implementation of a MES system:

- Placing the MES system in ZETA inside DELTA and adding a wireless network access point within DELTA (I). Figure 8.2.

- Placing the MES system in ZETA inside DELTA and use GAMMA wireless networks (II). Figure 8.3.

- Placing the MES system in GAMMA and use GAMMA wireless networks (III). Figure 8.4.

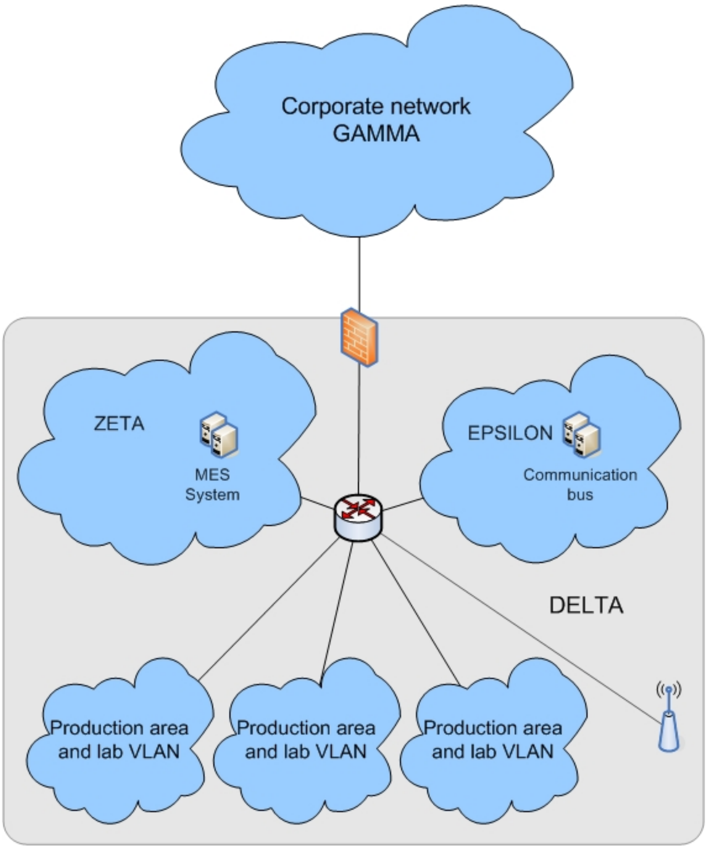


*Fig 8.2 MES system in ZETA segment and access point inside DELTA (I)*

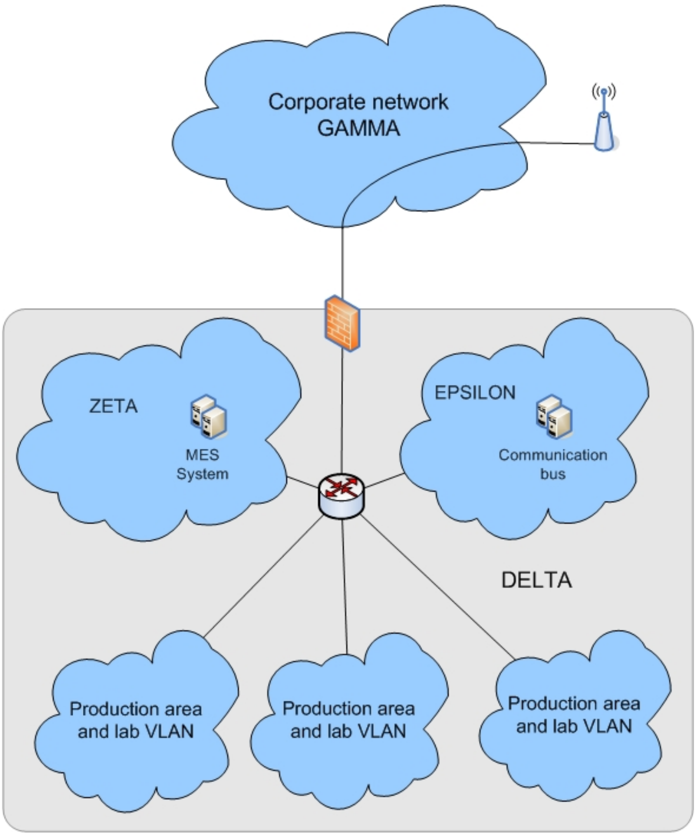


*Fig 8.3 MES system in ZETA segment and use of wireless networks from GAMMA (II)*

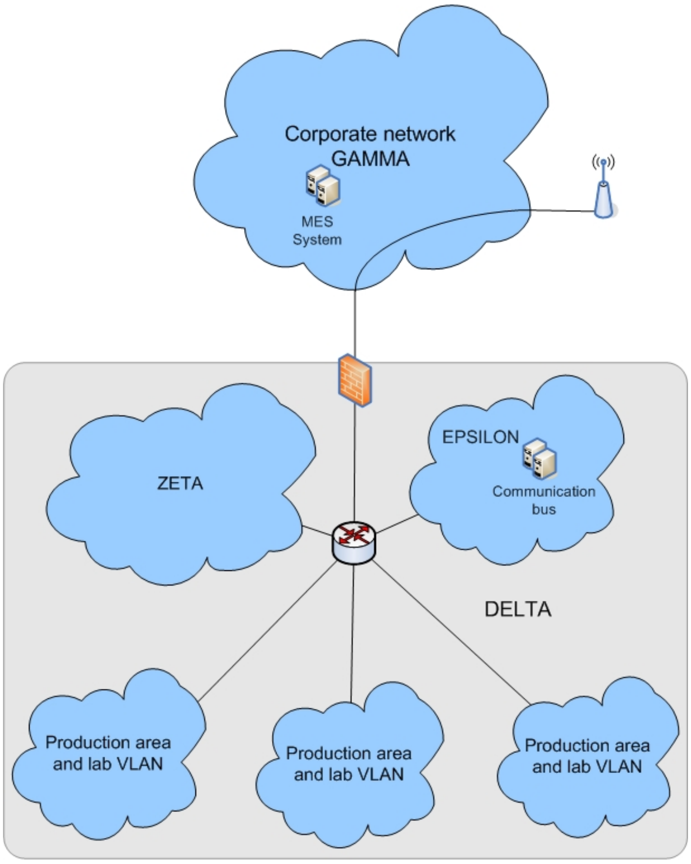


*Fig 8.4 MES system in GAMMA (III)*

## 8.3 MES/EBR system introduced IS security threats

The following IS security risks that especially relate to an MES/EBR system have been derived in cooperation with people involved in the MES/EBR project. In order to follow the scope of the study, the focus is on the EBR part of the system. [60] [75]

### 8.3.1 Possible threats and threat agents

Possible threats for IS security attacks on the MES/EBR system are the passive and active threats described in the theory chapter. For the EBR system this is mainly wiretapping, malicious code, intentional or unintentional human errors and possible hostile intrusion from the Internet, through a modem connection or through a wireless network connection. The possible threat agents are also presented in the theory chapter.

### 8.3.2 Wireless network vulnerabilities

With increased wireless connectivity and wireless connection access points there is a risk for war-driving attacks (hacker intrusion through a wireless access point) on the network that hosts the access point. Therefore it is very important that the wireless network must be properly encrypted and protected according to global AstraZeneca IS security standards. [4] [31] [37]

### 8.3.3 MES/EBR system availability

The production of pharmaceuticals becomes dependent on that the EBR part of the system is working. Thus the production is also dependent on that DELTA and the segment where the EBR system is operated from, is operational. Depending on where the system is placed in the reference architecture, the integrity of this segment becomes very important for Sweden Operations. There must also be an extraordinary capacity to quickly restore the system in the scenario of an IS security incident.

### 8.3.4 Availability of EBR critical systems

The EBR system will be dependent on EBR critical systems (like the THETA system) for data from the production. This makes the system vulnerable against malfunctions and IS security incidents in DELTA network, ZETA and the production areas. The THETA system has an estimated worst-case scenario recovery time of up to two weeks. This implies that if the THETA system suffers a major IS security incident, then the THETA connected production at the Södertälje site is forced to halt for up to two weeks. Therefore there is need for a very quick and effective recovery of the THETA system if the MES and EBR system is implemented.

### 8.3.5 Wiretapping of information

With the EBR implementation the amount of confidential information that is transmitted within DELTA increases. Without EBR, mainly recipes (electronic work instructions) and sensor and actuator values are transmitted, but with EBR more information will be transmitted within the DELTA network. Thus the impact of possible wiretapping of DELTA becomes a more serious problem with the implementation of a MES and EBR system (compare with section 6.3 and table 6.2). Encrypting communication within the DELTA network could reduce this threat. Furthermore a lot of the information is already available on papers in the production and lab environments.

Information that is used and transmitted is classified as confidential or internal depending on the estimated value for a competitor to AstraZeneca. Confidential information is assumed to be of value for a competitor to AstraZeneca. [71] [72] [63]

| Information | Confidential | Internal | Used or communicated within |
|---|---|---|---|
| Master batch recipe material | | | MES system and the DELTA network. |
| Batch and quality control protocols | | | MES system and the DELTA network. Production and Lab |
| Batch recipes (electronic work instructions) | | | MES system, ZETA, production area VLAN and the DELTA network |
| Batch report material | | | MES system, ZETA and the DELTA network |

*Table 8.1 Classification and use of information with MES system*

To transform this risk to an opportunity, the implementation of EBR increase the information sent electronically but at the same time have a potential to reduce the risk of industrial espionage in production due to the reduced amounts of printed batch protocols that have to be used. Thus the EBR implementation provides an opportunity to limit industrial espionage against Sweden Operations and AstraZeneca.

### 8.3.6 Validation of batches

With the increased automatization of the validation of batches that is one of the main benefits with the EBR system comes also a risk. If there is some malfunction in the EBR software or the underlying operating systems, there is a risk for errors in the validation process. Most likely the validation will not be approved. A worst-case scenario could be that the system becomes programmed or changed in a way that approves batches that not should be approved. An illegitimate insider might reconfigure the system in a way that makes the system approve batches that not should be approved. Even that this scenario might be seen as hypothetical, the impact could be serious harm of patients and a serious loss of AstraZeneca reputation. Thus the integrity of the EBR system is very important.

### 8.3.7 Traceability of batches

Failure in the EBR system might lead to that long term stored data from manufactured batches is lost.  The likelihood of this scenario can be reduced through printing the batch files for all manufactured batches or by providing data redundancy to the part of the MES system that is used for long-term data storage of batch records.

## 8.4 IS security evaluation of suggested implementation solutions

*This section assumes that a majority of the production areas at the Södertälje site becomes connected to the MES and EBR system and mainly focuses on the first three IS security risks identified in section 8.3; Wireless network vulnerabilities, MES/EBR system availability and Availability of EBR critical systems.*

### 8.4.1 Model I

Placing the MES system in ZETA and utilization of a wireless network with an access point connected inside the DELTA network. This solution will demands communication with ERP systems in GAMMA. This solution adds the less extra communication with GAMMA.

**Wireless network vulnerabilities**
The wireless connection creates a vulnerability to war-driving inside DELTA. Therefore it is very important that the added wireless access points have a high level of security. If the access points are assigned a separate VLAN, EPSILON could be used as a DMZ between the access points and the production or ZETA. If model I is chosen there must be a thorough risk assessment concerning the location and operation of such access points and wireless networks. [37]

**EBR system availability**
Placing the MES system in ZETA provides the MES system with the same level of IS security as the THETA system. According to the risk analysis in chapter 6 the main risks are virus from EPSILON, production VLAN, JOTA VLAN or a process automation system vendors or support organizations. It is concluded that the ZETA segment is less vulnerable to virus outbreaks than in GAMMA.

**Availability of EBR critical systems**
Placing both the MES and the THETA system in the ZETA segment reduces this problem to mainly concern communication with ERP systems if DELTA is isolated from GAMMA.

### 8.4.2 Model II

Placing the MES system in ZETA and utilization of a wireless network with access point connected to GAMMA network. This solution demands communication with GAMMA for the communication with the access points for a required wireless network and with ERP systems.

**Wireless network vulnerabilities**
Operating a wireless network from GAMMA will make it possible to use EPSILON as DMZ for the communication with the access points. Data from wireless connected personnel and equipment will not be in communication with the MES system if the DELTA is isolated from GAMMA.

**EBR system availability**
Placing the MES system in ZETA provides the MES system with the same level of IS security as the THETA system. According to the risk analysis in chapter 6 the main risks are virus from EPSILON, production VLAN, JOTA VLAN or a process automation system vendor or support organization. It is concluded that the ZETA segment is less vulnerable to virus outbreaks than in GAMMA.

**Availability of EBR critical systems**
Placing both the MES and the THETA system in the ZETA segment reduces this problem to mainly concern communication with ERP systems and wireless connected personnel and systems. In the scenario where DELTA must be isolated from GAMMA there will be problems with the communication to wireless devices.

### 8.4.3 Model III

Placing the MES system in GAMMA and use of wireless network with access points in GAMMA. Since the MES system is dependent on information from the SCADA and DCS systems this solution will add most extra traffic between GAMMA and the DELTA network. This solution does not demand a special DELTA wireless network access point and makes communication with ERP systems easier.

**Wireless network vulnerabilities**
The wireless connection will not directly affect DELTA.

**EBR system availability**
Placing the MES system in GAMMA will provide a situation where a DMZ not is protecting the MES system. Therefore this solution can be concluded as being the most vulnerable to malicious code (virus) and hacking incidents.

**Availability of EBR critical systems**
In the scenario where DELTA must be isolated from GAMMA there will be major problems with the communication between production and the MES system. Thus this solution is likely to cause the MES connected production to halt if the connection to GAMMA is intentionally closed or disrupted due to for example an IBM caused network problem or virus outbreak in GAMMA.

### 8.4.4 Connecting to IS security standards

Connecting to AstraZeneca IS security standards the MES system will be needed to perform communication directly to the corporate network. Therefore there is no mandatory rule that states that the MES system has to be operated from inside the DELTA network. It is recommended to perform an IS security risk analysis based on the three models (presented above) to determine in which segment the MES system will be most vulnerable. If it is concluded that the MES system not have to communicate directly to GAMMA then it should be operated from ZETA according to AstraZeneca IS security standards. [32]

Deployment of the MES system in the corporate network creates a situation where many process automation systems must communicate with GAMMA through EPSILON. Comparing with a deployment of the MES in the ZETA segment, ERP systems must instead communicate with the MES through the DELTA-GAMMA firewall. Thus an analysis should be conducted in order to decide if it is desired to have MES-ERP or MES-process automation system communication through EPSILON. Consideration should also be given to the differences in time constants between process automation systems and ERP and MES systems. The communication bus must have capacity to handle large amounts of data if the process automation systems use EPSILON as DMZs for communication with the MES/EBR system.

With a MES system deployment in the corporate network it must be assured that the network connection or communication to process automation systems (BRONZE networks) is indirect (network connection (b)). That is ensuring that the communication bus in EPSILON works as DMZ. If it is concluded that this communication or connection is direct (network connection (a)), then all process automation must meet all mandatory aspects in the AstraZeneca document Mandatory standards and good practice for the security of process automation systems, or have global AstraZeneca approval for exceptions. This scenario will create a challenge for Sweden Operations in terms of administration, technical solutions and costs. This also removes some of the main advantages with the DELTA network architecture.

According to the NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, The NIST Guide to Supervisory Control and Data Acquisition (SCADA) and industrial Control Systems Security and DHS Control Systems Cyber Security: Defence in depth strategies documents, the use of a DMZ between production data historian servers or process automation systems and the corporate network is recommended. Both the NISCC document and the NIST document refer to as EPSILON and ZETA as a MES layer or a Process Information Network. Hence it is concluded that it is recommended to operate the MES system from inside the DELTA network within ZETA with EPSILON as DMZ between the MES system and GAMMA. [11] [17] [18]

According to the ISA 99 part 2 standard, it is very important to build in IS security in process automation systems from the beginning. Thus it is important to include IS security requirements in the system specifications when purchasing the system. This includes building the system on a platform that provide a good level of IS security including easy patching management of operating systems and applications, system hardening, good BCP and DRP possibilities and possibility to use encrypted communication. [13]

Since the MES/EBR system will be very important for the production, it is important that the system is constructed with ability for quick recovery from IS security incidents. The system might for example include automatic recovery software. Since the system is likely to be in operation for a long time, it is also important to choose a platform that is likely to be supported by a vendor in the future, in order to ensure that security patches will be developed continuously.

Thus the system should be built on reliable and secure technology that will be supported in the future and allows for easy maintenance and quick recovery from IS security incidents.

### 8.4.5 Conclusions and suggestions

Model I ads a war-driving attack (wireless hacking) possibility to the DELTA network. Model II might create problems for production due to that communication with devices that are connected through wireless networks, will be closed if DELTA is isolated from GAMMA. Model III is most vulnerable to virus incidents and violate recommendations in industrial IS security standards. This solution is also very vulnerable to the scenario where DELTA is isolated from GAMMA.

In a perspective of IS security, a conservative suggestion is therefore that the MES/EBR is operated from inside the DELTA network. If model I is implemented a further suggestion is to evaluate the use of EPSILON as DMZ between a wireless access point and ZETA or the production area networks.

It is recommended to perform a risk assessment of the possibility for wiretapping of information in the DELTA network. Evaluation of encrypting communications within the DELTA network based on this risk assessment should be made if the MES/EBR system is implemented.

## 8.5 Summary

The identified IS security risks with the MES/EBR implementation are:

- The scenario where the MES system malfunction or becomes infested with a virus

- The scenario where EBR critical systems becomes unavailable or infested with a virus

- Increased wireless network vulnerabilities in DELTA.

- Wiretapping of information in DELTA

- Problems with software for automatic validation of batches

- Problems with electronic storage of records and traceability of batches

The two first risks might cause the production to undesired halts. Due to these risks, a conservative suggestion is to operate the MES system from inside the DELTA network. The implementation of a MES and connection of a wireless network to the DELTA network demands thorough IS security risk assessment.

The MES/EBR implementation provides an opportunity for reducing the risk of espionage against Sweden Operations through that the amount of printed batch protocols that are used in the production and lab environments is reduced.

# 9 Conclusions

## 9.1 Overview

This chapter presents the main conclusions from the study. Some ideas for future work, investigations and research, are also presented.

## 9.2 Evaluation of DELTA and IS security compliance

According to current available IS security standards the DELTA architecture is suitable for a large manufacturing site within Sweden Operations. It is considered as almost a best practice solution for a large manufacturing site with highly vulnerable process automation systems that demands a high level of IS security and at the same time connectivity to the corporate network. It is less suitable for a small manufacturing site.

The architecture and implemented IS security measures are mainly compliant with global AstraZeneca IS security standards. Most exceptions from global AstraZeneca IS security standards are found on local process automation systems in the production areas.

The impression is that the IS security level and the effectiveness of DELTA would benefit from a clear security program. There exist AstraZeneca policies, guidelines and SOPs for how to secure process automation systems and networks. These documents aim for systems and networks on different levels or are in general intended for a specific system or a special kind of systems.

## 9.3 Most severe IS security risks in the production at the Södertälje site

According to the risk analysis there are threat scenarios with consequences and impacts that might be very costly for Sweden Operations. A Day zero scenario (Major virus outbreak in the production due to that the anti-virus in the DELTA network not is updated in time) might cost Sweden Operations as much as -. A major virus outbreak in the THETA system might cost -.

The most severe IS security risks that endangers DELTA and the production of pharmaceuticals at the Södertälje site are:

- An unknown virus from GAMMA or the Internet that the antivirus in EPSILON can resist, with major impact on all the different networks and production areas within the DELTA network (known as a Day zero scenario).

- An IBM error that have major effects on both the DELTA network and the production area networks.

- Non-validated updates or patching of infrastructure services or network equipment prevents friendly communications or network services in the DELTA network.

- Major virus infection from system providers in a production area network with PLC based process automation systems.

- Major virus infection from direct-dial up access in a production area network with PLC based process automation systems.

- Major incident due to remote access through a direct-dial up connection in a production area network with PLC based process automation systems.

- Major incident due to virus outbreak from a non-standard client in a production area network with PLC based process automation systems.

The built in architecture and IS security safeguards address most of the identified threat scenarios, except for the Day zero scenario. The Day zero scenario potential is well known to the site Local IS security managers.

## 9.4 IS security evaluation of MES/EBR system implementation

The main IS security risks with the MES/EBR implementation are:

- The scenario where the MES becomes unavailable

- The scenario where EBR critical systems becomes unavailable

- Increased wireless network vulnerabilities

- Wiretapping of information

- Problems with automatic validation of batches

- Problems with electronic storage of records and traceability of batches

The two first risks might cause the production to undesired halts if the MES for example is infested with a virus. Due to these risks, a conservative suggestion is to operate the MES from inside the DELTA network. The implementation of a MES and connection of a wireless network to the DELTA network demands thorough IS security risk assessment.

## 9.5 Organizational conclusions about the IS security work in the production at the Södertälje site

According to ISA 99, IS security can be viewed as a cultural issue and should be addressed in a holistic manner. Therefore there is need for a view on the IS security work at the Södertälje site in perspectives of organization and culture. Putting an organizational perspective on IS security in the production at the Södertälje site defines four major parts: Global AstraZeneca IS security directions and standards, IBM, the Infrastructure (DELTA) and finally the operations. The operations include personnel from departments such as DSS, DPS, and personnel that works with lab systems.

Global AstraZeneca IS security provides standards and rules that are difficult to adapt to the business needs and requirements that the operations have (see section 9.6 second paragraph).

IBM officially provide their services as agreed but there is doubt whether their services comply with the GMP regulations, that they will deliver the promised DRPs and BCP executions and that they sometimes fail to deliver their services as agreed. Examples that cost Sweden Operations time and money include patching of wrong systems and network malfunctions. The impression is also that IBM creates a lot of administrative work for Sweden Operations and not always understand the special requirements that pharmaceutical manufacturing demands.

The operations is constantly under pressure to become more efficient and to cut costs. Therefore the requirements for increased IS security protection on process automation systems is viewed as something that mainly interfere and create problems. The impression when discussing IS security with personnel in production is that they identify virus infection as the major threat source. In most cases the virus is believed to origin from GAMMA and the Internet. The threat of social engineering, misbehaving personnel (both intentionally and unintentionally) and the risk for local virus infection outbreaks in a production area VLAN is unknown or somewhat naively neglected.

Only the infrastructure is considered to deliver a satisfying level of IS security in a way that oblige with the other parts.

Thus there is a need for harmonization between AstraZeneca Global IS security standards and the special conditions and business requirements that the operations have. The communication between Sweden Operations and IBM must also be improved and simplified to ensure that IBM deliver their services as agreed and with a satisfying level of IS security.

The intention with the DELTA ISA 99 security program and especially the DELTA security group (DSG, section 7.3) is to overcome those problems and address the IS security risks in the production at the Södertälje site in an organizational manner. Selective actions for an increased IS security level will in the long run be more expensive than well-reasoned, strategic and cooperative work from all involved parts. With the DSG the communication might also be simplified and sharing of knowledge increased, and the IS security work less bureaucratic and more effective.

## 9.6 Future work, investigations and research

**AstraZeneca**
Despite that the AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services recently has been approved as an AstraZeneca global IS security standard, it can be concluded that the document needs to be changed and updated. [31]

There is need for a mandatory and more specified section the network scenario (b) in the AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services, that demands global exception, that states that process automation system clients needs to have closed USB, CD-ROM and floppy drives and hardening of operating systems (section 4.3.4 in AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services). This section should replace the physical security section (4.3.11 AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services) as requiring global approval.

The vast amounts of exceptions that demand local approval will probably also create administrative problems at the different AstraZeneca sites.

Isolation from the corporate network is not the solution for all IS security problems. Moving from network connectivity scenario (b) to network connectivity scenario (c) might be concluded as removing all mandatory requirements that need global or local approval in the document. But this is not the solution for all threats. Viruses can still be locally injected and systems intentionally or unintentionally abused.

The AstraZeneca Mandatory Standards and Good Practice for the Security of Process Automation Services is also very indistinct and can be interpreted very differently at different AstraZeneca sites. Thus AstraZeneca needs to update the Mandatory Standards and Good Practice for the Security of Process Automation Services document.

When ISA 99 part 3 and 4 and the IEC 62443 have been released there is need for a new evaluation of the DELTA architecture and implemented IS security work and measures, with the help of these standards. This work could identify new threats and vulnerabilities as well as new technical and administrative solutions for combat of new and already identified threats. There is also need for keeping an eye out after new standards concerning architectures and DMZs in the manufacturing systems context. This area is currently underrepresented in the ISA 99 work. [27]

The MES/EBR system implementation must be carefully looked after to ensure that the present IS security level in the DELTA network is maintained. Together with a possible need for encrypting of the communication on the DELTA network this also remains as a topic for future investigations. The AGA 12 standards represent a good reference source for SCADA systems communication and cryptography. [9]

**ISA**

Finally the area of IS Security concerning MES and MIS systems implementation and operations, remains as an area for future research. In the future this could possibly be added as fifth part of the ISA 99 standard. This part could also include network and system architecture solutions for connecting process automation system networks, MES, MIS and corporate networks, according to ISA 99 and ISA 95.

# 10 References

## Printed material

**[1]** AstraZeneca PLC (2007); *Annual report 2006*

**[2]** ISPE (2001); GAMP 4 – *GAMP Guide for Validation of Automated Systems*, *Good Automated Manufacturing Practice*, ISPE

**[3]** Olsson, Gustaf & Rosen, Christian (2005); *Industrial Automation; applications, structures and systems*, Revised Edition, Media-Tryck, Lund University, Lund, Sweden

**[4]** McClure, Stuart, Scambray Joel & Kurtz George (2005); *Hacking Exposed; Network Security Secrets & Solutions*, Fifth Edition, Mcgraw-Hill, California, USA

## Articles

**[5]** Anonymous, (2007); *CYBER SECURITY - PLANT SAFETY: Beating the hackers*, Process engineering, February 2007, p. 21-22

**[6]** Byres, Eric & Lowe, Justin (2004); *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*, VDE Congress Berlin 2004

**[7]** Henrie, Morgan & Carpenter, Philip (2006); *Process Control Cyber-Security: A Case-Study with Design Proposals*, IEEE, Industrial and Commercial Power Systems Technical Conference paper

**[8]** Singer, Bryan L & Weiss Joe (2005); *Control systems cyber security*, Control Engineering, Volume 52, Issue 2, p. 26-31

## Standards, guidelines and policies

**[9]** AGA (2006); *AGA 12, part 2,* draft 2006-03-31

**[10]** CIDX (2004); *Report on Cyber security Vulnerability Assessment Methodologies*, Version 2.0, http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm , 20070223

**[11]** Department of Homeland Security (2006); *Control Systems Cyber Security: Defence in Depth Strategies*, External report # INL/EXT-06-11478, http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf , 20070227

**[12]** ISA (2000); *ISA-95.00.01-2000 Enterprise-Control System Integration Part 1: Models and Terminology*, ISBN: 1-55617-727-5

**[13]** ISA (2006); *ISA-d99.00.01 Security for Industrial Automation and Control Systems Part 1: Concepts, Terminology and Models*, Draft 2 Edit 8

**[14]** ISA (2006); *ISA-d99.00.02 Security for Industrial Automation and Control Systems Part 2: Establishing an Industrial Automation and Control Systems Security Program*, Draft 2 Edit 9

**[15]** ISA (2003); *ISA-dTR99.00.01 Security Technologies for Manufacturing and Control Systems*, Draft 14

**[16]** ISA (2004); *ISA-dTR99.00.02 Integrating Electronic Security into the Manufacturing and Control Systems Environment*, Draft 15

**[17]** NISCC (2005); *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, Revision 1.4, http://www.cpni.gov.uk/ProtectingYourAssets/ElectronicSecurity/scada.aspx , 20070220

**[18]** NIST (2006); *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security; Recommendations of the National Institute of Standards and Technology*, Special publication 800-82, Initial public draft, csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf , 20070220

**[19]** Primatech Inc (2003); *A Scenario Based Approach For Industrial Cyber Security Vulnerability Analysis*, http://www.primatech.com/info/paper_a_scenario_based_approach_for_industrial_cyber_security_vulnerability_analysis.pdf , 20070223

## Course material

**[20]** ISA (2004); *Securing Industrial Networks; Cyber Protection for Automation, Control and SCADA Systems*, Course IC32C Participant Note set, Version 1.5

**[21]** Sweden Operations/OKT (2006); *Introduktion i GMP*

## Electronic sources

**[22]** AstraZeneca Sweden, www.astrazeneca.se, 20070306

**[23]** http://bridgefieldgroup.com/bridgefieldgroup/glos6.htm#M, 20070424

**[24]** Cyber Threat Source Descriptions, http://www.us-cert.gov/control_systems/csthreats.html, 20070306

**[25]** Overview of Cyber Vulnerabilities, http://www.us-cert.gov/control_systems/csvuls.html , 20070305

**[26]** Pressmeddelande; AstraZenecas tidigare aviserade effektiviseringsprogram i produktionen tar nu form, http://www.astrazeneca.se/5804_18923.aspx?year=2007&l1=&l2=&l3= , 20070330

**[27]** Project : IEC 62443 Ed. 1.0, http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=sea22.p&search=iecnumber&header=IEC&pubno=62443&part=&se=&submit=Submit, 20070425

## AstraZeneca documentation

**[28]** Enckell, Carl & Perhsson, Mikael (2005); *A model for MES in Pharmaceutical Production*, Master Thesis, Department of Automatic Control, Lund University

**[29]** AstraZeneca Aggregating risks to site level; (Swe Ops, UK OPS, US OPS), PowerPoint presentation

**[30]** AstraZeneca global Computer Users Code of Conduct,

**[31]** Global Automation Strategy Team – Security Group (2006) *Mandatory standards and good practice for the security of process automation systems*, Draft J

**[32]** Global Automation Strategy Team – Security Group (2004) *Secure Network Isolation of Process Automation Computer Systems*, Version 1.0

**[33]** AstraZeneca Global IS Incident reporting in 2005

**[34]** Alfa plant description

**[35]** AstraZeneca IRM tips and guidance

**[36]** Password Standards, IS SEC 027

**[37]** Wireless LAN Security, IS SEC 029

**[38]** AstraZeneca IS Security FAQ's

**[39]** Mission Sweden Operations OI

**[40]** Mission Sweden Operations

**[41]** Presentation of THETA system, PowerPoint presentation

**[42]** Beta plant description

**[43]** Vision Sweden Operations OI

**[44]** BaDS DELTA *Beskrivning av datoriserat system DELTA*, Version 1.0

**[45]** BaDS DCS *Beskrivning av datoriserat system DCS*

**[46]** RUT 310235 *Viruskontroll av extern programvara som implementeras i processtyrsystem förvaltade av*

**[47]** RUT 400113 *Krav och regler för extern personal med GMP-relaterade uppdrag inom Analytisk Kontroll.*

**[48]** RUT 400038 *Katastrof och kontinuitetsplan för produktionssystem THETA*

**[49]** RUT 400451 *Utförande vid anslutning av Remote Control inom Gärtuna*

**[50]** SOP 016054 *Vulnerability Assessment Standard Operating Procedure*

**[51]** SOP 110104 *Behörighetshantering av datoriserade produktionssystem THETA*

**[52]** SOP 110179 *Viruskontroll av datautrustning för produktionssystem inom Tabletttillverkning*

**[53]** SOP 200014 *Validering*

**[54]** SOP 200082 *Validering av datoriserade system*

**[55]** SOP 300091 *Behörighet - processtyrsystem*

## Interviews

**[56]** Roger Belvén, IS-quality Manager, OI, 20070316

**[57]** Dan Bergvall, System Manager, CTS, 20070509

**[58]** Mikael Björklund, Automation Engineer, CTS, 20070319

**[59]** Tomas Borg, Group manager, QC Lab Coordination, 20070416

**[60]** Max Börjesson, System Service Manager, OITP, 20070316

**[61]** Johan Callin, Associate Director Automation, AstraZeneca Engineering, 20070316

**[62]** Henrik Carnborg, System Manager, CTS, 20070509

**[63]** Chatarina Daggenfelt, First Line Manager, QA & QC Systems, 20070522

**[64]** Tomas Ersson, System manager, OITP, 20070313

**[65]** Christer Gottschalk, LISSM, OITI, 20070424

**[66]** Torbjörn Hjalmarsson (Phone), Technical Specialist, CTS, 20070321

**[67]** Malin Holmstrand, Business Controller, OF, 20070326

**[68]** Robert Järn, Process Technician, TP, 20070507

**[69]** Fredrik Lundgren (Phone), Quality Manager, QA Computerized systems, 20070319

**[70]** Britt-Marie Linder (Phone), Group manager, TP, 20070425

**[71]** Monica Lindmark-Hamberg, (Phone), Group manager, TP, 20070425

**[72]** Catrin Mattson, Business Controller, OF, 20070326

**[73]** Joakim Moby, IT Infrastructure Manager, OITI, Numerous interviews spring 2007

**[74]** Fredrik Paulsson (Phone), Finance manager, OF, 20070411

**[75]** Ola Persson, IS project manager, OI Project Management, 20070411

**[76]** Tomas Raidma (E-mail), DPS , 20070329

**[77]** Ted Svensson, DSS, 20070325

**[78]** Björn Vingek, IS/IT, 20070321

**[79]** Östh, Anna, LISSM, OITI, 20070321

## Other sources

**[80]** MESA international (2006); *MESA Metrics that Matter Guidebook & Framework*

**[81]** Observations in ALFA and BETA, Spring 2007

**[82]** Test of connection of laptop to production area and JOTA VLANs, 20070320 (Appendix D)

# Appendix A

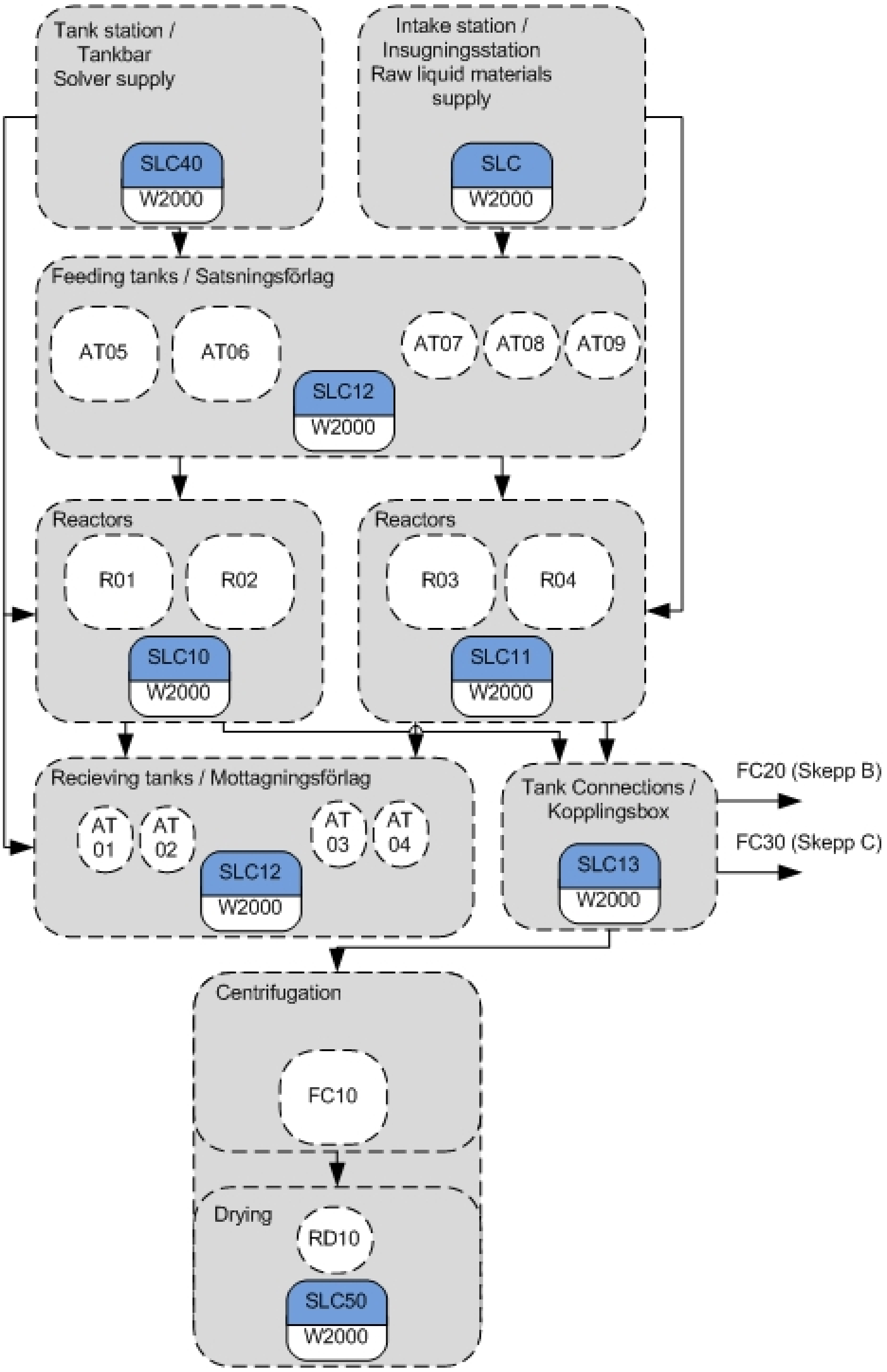
## AstraZeneca Risk criterions

| Definitions | Likelihood | | Impact (financial or time delay) | |
|---|---|---|---|---|
| | Measure | Score | Time Delay | Score |
| VH - Very High 5 | An event you can expect to happen (Once per year or more) | VH | 4 months | VH |
| H - High 4 | An event that can be anticipated to happen and this area/AZ or a closely allied company have experienced such an event (Once in 3 year) | H | 6 weeks | H |
| M - Medium 3 | A rare event that can be envisaged but has not occurred in this area or in AZ (Once in 10 year) | M | 2 weeks | M |
| L - Low 2 | An event that can be envisaged but hasn't occurred in the company history (e.g. requires a combination of two or more events to occur).(Once in 30 years) | L | 1 week | L |
| VL - Very Low 1 | An event that can be conceived but is considered to be very difficult to realise (e.g. requires a combination of several events to occur) (Once in 100 year or less) | VL | 1 day | VL |

# Appendix B

## Equipment and processes in ALFA and BETA

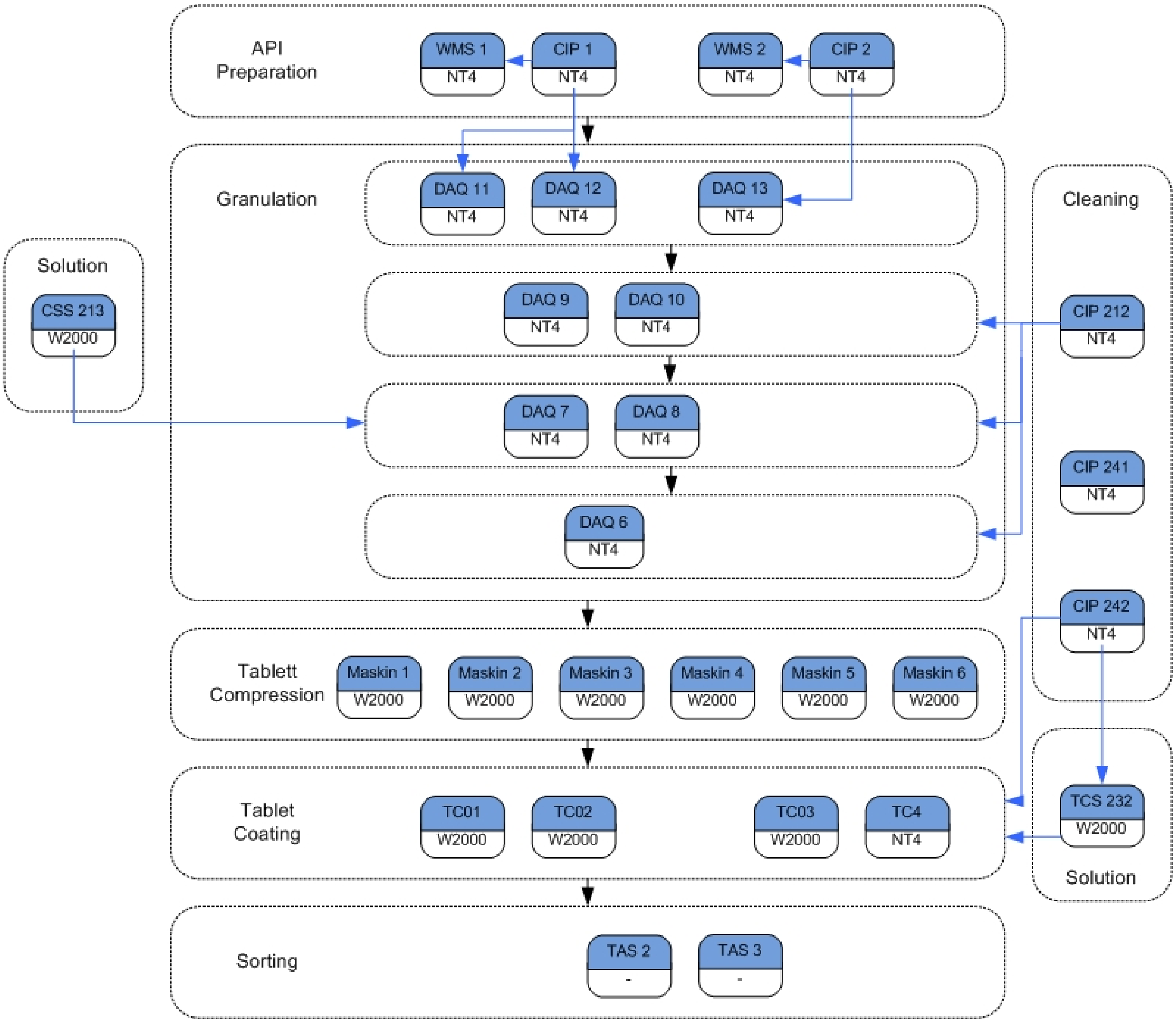
### Segment/Skepp A ALFA plant



## Tablet production area (BETA)

### Production flow in tablet production area in BETA

Blue arrows indicate feeding of solvers or sanitation fluids. Black arrows indicate production material workflow.



# Appendix C

## Threat scenarios and vulnerabilities

### DELTA CONDUIT

| Threat scenario | Consequences | Likelihood | Financial impact (lost production capacity) | Severity | Total cost for worst case scenario |
|---|---|---|---|---|---|
| Passive threats | | | | | |
| Information collection through wire-tapping. | | | | | |
| Scanning of the network architecture. | | | | | |
| **Malicious code** | | | | | |
| Unknown custom made virus for an attack against AstraZeneca or DELTA (Day zero attack) | | | | | |
| ***Unknown virus from GAMMA & Internet. (Day zero scenario)*** | | | | | |
| Virus from corporate network (GAMMA) & Internet | | | | | |
| Human errors | | | | | |
| Social engineering. Individual with knowledge about architecture and network weaknesses might be tricked or forced to reveal information or destroy critical computer equipment. | | | | | |
| ***IBM error that have major effects on both DELTA and the production area networks.*** | | | | | |
| Insider intentionally damages or abuse system or network. | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| ***Non-validated update or patching prevents friendly communications or network services.*** | | | | | |
| **Interference of systems and communication** | | | | | |
| Denial of service attack from the Internet. | | | | | |
| Undesired remote access from the Internet to a network inside DELTA | | | | | |

## EPSILON ZONE

| Threat scenario | Consequences | Likelihood | Financial impact (lost production capacity) | Severity | Total cost for worst case scenario |
|---|---|---|---|---|---|
| **Passive threats** | | | | | |
| Not applicable. | | | | | |
| **Malicious code** | | | | | |
| Virus from corporate network (GAMMA). | | | | | |
| Virus from ZETA. | | | | | |
| Virus from production area VLAN zone. | | | | | |
| Virus from JOTA VLAN zone. | | | | | |
| Virus from system provider. | | | | | |
| **Human errors** | | | | | |
| Social engineering. Individual with knowledge about architecture and network weaknesses might be tricked or forced to reveal information or destroy critical computer equipment or inject virus. | | | | | |
| Insider intentionally damages or abuse system. | | | | | |
| **Interference of systems and communication** | | | | | |
| Remote access from Internet to systems in EPSILON. | | | | | |

## ZETA ZONE

| **Threat scenario** | **Consequences** | **Likelihood** | **Financial impact (lost production capacity)** | **Severity** | **Total cost for worst case scenario** |
|---|---|---|---|---|---|
| **Passive threats** | | | | | |
| Not applicable. | | | | | |
| **Malicious code** | | | | | |
| Virus from corporate network (GAMMA). | | | | | |
| Virus from EPSILON. | | | | | |
| Virus from production area VLAN zone. | | | | | |
| Virus from JOTA VLAN | | | | | |
| Virus from system provider. | | | | | |
| **Human errors** | | | | | |
| Social engineering. | | | | | |
| Insider intentionally damages or abuse system. | | | | | |
| **Interference of systems and communication** | | | | | |
| Remote access from Internet to systems in ZETA. | | | | | |

## PLC based production area VLAN ZONE (BETA)

| Threat scenario | Consequences | Likelihood | Financial impact (lost production capacity) | Severity | Total cost for worst case scenario |
|---|---|---|---|---|---|
| **Passive threats** | | | | | |
| Wiretapping of information through direct dial-up. | | | | | |
| Scanning of network through direct dial-up. | | | | | |
| **Malicious code** | | | | | |
| Virus from corporate network (GAMMA). | | | | | |
| Virus from EPSILON. | | | | | |
| Virus from ZETA. | | | | | |
| Virus from other production area VLAN zone. | | | | | |
| Virus from JOTA VLAN zone. | | | | | |
| ***Virus from system vendor or laptop.*** | | | | | |
| Virus from AZ laptop. | | | | | |
| Virus from operator on standard client. | | | | | |
| ***Virus from operator on non-standard client.*** | | | | | |
| E-mail carried virus. | | | | | |
| ***Virus through direct dial-up.*** | | | | | |
| **Human errors** | | | | | |
| Manipulation of operating system. | | | | | |
| Manipulation of Process control related system. | | | | | |
| Social engineering. | | | | | |
| **Interference of systems and communication** | | | | | |
| ***Direct Dial-up access.*** | | | | | |
| Remote access to systems from the Internet. | | | | | |

## DCS production area VLAN ZONE (ALFA)

| Threat scenario | Consequences | Likelihood | Financial impact (lost production capacity) | Severity | Total cost for worst case scenario |
|---|---|---|---|---|---|
| **Passive threats** | | | | | |
| Wiretapping of information through direct dial-up. | | | | | |
| Scanning of network through direct dial-up. | | | | | |
| **Malicious code** | | | | | |
| Virus from corporate network (GAMMA). | | | | | |
| Virus from EPSILON. | | | | | |
| Virus from ZETA. | | | | | |
| Virus from other production area VLAN zone. | | | | | |
| Virus from JOTA VLAN | | | | | |
| Virus from system vendor or laptop. | | | | | |
| Virus from AZ laptop. | | | | | |
| Virus from operator on standard client. | | | | | |
| Virus from operator on non-standard client. | | | | | |
| E-mail carried virus. | | | | | |
| Virus through direct dial-up. | | | | | |
| **Human errors** | | | | | |
| Manipulation of operating system. | | | | | |
| Manipulation of Process control related system. | | | | | |
| Social engineering. | | | | | |
| **Interference of systems and communication** | | | | | |
| Direct Dial-up access. | | | | | |
| Remote access to systems from the Internet. | | | | | |

## JOTA VLAN ZONE

| Threat scenario | Consequences | Likelihood | Financial impact (lost production capacity) | Severity | Total cost for worst case scenario |
|---|---|---|---|---|---|
| **Passive threats** | | | | | |
| Not applicable. | | | | | |
| **Malicious code** | | | | | |
| Virus from corporate network (GAMMA). | | | | | |
| Virus from EPSILON. | | | | | |
| Virus from ZETA. | | | | | |
| Virus from production area VLAN zone. | | | | | |
| Virus from system vendor or laptop. | | | | | |
| Virus from AZ laptop. | | | | | |
| Virus from operator on lab client | | | | | |
| **Human errors** | | | | | |
| Manipulation of operating system. | | | | | |
| Manipulation of lab instrument related system. | | | | | |
| Social engineering. | | | | | |
| **Interference of systems and communication** | | | | | |
| Remote access to systems from the Internet. | | | | | |

# Appendix D

## Test of connection of laptop to production area and JOTA VLAN

| Test | AZ laptop | 'External' laptop |
|---|---|---|
| Automatic assignment of IP address (DHCP)? | No | No, no automatic DHCP assignment |
| Possibility to assign IP address (DHCP)? | No | Yes, DHCP |
| Possibility to generate 'ping'? | - | Yes, the gateway, main router and EPSILON. ZETA no. |
| Possible to ping the firewall? | - | No |
| Possible to run Remote Desktop on EPSILON-servers? (Access with normal PRID?) | - | Yes, no access with normal PRID account. |
| Possible to run Remote Desktop on ZETA-servers? | - | No |
| Possible to run Telnet and http protocols on EPSILON? | - | Telnet activated (password protected), http activated (password protected) |
| Connect shares on EPSILON-servers (c$)? | - | No |
| Possible to ping clients in other 'BRONZE' VLAN | - | No |

# Appendix E

## DELTA IS security program implementation responsibilities

### Translation

| Swedish title | English title |
|---|---|
| Systemägare | System owner |
| Systemförvaltare | System manager |
| Systemapplikationsägare | System application owner |
| Systemapplikationsförvaltare | System application manager |
| System/Tjänsteleverantör | System/Service provider |
| Chef IT SWEOPS IS | Director IT SWEOPS IS |
| Lokal enhetschef eller fabrikschef | Head of local production area or lab department |
| Lokal CTS or Lab system manager | Head of local system managers group |
| Standardklient eller -server / Icke standardklient eller -server | Standard client or server / Non-standard client or server |

### Defence-in-depth strategy

| | System, service or network owner (suggested future system owner) | Demand or management responsible department / personnel<br>Key Stakeholder | Governance responsible department / Personnel | Supplier of service responsible department / personnel | Mandatory | Priority |
|---|---|---|---|---|---|---|
| 1 | DELTA owner | DELTA manager | IT Services | IBM | M | * |
| 2 | DELTA owner | DELTA manager | IT Services | IBM | M | * |
| 3 | (DELTA owner) | DELTA manager | IT Services | IBM | | * |
| 4 | DELTA owner / System owner of non-standard client | DSG + LISSM | IT Services / System governing organization | IBM / Service supplier | M | * |
| 5 | DELTA owner | DSG + LISSM | AZ Engineering | IBM | | ** |
| 6 | DELTA owner / System owner of non standard-clients | DELTA manager / System owner | IT Services / System manager | IBM / System provider | M | *** |
| 7 | Director IT SWEOPS IS | IT Coordination and Security Manager | IT Infrastructure Manager (DELTA | - | | ** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | manager) | | | |
| **8** | LISSM | DSG + LISSM | DSG | DSG | | ** |
| **9** | Director IT SWEOPS IS | DSG + LISSM | DSG | HR + LISSM | | ** |
| **10** | DELTA owner + System application owner / System owner | DSG + LISSM | IT Services + system application manager / System manager | IBM+ service provider / System supplier | | ** |
| **11** | DELTA owner + System application owner / System owner | LISSM | IT Services + System application manager / System manager | IBM / System service provider | **M** | *** |

## IS security policy for DELTA network, services and applications

| | **System, service or network owner (suggested future system owner)** | **Demand or management responsible department / personnel**<br>Key Stakeholder | **Governance responsible department / Personnel** | **Supplier of service responsible department / personnel** | **Mandatory** | **Priority** |
|---|---|---|---|---|---|---|
| **12** | DELTA owner | DELTA manager | IT Services | IBM | **M** | * |
| **13** | DELTA owner | DELTA manager | IT Services | IBM | | * |
| **14** | DELTA owner | DELTA manager | IT Services | IBM | **M** | * |
| **15** | DELTA owner | DELTA manager + DSG | IT Services | IBM | | ** |
| **16** | DELTA owner | DELTA manager | IT Services | IBM | **M** | * |
| **17** | DELTA owner | DELTA manager | IT Services | IBM | **M** | ** |
| **18** | DELTA owner | DELTA manager | IT Services | IBM | **M** | ** |
| **19** | Director IT SWEOPS IS + DELTA owner | LISSM | DSG | DSG | | ** |
| **20** | DELTA owner + THETA owner + Eta systems owners | DELTA manager + THETA manager + Eta systems manger | IT Services + Omikron + provider of Lab systems | IBM + Omikron + Provider of Lab systems | **M** | * |
| **21** | DELTA owner / System application owner | DELTA manager / System application manager | IT Services / Service application provider | IBM / Service application provider | **M** | ** |
| **22** | (System owner) | DSG | Project manager | System provider | | ** |
| **23** | DELTA owner / THETA owner / Eta systems owner | DSG | IT services / IT Services + OITP / IT Services + Eta systems manager | IBM / IBM + Omikron / IBM + Eta systems provider | | *** |
| **24** | DELTA owner | DSG | DSG | IBM / IBM + Omikron + OITP | | * |
| **25** | DELTA owner | DSG | IT Services | IBM | | ** |
| **26** | DELTA owner / THETA owner / Eta systems owner | DSG | IT services / IT Services + OITP / IT Services + Eta systems manager | IBM / IBM + Omikron / IBM + Eta systems provider | | *** |
| **27** | DELTA Owner | DSG | DSG | IBM + Omikron + IT services + System application managers in | | ** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ZETA | | |
| **28** | DELTA owner | DELTA manager | IT Services | IBM | | * |
| **29** | DELTA owner | DELTA manager | IT Services | IBM | **M** | * |

## IS security policy for Production area and Lab VLAN environments

| | System, service or network owner (suggested future system owner) | Demand or management responsible department / personnel<br>Key Stakeholder | Governance responsible department / Personnel | Supplier of service responsible department / personnel | Mandatory | Priority |
|---|---|---|---|---|---|---|
| **30** | Director IT SWEOPS IS | LISSM | Head of local production area or lab department | HR + LISSM | | ** |
| **31** | Director IT SWEOPS IS | LISSM | Head of local production area or lab department | HR + LISSM | | ** |
| **32** | DELTA owner + System application owner / System owner of non-standard client | LISSM | IT Services + System application manager / System manager | IBM / System service provider | **M** | * |
| **33** | Director IT SWEOPS IS | LISSM | Head of local production area or lab department | QQU | | ** |
| **34** | Director IT SWEOPS IS | LISSM | LISSM | DSG | | *** |
| **35** | DELTA owner | DSG | IT Services | IBM | | ** |
| **36** | DELTA owner | DSG | AZ Engineering / CTS project managers / Lab system project managers | AZ Engineering / CTS project managers / Lab system project managers | | ** |
| **37** | DELTA owner + System application owner / System owner of non-standard client | DELTA manager / System owner of non-standard client | IT Services + System application manager / System manager | IBM+ System application provider / System service provider | **M** | |
| **38** | System owner | System owner | System application manager / System manager | IBM+ System application provider / System service provider | **M** | *** |
| **39** | System owner | System owner | System application manager / System manager | IBM / System service provider | | |
| **40** | DELTA owner / System owner of non-standard client | DELTA manager / System owner of non-standard client | IT Services + System application manager / System manager | IBM / System service provider | **M** | *** |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| **41** | DELTA owner / System owner of non-standard client | DELTA manager / System owner of non-standard client | IT Services + System application manager / System manager | IBM / System service provider | **M** | *** |
| **42** | DELTA owner + System application owner / System owner | DELTA manager / System owner | IT Services + System application manager / System manager | IBM / System service provider | **M** | ** |
| **43** | DELTA owner / System owner | DELTA manager / System owner | IT Services / System manager | IBM / System service provider | **M** | ** |
| **44** | DELTA owner / System owner of non-standard client | DELTA manager / System owner of non-standard client | IT Services / System manager | IBM / System service provider | **M** |  |
| **45** | Director IT SWEOPS IS | Head of local system managers group | Head of local production area or lab department | Local system managers |  | ** |
| **46** | Director IT SWEOPS IS | Head of local system managers group | Head of local production area or lab department | Local system managers |  | ** |
| **47** | Director IT SWEOPS IS | DSG | System managers + CTS + IT Services + IBM + OITP/Omikron | System managers + CTS + IT Services + IBM + OITP/Omikron |  | ** |
| **48** | System owner | DSG + LISSM | IT Services / System manager + CTS | IBM / System manager + CTS |  |  |
| **49** | DELTA owner | DSG | Local CTS + System supplier | Local CTS + System supplier | **M** |  |
| **50** | Director IT SWEOPS IS + Associate Director, Automation AZ Engineering | DSG | AZ Engineering / CTS project managers / Lab system project managers | AZ Engineering / CTS project managers / Lab system project managers |  | ** |
| **51** | Director IT SWEOPS IS | DSG | IT Infrastructure and Coordination manager + DSG | LISSM |  | ** |

## Integrated risk management (IRM)

| | System, service or network owner (suggested future system owner) | Demand or management responsible department / personnel<br>Key Stakeholder | Governance responsible department / Personnel | Supplier of service responsible department / personnel | Mandatory | Priority |
|---|---|---|---|---|---|---|
| **52** | **DSG** | **DSG** | **DSG** | **DSG** | | ** |

## Monitoring and reviewing of the DELTA IS security program

| | System, service or network owner (suggested future system owner) | Demand or management responsible department / personnel<br>Key Stakeholder | Governance responsible department / Personnel | Supplier of service responsible department / personnel | Mandatory | Priority |
|---|---|---|---|---|---|---|
| **53** | DELTA owner | DSG + DELTA manager | IT Services | IBM | | ** |
| **54** | DELTA owner | DSG + DELTA manager | IT Services | IBM | | ** |
| **55** | DELTA owner | DELTA manager | IT Services | IBM | M | * |

# Appendix F

## Abbreviations

| | |
|---|---|
| API | Active pharmaceutical ingredient |
| BaDS | Beskrivning av datoriserat system |
| BCP | Business continuity plan |
| CIDX | Chemical industry data exchange |
| CTS | Common Technical Support |
| DCS | Distributed control system |
| DHCP | Dynamic host configuration protocol |
| DHS | Department of homeland security |
| DMZ | Demilitarized zone |
| DRP | Disaster recovery plan |
| EBR | Electronic batch records |
| FDA | Food and drug administration |
| DSG | DELTA security group |
| FTP | File transfer protocol |
| GAMP | Good automated manufacturing practice |
| GAST | Global automation strategy team |
| GMP | Good manufacturing practice |
| HTTP | Hyper text transfer protocol |
| IP | Internet protocol |
| IRM | Integrated risk management |
| IS | Information systems |
| ISMO | international sales and marketing organization |
| IT | Information technology |
| KPI | Key performance indicators |
| LISSM | Local infrastructure IS security manager |
| MES | Manufacturing execution system |
| MIS | Manufacturing information systems |
| NISCC | National infrastructure security co-ordination centre (UK) |
| NIST | National Institute of Standards and Technology (USA) |
| OI | Information Services |
| OF | Finance |
| OIT | Information Technology |
| OITI | IT Infrastructure and Security |
| OITP | Production Information Systems |
| PLC | Programmable logic controller |
| QA | Quality Assurance |
| QC | Quality Control |
| R&D | Research and Development |
| RTU | Remote terminal units |
| RUT | Routine |
| SCADA | Supervisory control and data acquisition |
| SOP | Standard operating procedure |
| TP | Process Technology |
| TR | Technical report |
| USB | Universal serial bus |
| WAN | Wide area network |