chemtech

A Siemens Company

SABESP Water Supply Operation Control System – Security Design and Implementation

Raphael Pereira, CISSP CISA - Chemtech
Douglas Silva - Chemtech
Samuel Marques - SABESP

Complete Solutions for
Business Optimization

www.chemtech.com.br

sabesp

A little bit about Chemtech

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

BUSINESS process engineering and IT solutions and services since 1989

OBJECTIVES process and business optimization

FOCUS long-term relationship with clients, employees and the society

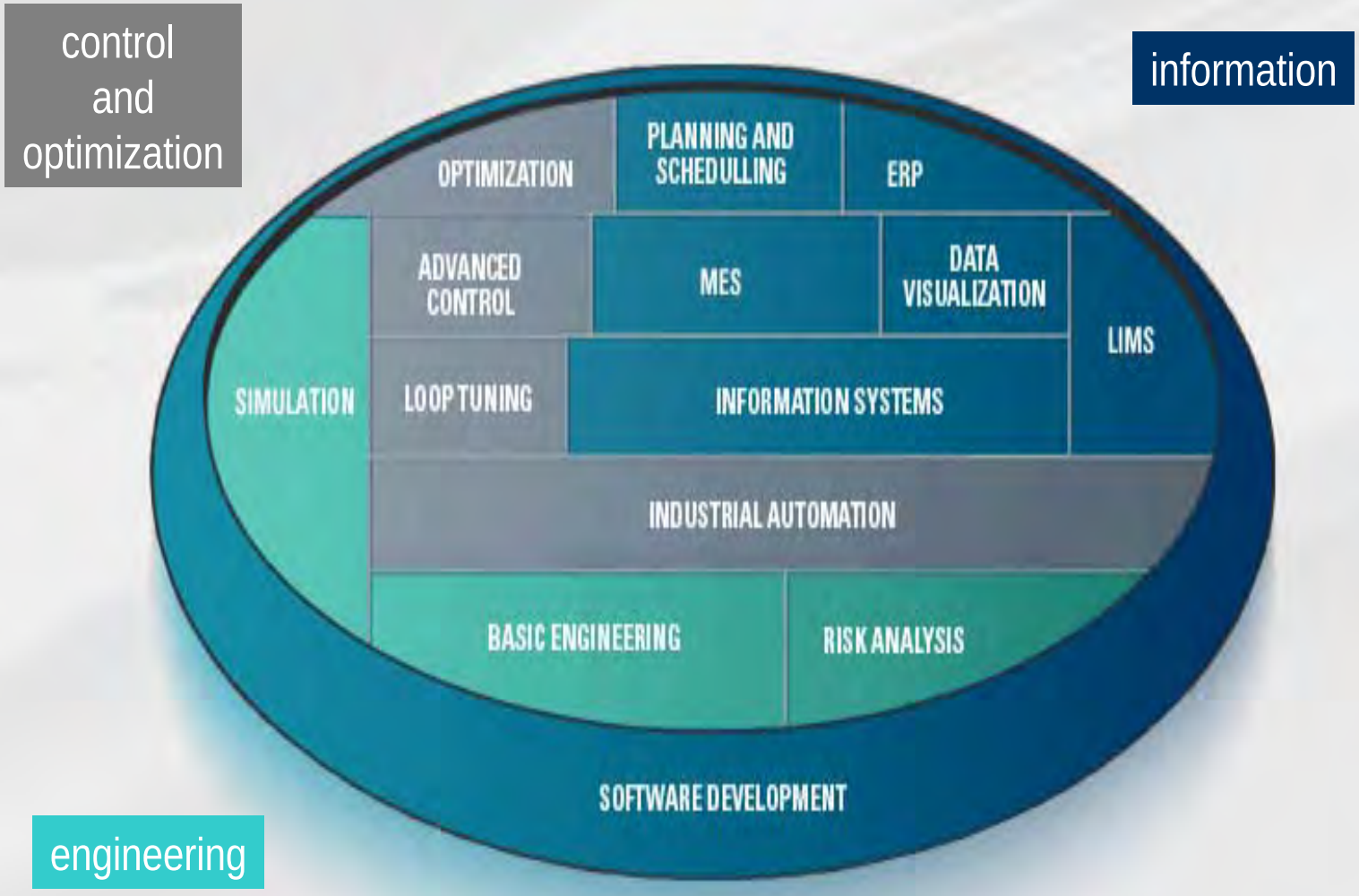
TEAM 350 highly qualifyied and motiveted employees around the world

More information on www.chemtech.com.br

Chemtech presence in the World

Global Solutions

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions



A little bit about SABESP?

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Mixed economy and open capital company

- Main shareholder is the Government of São Paulo's State
- It's shares are traded in the New York and São Paulo Stock Exchanges.
  - NYSE:SBS

Sabesp supplies 60% of water to the State's population

- Providing services to 367 out of the 645 cities
- It's goals until 2010 are to provide:
  - 100% of treated water
  - 85% of collected sewage
  - 76% of treated sewage

www.sabesp.com.br

Project History

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

In 2003, Sabesp started the new system functional specification with an external consulting.

- Didn´t have any security controls
- Only Sabesp Automation area was involved.

After that, Sabesp security area was involved to help this security design. The new design has two objectives:

- Network segregation
- Secure access from corporate users to information

Finally, at the end of 2005 the project began.

Main Goals

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Project main goals:

- Provide a reliable, secure and efficient water distribution to the third biggest metropolitan region in the world
- Provide detailed and specific water distribution information
  - new visions of the water distribution
  - Integrate with PMS System
- Be scalable to support new sites
  - remote operation from other distribution business areas
  - Integration with WTS controls systems
- Working with the old control system
  - during and six months after the implementation
- Pass tags only in control system network
- Support to SOX rules

Security Requirements

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Stability

- It's the main requirement

High availability and Integrity

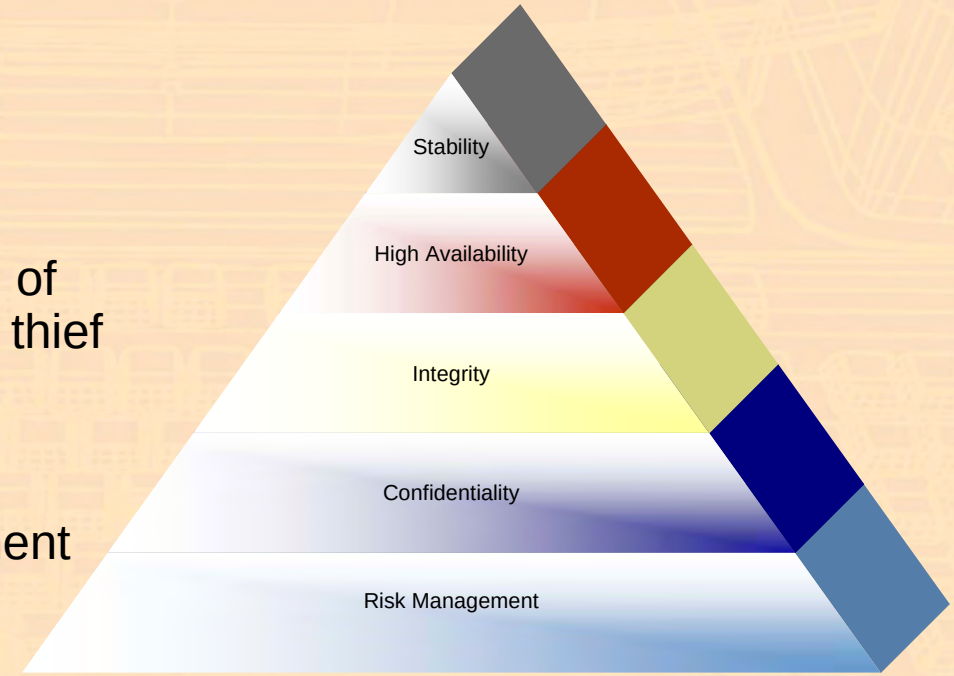
- To support the stability requirement

Confidentiality

- To support segregation of duties and protect data thief

Risk Management

- To permit risk assessment and treatment
- Threats change every day



RFP Security Controls

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

	Preventive		Detective	Corrective
Infrastructure	Access Control	HVAC	CFTV	System Tests
	Cabling Security	Electrical		Acceptance Tests
Network	Firewall	Network Segregation	Logging and Reporting	Functional and Operational Tests
	Switches and Firewalls with High Availability		AAA Server	Acceptance Tests
	Port Security and MAC Filtering			Penetration and security tests
System	System security configuration		Antivirus and Host IDS	Functional and Operational Tests
	NetworkTeaming		Logging and Reporting	Acceptance Tests
	Antivirus and Host IDS			Penetration and security tests
	Critical systems high availiability			
Application	Segregation of Duties		Application logging	Functional and Operational Tests
	Secure coding pratics			Acceptance Tests
	Source code revision and Control			Penetration and security tests
	Separeted development and test enviroment			

Project Information

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Project phases:

- Design
  - December 2005 to March 2006
  - Development of the Security Guideline
- Development
  - April 2006 to September 2006
  - Most of security controls are implemented using standards from security guideline
  - Development environment at Chemtech
- Implementation
  - September 2006 to November 2006
  - All security controls are implemented at Sabesp's Site
- Tests
  - December 2006
  - All Security and Functional/Operational tests are executed
  - Correct issues found in tests

Security Design

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

In this phase Chemtech developed a Security Guideline:

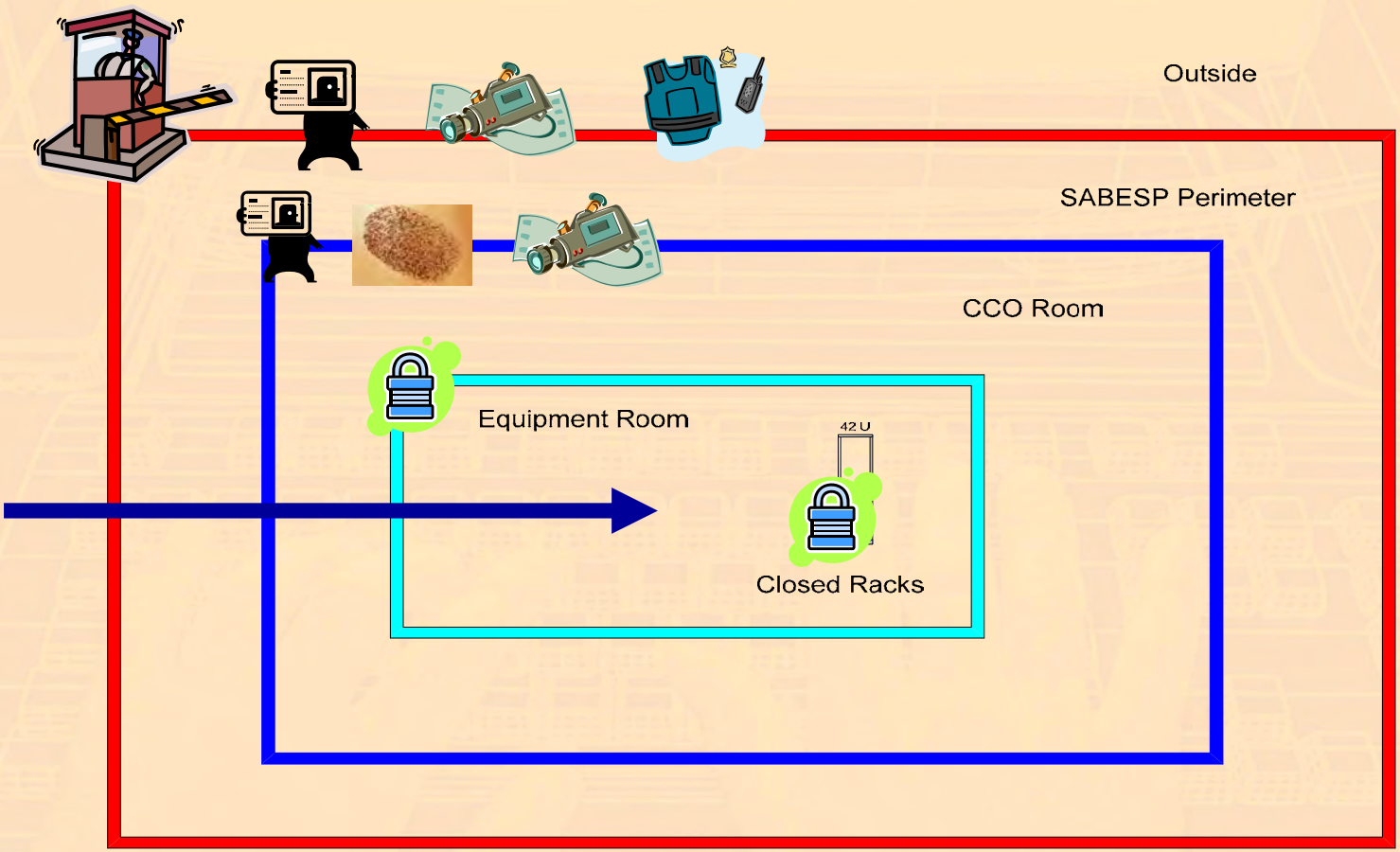
- All Sabesp business requirements were identified
- Planning, design and tests phases were defined
- Sabesp standards were mapped (hostnames, dns, windows domain standards, IP address and others)
- All the security concerns were planned, like firewalls, IDS, network equipments, authentication methods, etc
- All internal systems required or used were mapped
- Physical and cabling security specifications
- Security standards were mapped such as NSA Guides and others to help the implementation

This document was approved and revised by Sabesp

Security Implementation

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Physical and Infrastructure Security



Security Implementation

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

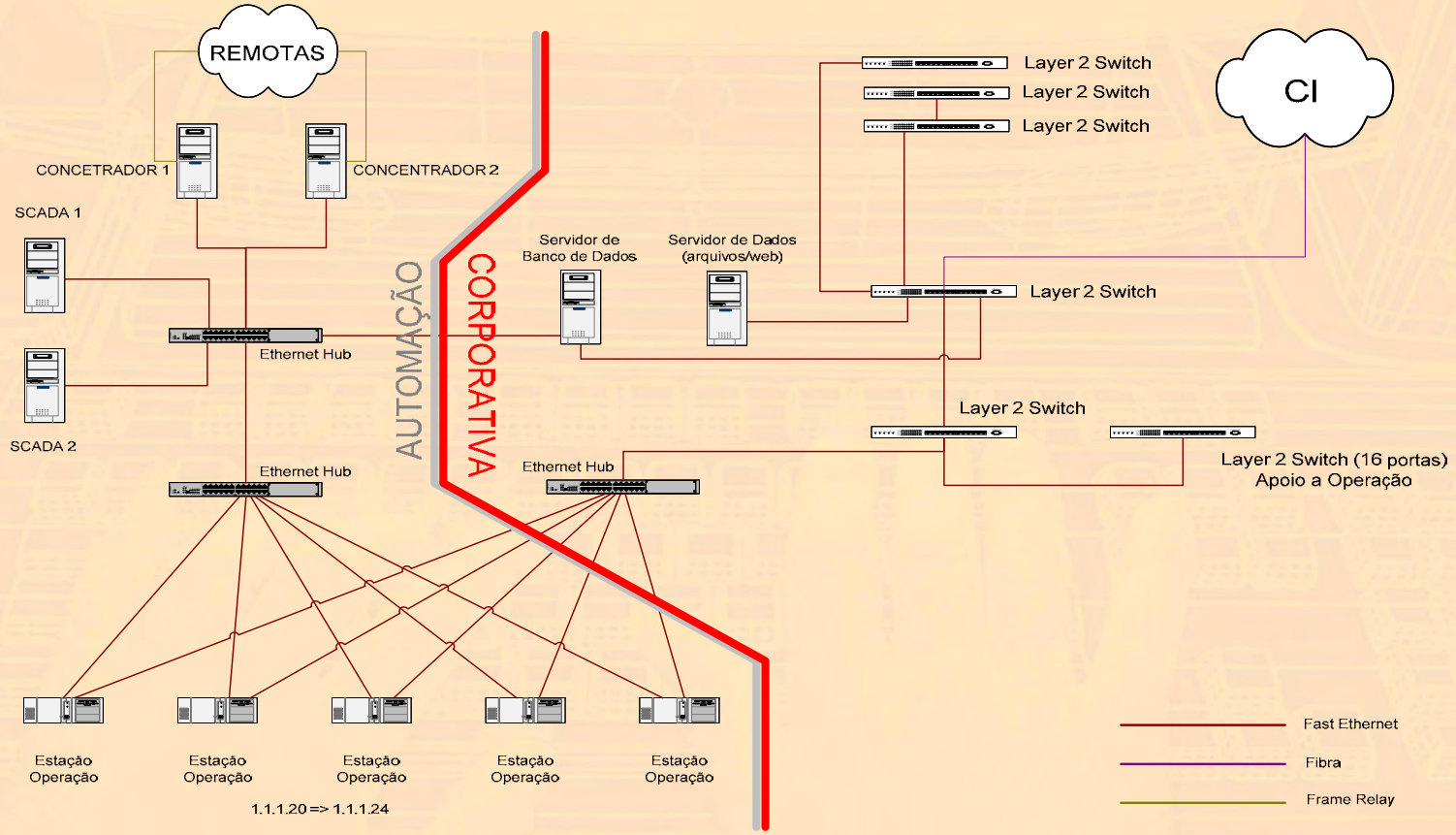
Physical and Infrastructure Security (Cont.)

- Power and Data Cabling Security
  - Rebuilt to support redundant electrical circuits and components
  - Old cabling removed and new one implemented following the standards of:
    - TIA/EIA
    - ISO
    - BICSI
    - ABNT (Associação Brasileira de Normas Técnicas)
- HVAC
  - Rebuilt to support the new environment (more equipment and people working)

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Network Security

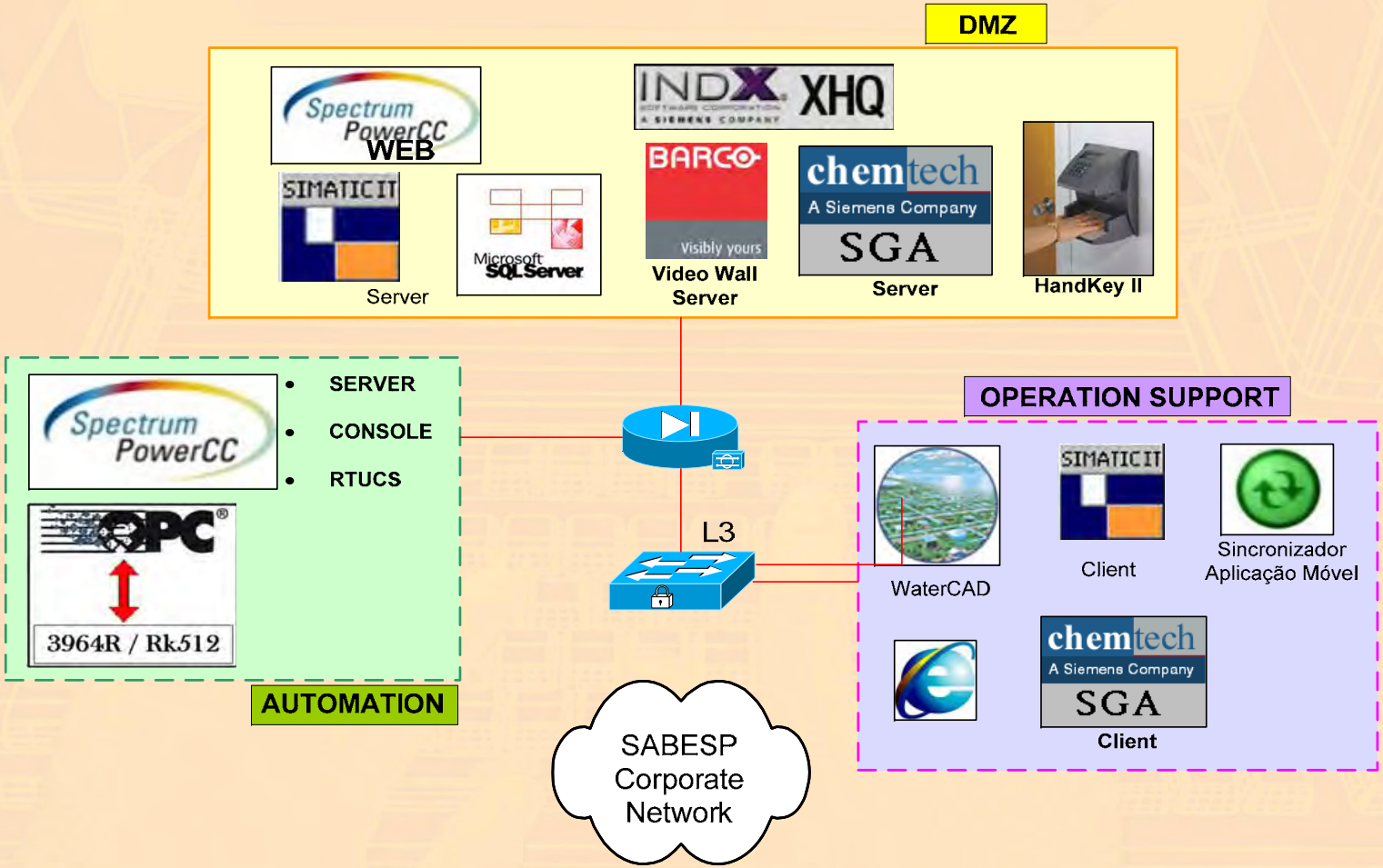
- Old system network design



Security implementation

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

New network concept



Security Implementation

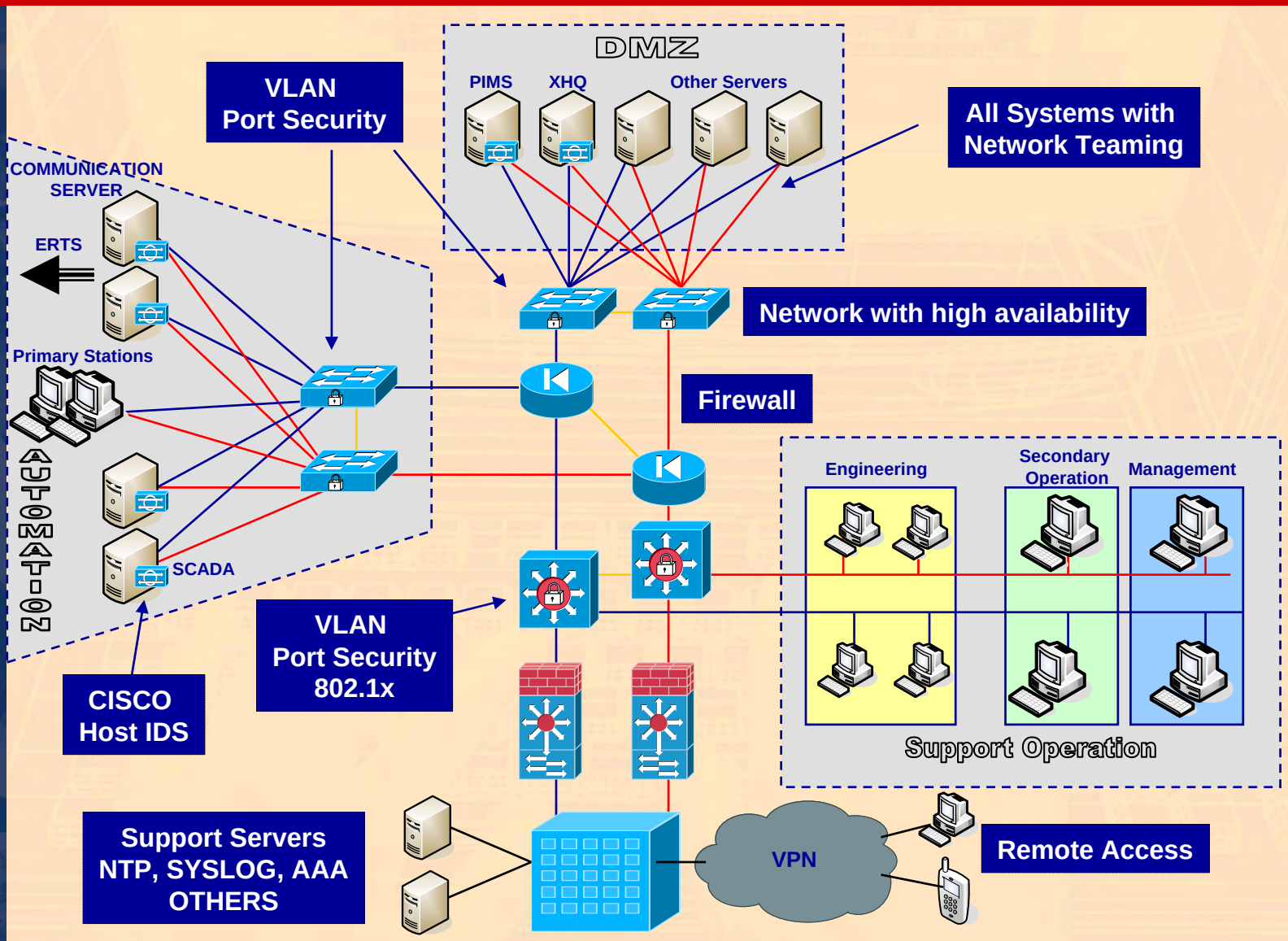
Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Controls implemented by Network

Control / Network	External	DMZ	Automation
IDS/IPS			
802.1x	X		
Routing Protocols	X		
Firewall		X	X
Host IDS		X	X
ARP Spoofing Protection	X	X	X
Access List	X	X	X
IP Address control	X	X	X
High Availability	X	X	X
Syn Flooding and Denial of Service Attacks protection	X	X	X
VLAN	X	X	X
Antivirus	X	X	X
System security configuration	X	X	X
Port Security	X	X	X

Security Implementation

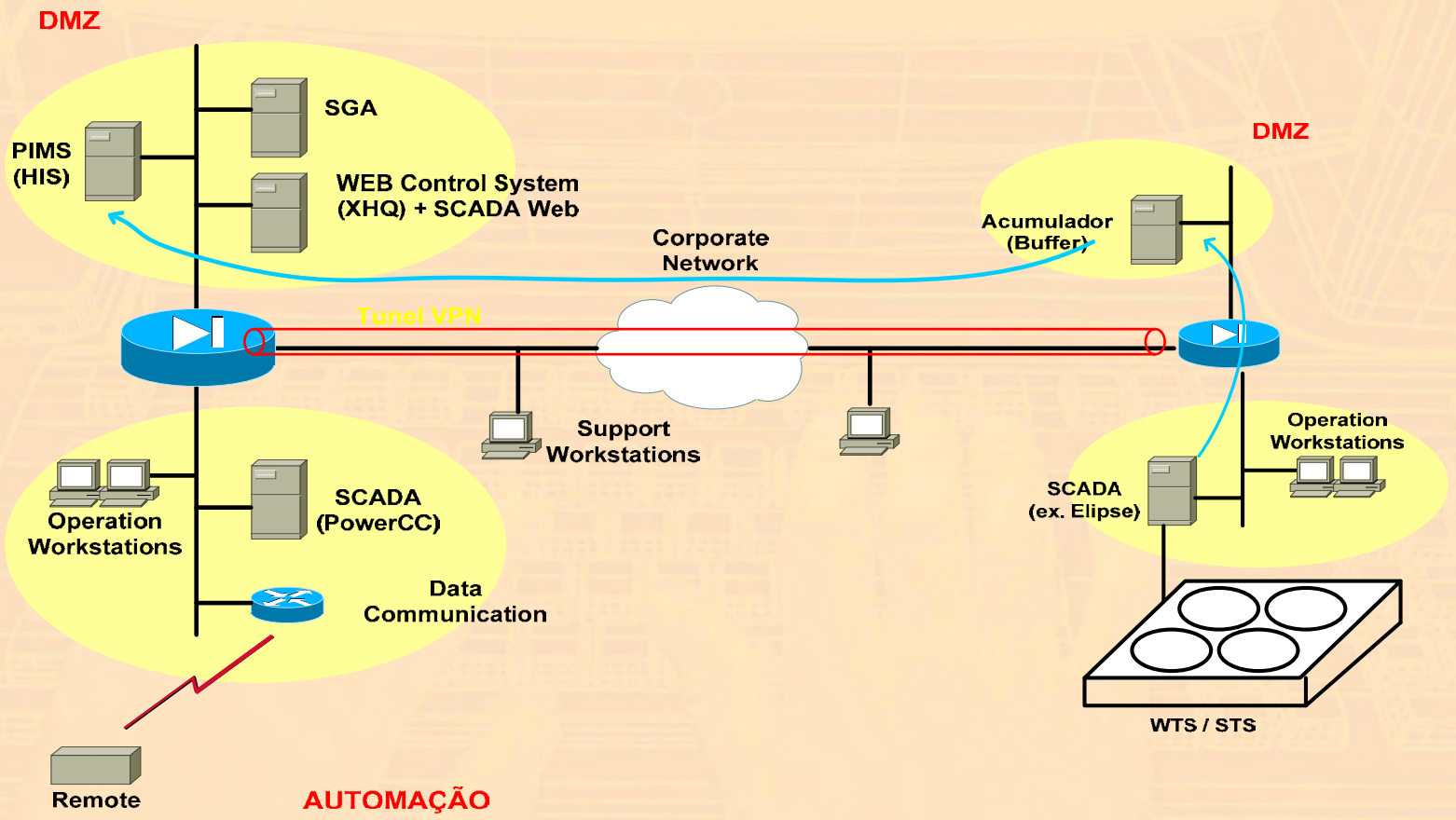
Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions



Security Implementation

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

- Future network integration with others control system



Security Implementation

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Network Security

- Firewall
  - Rules configuration strategy
    - Firewall configuration started at Chemtech with pass all rule and logging
    - Generated log was used to create all rules
      - after that default rule was changed to Deny all
    - All traffic is logged
  - Support to VPN Access
    - Focus with system expansion and remote access

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Network Security

- Switches
  - Automation and DMZ Networks
    - All ports use Cisco Port Security (MAC Address Filtering)
    - Used ports assigned to a dedicated VLAN
      - Unused ports assign to dummy VLAN
  - Support Operation
    - Secondary Operation VLAN with Port Security
    - All others ports using 802.1x network authentication
  - Use ACL to control management access
    - Management VLAN

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Network Security

- Support Servers
  - Radius
    - SABESP internal Microsoft IAS
    - AAA for VPN, 802.1x and management access
  - NTP Server
    - Sabesp had a internal NTP server used for clock synchronization
  - Syslog
    - SABESP Cisco works is the syslog server
  - Management Station
    - SABESP Cisco works as a Asset Management

Security Implementation

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

System Security

- All systems were configured following Security Best Practices
  - NIST Security Guidelines
  - Modulo Risk Management Software
- Host IDS
  - Cisco Host IDS
    - SCADA Servers
    - Communication Servers
    - PIMS Server
    - XHQ/SCADA WEB Server
  - In lab at this moment. Will be implemented in future project
- Antivirus
  - All systems have Antivirus
  - MacAfee VirusScan Enterprise
    - Managed by ePO (ePolicy Orchestrator)
    - Customized configuration
      - Not search in some directories
      - Not block some TCP/UDP ports

Security Implementation

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Application Security

- Development process
  - High Level specification
  - Prototype generation and approval by Sabesp
  - Final Implementation and Acceptance Tests
- Source code revision and control
  - Weekly team code revision meeting to find:
    - Bugs
    - Anti-patterns
    - Standards and practices awareness
  - Use SVN (Subversion) Server
  - One central database and integration server
  - Integrity check after commit using automatized tests, updating static code analyze
    - Notification on problems findings
- Development Environment
  - Segregated Environment
    - Code was developed in Chemtech
    - At acceptance tests code coming to Sabesp

Security Implementation

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Application Security (Cont.)

- Coding Standards
  - .NET development with use of Microsoft Standard
    - Design Guidelines for Class Library Developers
  - Graphical Interface Standards
    - SSW Rules to Better Windows Forms Applications
  - Use of Wiki to publish
    - all guidelines and standards
    - Coding exceptions
- Application development tests
  - Three level of tests
  - Internal team test
    - During and after features development
  - FAT (Factory Acceptance Tests)
    - At Chemtech
    - With Sabesp to approve the features
  - SAT (System Acceptance Tests)
    - At Sabesp
    - In running test environment

Security Tests

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Operational Tests

- Basic communication and hardware tests

Functional Tests

- Infrastructure
  - CCTV
  - Biometric access
  - HVAC
  - Electrical Components
- System and Network
  - All components
  - Basic failover tests

Security tests

- Use of ISACA IS Auditing Procedure
  - Document P8
- Many tools:
  - Nessus
  - Nmap and other tools at Backtrack Boot CD (www.remote-exploit.org)

Challenges and lessons learned

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Avoided the use of NAT

- Could have some OPC problems
- Corporate DNS register problems

Avoided the use of port security on firewall ports

- Firewall Failover could disable the ports

Check all hardware when you received

- Keyboards were received in Portugal Portuguese layout
- Cisco switches received without FO ports

Didn't forget the management layer in RFP

- After the project all management rules must be created
  - Backup Process
  - Management Process
  - Risk Management

Next steps

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions

Add new sites to the environment

- PIMS integration
- Remote Management

Create the management layer

- Backup Process
- Risk Management

Install and configure IDS in running environment

- Using Lab configuration example

Questions

Chemtech
Global Solutions
Sabesp
Project History
Main Goals
Security Requirements
RFP Security Controls
Project Information
Security Design
Security Implementation
Security Tests
Challenges and Lessons Learned
Next Steps
Questions