



**Process Control Systems
Industry Conference**

V&M of Brazil Business and M&C Networks Segregation Project

Leandro Pflieger de Aguiar, Computer Security Analyst – Chemtech

Ana Alda Gomes Tavares, Automation Solutions Analyst – V&M



Agenda

- ◆ **About V&M**
- ◆ **About Chemtech**
- ◆ **Motivations**
- ◆ **Project Goals**
- ◆ **Methodology**
- ◆ **Security Strategies**
- ◆ **Norms and References**
- ◆ **Challenges and Lessons Learned**
- ◆ **Results and Future Directions**

About Vallourec & Mannesmann



- **World Leaders in manufacture of Seamless Pipes;**
- **Rotary Piercing Mill Process**
 - High Pressure Supporting Pipes for **Automobile, Oil & Gas, OCTG** and **Civil Construction** Industries.
- **Total Production Capacity:** 3 Million tons of hot-rolled tubes;
- **V&M was founded in 1997 as a joint-venture between the french group Vallourec and the german Mannesmannröhren-Werke GmbH. In 2000, the VALLOUREC & MANNESMANN TUBES has incorporated the brazilian part of the company Mannesmann S.A., which became to be named as V & M do BRASIL;**
- **Some of V&M offering benefits:**
 - Total competence in production of seamless hot-rolled steel tubes;
 - Internal research with scientists and experts in the development of products and technology;
 - State-of-art in technology and processes (one of the World Most Modern factories producing Seamless Pipes);



About Chemtech

- ◆ **Set up in 1989 with 100% Brazilian capital**

- Engineering and IT consulting services, combining a deep process knowledge with the expertise on highly modern technological solutions;

- ◆ **A Siemens Company (joined in 2001)**

- ◆ **Products and Services**

- Basic Engineering, Risk Analysis, Simulation, Industrial Automation, Information Security, Loop Tuning, Advanced Control, Optimization, Information Systems (PIMS, LIMS, MES, ERP), Planning and Scheduling, Data Visualization.



Chemtech presence in World: Brazil, Germany, United States, Russia, Japan, Singapore, Thailand, Saudi Arabia, France, South Africa, Canada and Spain

About Chemtech



- Chemtech is The Best Company to Work for in Latin America – Great Place to Work Institute 2008 Edition
- Chemtech is The Best Company to Work for in Brazil – Great Place to Work Institute 2007 Edition

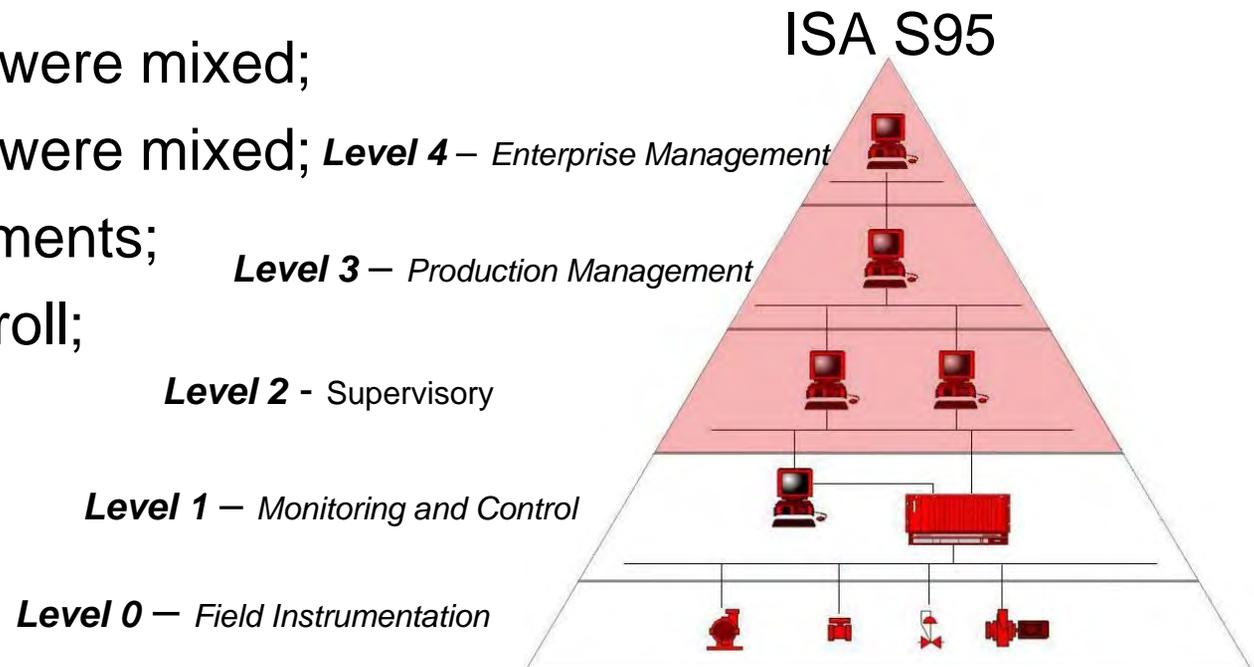


Motivations

Motivations

1) Absence of a Clear Separation between Network Levels

- Level 1 and 2 were mixed;
- Level 2 and 3 were mixed; *Level 4 – Enterprise Management*
- Shared Equipments;
- No traffic control;



Motivations

1) Absence of a Clear Separation between Network Levels: **Problems**

- Large Broadcast domains;
- Difficulty to TroubleShoot;
- Difficulty to isolate problems;
- Problems in one level affecting the other levels;
- Network Performance problems;



Motivations



2) Usage of Business (IT) Infrastructure to Connect Level 2 to the Higher Levels

- In situations where there wasn't a Backbone to connect;
- To support MES and PIMS communication to the higher levels;
- Just plugging the SCADA system to Business Network;
- Absence of appropriated and dedicated equipments, and network links;
 - Economy in physical links, but it caused the following problems.

Motivations



2) Usage of IT Infrastructure to Connect Level 2 to Higher Levels: **Problems**

- Equipments were not prepared to support the desired High Availability;
- Corporate IT services dependency;
- Difficulties on Shared Management
 - IT and Automation Differences;
 - Incompatible SLA's;
 - Problems in maintenance activities;
- Security Problems;

Motivations

3) Absence of Standardization Between Areas

- V&M Automation has six areas:
 - Automatic Lamination
 - Continuous Lamination
 - Maintenance and Utilities
 - Petroliferous Pipes
 - Siderurgy
 - Automotive Pipes and Precision Pipes (Trefilaria)
- Management Autonomy
- Financial Autonomy
- Technological Autonomy

Motivations

3) Absence of Standardization Between Areas: Issues

- Good because it causes agility,
- on the other hand...
 - Different levels in the quality of the documentation;
 - Different used protocols;
 - Different equipments;
 - Different strategies;
 - Hard to define traffic control between areas and between Business and M&C networks;

Motivations

4) Security Issues (CIA triad)

- Absence of Separation
 - Performance problems;
 - Availability Problems;
 - Difficulty in isolating Problems;
 - Threats sharing;
- Business infrastructure Usage
 - Maintenance Activities on Business network causing stops in Automation Area;
 - Malicious Code (e.g. virus) easily Spreading;
 - Applicability of Security Mitigating Controls and Policies;

Motivations

◆ In short

- Absence of clear separation between network levels;
- Usage of Business infrastructure to connect level 2 to the higher levels;
- Absence of standardization;
- Security Issues;
- **Recommendation from ISA 99**

8.3.11.5.4 Additional M&CS Security Practices

- An access control device is used to separate the business systems network from the M&CS network and limit user access to critical assets on both sides.

Project Goals

Goals

- ◆ **Project Main Goal: Business and M&C Networks Segregation**
 - Physical and Logical Business and M&C Networks Segregation;
 - LAN (Installing new Equipments and Configuring the olds), IP Address Plan;
- ◆ **Security Improvements (New Mitigating Controls)**
 - Network Security;
 - Firewall, VLANs Segregation, ACL's, Equipments and Services Configuration...;
 - OS Security;
 - Software and OS Updates (WSUS);
- ◆ **Implementation of a New AA Model (Active Directory)**
 - New Independent Network Services (DNS, DHCP, etc...);
- ◆ **Documentation**
 - Inventory, Topology Draws, Security Policies and Best Practices Manuals.
- ◆ **Major Requirement: no interference in production**

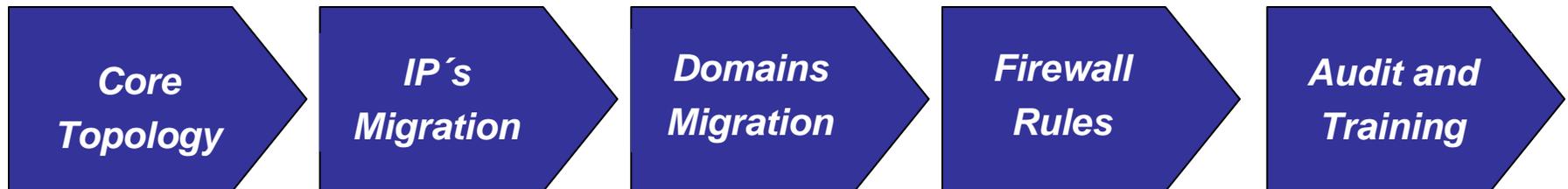
Methodology

Methodology

◆ Project Steps

- Conceptual Engineering;
- Physical infrastructure and hardware/software acquisition;
- Network Implementation;

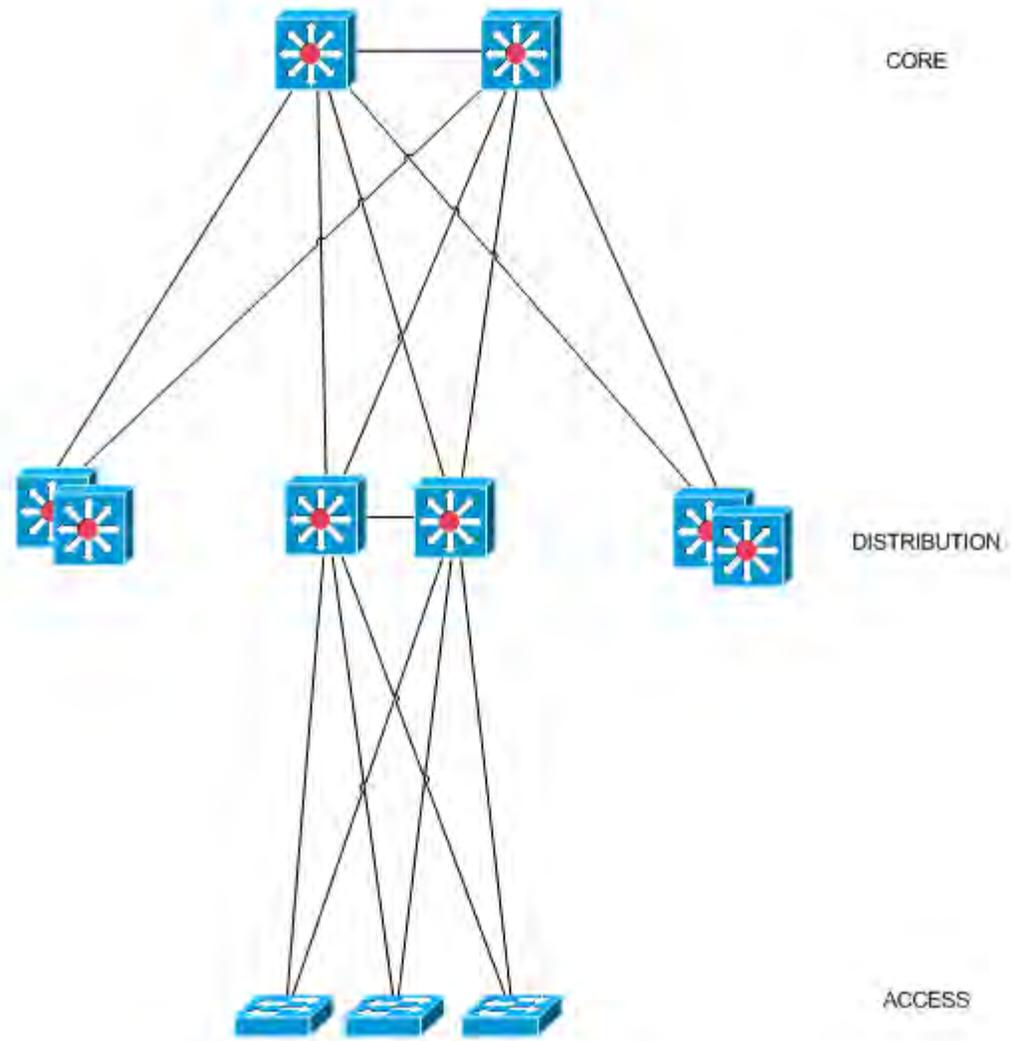
◆ Implementation Steps



Methodology

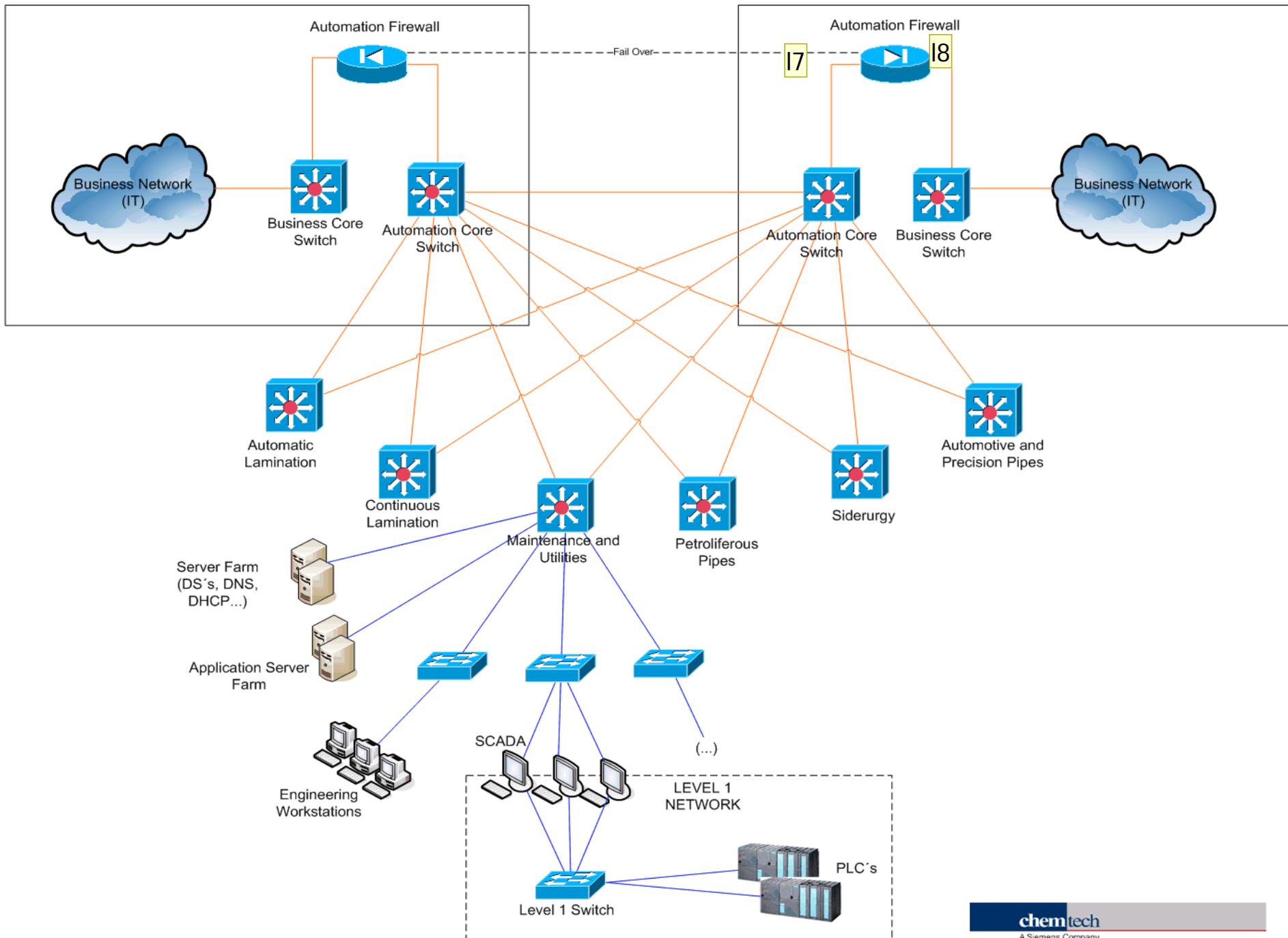
◆ Hierarchical Network Model

- Scalability;
- Fail Isolation;
- Performance;
- Easiness for SLA's;
- Easiness for administer;
- Small Fault Domains;
- Security: net traffic restricted to VLAN members.



Primary Datacenter

Secondary Datacenter (Contingency)



17 Rede TI
Serviços Corporativos: e-mail, Internet, ...
Servidores SAP;
Servidor PIMS;
Servidor MES;
Rede TA
Servidores de Aplicação;
Servidores de Comunicação PIMS;

Rede Nível 1
PLC´s;

leandro, 7/12/2008

18 Alta Disponibilidade Core
Firewalls Redundantes;
Switches Core Redundantes;
Fibras Ópticas Redundantes por Caminhos Distintos;
Redundância Ativo/Passivo (solução TI)
Mas possível Load Balance;
Segmentação por VLAN´s;
Local VLAN´s (end-to-end não necessária);
Apenas Equipamentos Gerenciáveis;
Equipamentos do Core Escaláveis;

leandro, 7/12/2008

Methodology

◆ Migration Strategies

- Lab tests (failover mechanisms, performance metering, spent time);
- Change Management
 - Gradative Changes;
 - High Impact Changes taking advantage of Programmed Repairing Stops;
 - Implementation Plans (step-by-step);
 - Rollback Plan (considering total available stop time);
 - Meetings prior to changes to understand and approve.
- Temporary Network Management Services
 - During and after Migrations, from our lab;
 - Fault Management for fast fail detection and response;
 - Performance Management to analyze overall behavior;
 - Accounting Management to characterize network traffic;

Security Strategies

Methodology – Firewall Rules Strategy

◆ Implement Firewall Rules isn't an Easy Task

- It can stop communication processes;
- Taking TCP/IP ports from vendors might cause problems;
- Technicians might have changed original TCP/IP ports;

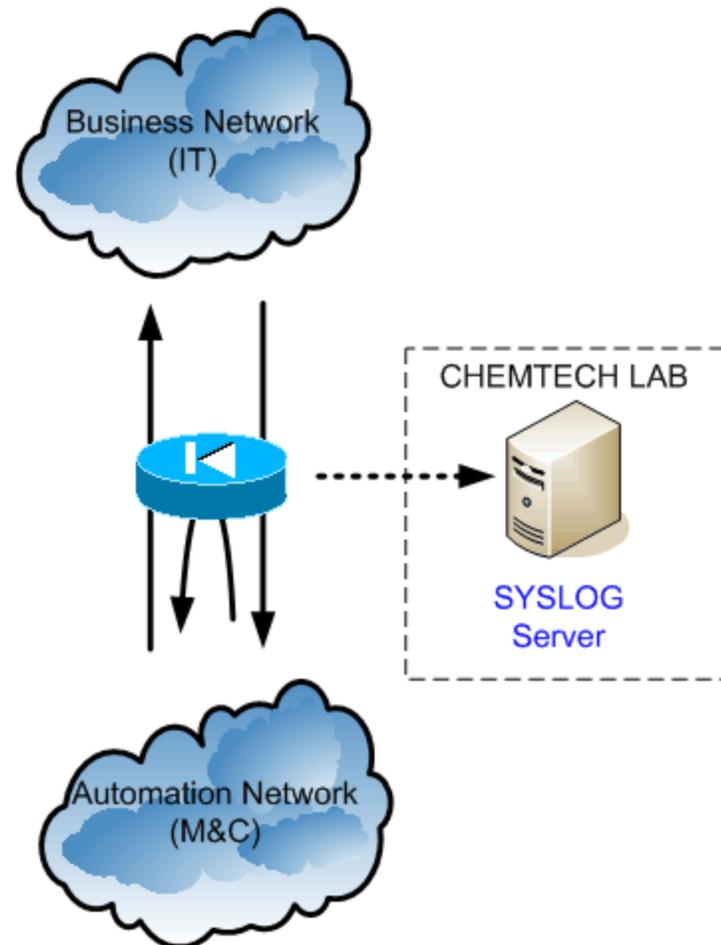
◆ Our Strategy

- Based on Pre network traffic characterization;
 - First measure, then compare to vendors datasheets;
- Changes insights by evidences;
- Changes M&C manager knowledge by his time;
- Low production impact;

Methodology – Firewall Rules Strategy

◆ How it works?

- Connection to Core;
- Creation of Free Access Rules;
- Information sent to Syslog Server;
- Summarization;
- Validation Meeting;
- Implementation;
- Observation (top denied for 3 days).



Methodology – Firewall Rules Strategy

◆ Summarization Process

- Traffic Summary;
- Table ordering
 - By Hits
 - By Bytes
- Validation Meeting
 - Vendor Recommendations (official ports);
 - Project Security Rules;

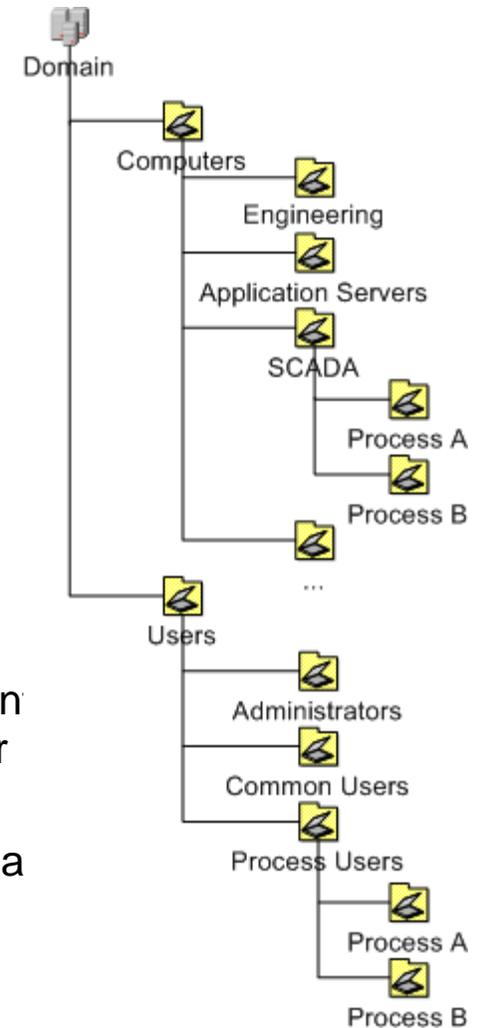
Showing : 1 to 20 of 558 Page : [1] 2 3 4 5 | [▶] [⏪] View per page : 5 10 [20] 25 50 75 100 150 200

Host	Destination	Protocol	Hits	Total Bytes(MB)	% Total Bytes
10.96.1.43	10.64.3.8	http	1462	551.9	1.4
10.64.3.6	10.75.1.68	Unknown	2	364.27	0.92
10.64.1.70	10.74.1.82	netbios-ssn	6	314.22	0.8
10.64.1.69	10.87.1.58	microsoft-ds	6	255.45	0.65
10.64.1.69	10.73.1.89	microsoft-ds	3	190.79	0.48
10.64.1.83	10.99.1.87	netbios-ssn	3	165.52	0.42
10.64.1.70	10.74.1.82	microsoft-ds	6	153.19	0.39
10.96.1.62	10.64.3.9	Unknown	229	150.79	0.38
10.64.1.63	10.87.1.58	netbios-ssn	10	118.63	0.3
10.64.1.84	10.99.1.117	netbios-ssn	4	101.84	0.26

Methodology – Active Directory

◆ Active Directory as AA Model

- Following Microsoft Best Practices and design methodology;
- Strong Usage of Group Policy;
- Considerations over OU Structure Design:
 - Separation between **Users and Resources** Accounts;
 - **Computer Accounts** Separated by System type (different softwares have different limitations) and Processes (for safe policy deployment);
 - **Process User Accounts Separated** from other users a by Process Type;

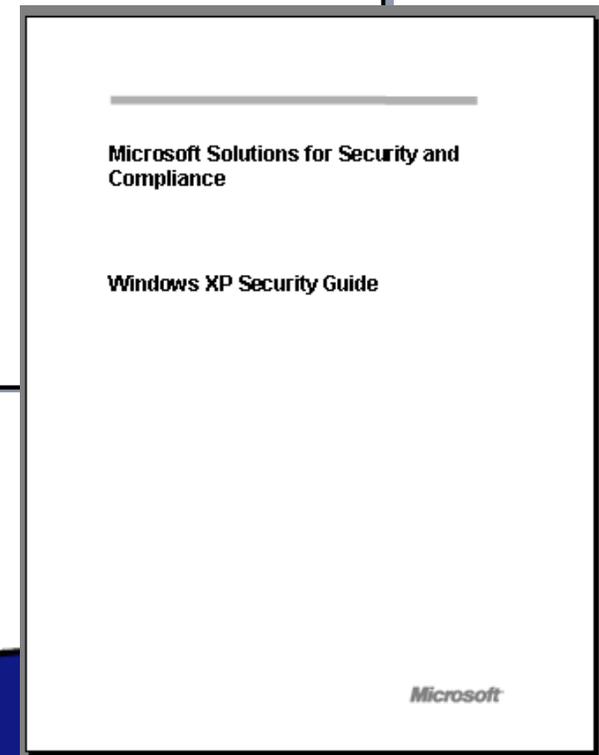
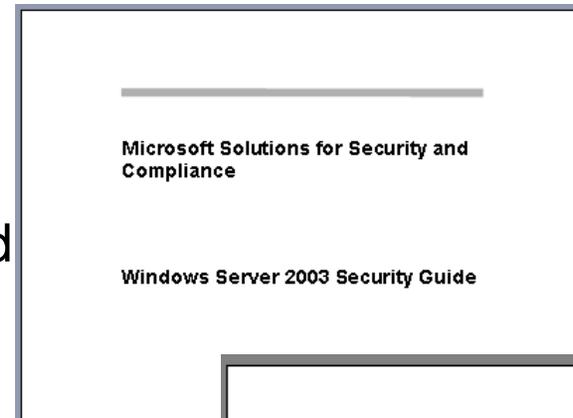


Methodology – Group Policy

- ◆ **Microsoft Security Guides Using GPO**

- Stronger templates (SSLF) adapted for Automation Limitations;

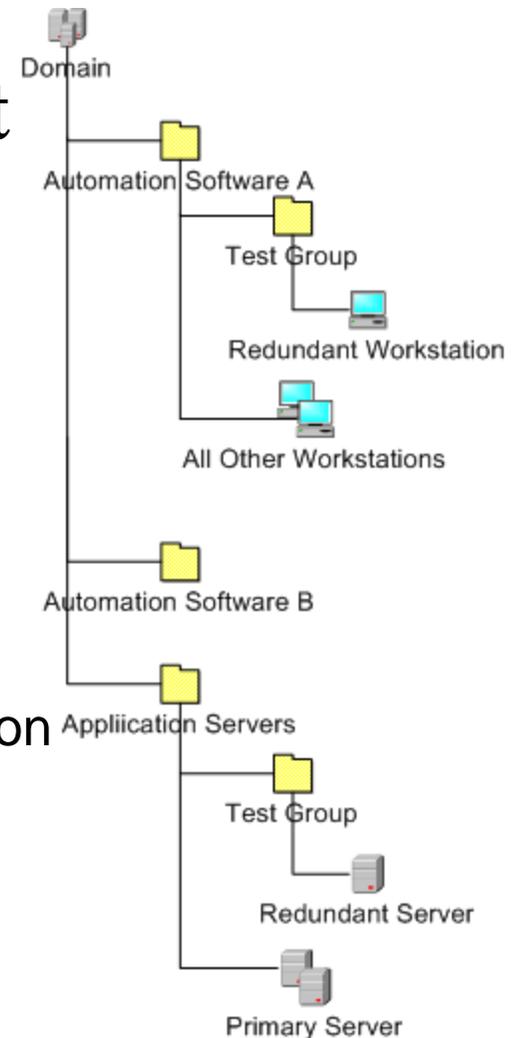
Setting	EC desktop	EC laptop	SSLF desktop	SSLF laptop
Audit account logon events	Success	Success	Success, Failure	Success, Failure
Audit account management	Success	Success	Success, Failure	Success, Failure
Audit directory service access	Not Defined	Not Defined	Not Defined	Not Defined
Audit logon events	Success	Success	Success, Failure	Success, Failure
Audit object access	No Auditing	No Auditing	Failure	Failure
Audit policy change	Success	Success	Success	Success
Audit privilege use	No Auditing	No Auditing	Failure	Failure
Audit process tracking	No Auditing	No Auditing	No Auditing	No Auditing
Audit system events	Success	Success	Success	Success



Methodology – Patch Management

◆ Patch Management Deployment Strategy

- Following ISA99 Recommendations;
 - Test before Apply;
- Separation between Servers and Workstations;
- Separation by Automation Software and by Process, when relevant;
- Separation of Primary and Redundant Application Servers;



Methodology – Security Assessment

◆ Detailed Security Assessment

– Following ISA99 Recommendations;

- Accompanied by a key person do lead the assessment process on each site;
- Separated by productive areas (different technological levels);
- Common database to record assessment results;
- Centrally reviewing all assessment results (realistic and comparable);
- Performed by an External Auditing Company;



– Auditing Methodology

- Performed by the company Modulo (Microsoft Partners Awards – Excellence in Security Management);
- Using a Specialized Risk Management Software
- Representative Assets;



Methodology – Security Assessment

◆ Detailed Security Assessment

- Types of Assets: Technology, People, environment, Processes;
- Vulnerability Assessment: using software internal knowledge base (Microsoft, Cisco, Physical Environments, ...);
- Compliance analysis for NBR ISO/IEC 27001, ISO/TR 13335 and ISO Guide 73;
- Deliverables
 - Risk Analysis Report;
 - Quantitative results;
 - Classified by: **Very High, High, Medium, Low, Very Low**;
 - Classified by Possible threats, perimeters, type of asset;
 - Operational Risk Report;
 - Asset analyzed, Justificative for threat, used knowledge base, mitigation solution.

C19

13335 - Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management

ISO GUIDE 73 Document Information: Risk Management - Vocabulary - Guidelines for Use in Standards

Chemtech, 8/17/2008

Norms and References

Methodology – Norms and References

◆ ISO27001

 ABNT – Associação Brasileira de Normas Técnicas <small>End.: Rio de Janeiro Av. Trecho de Vela, 13 / 2º andar CEP 20033-900 - Caixa Postal 1888 Rio de Janeiro - RJ Tel.: Fone (21) 2124-8122 Fax: (21) 2524-7902/2234-8433 E-mail: abnt@abnt.org.br www.abnt.org.br</small> <small>Copyright © 2005 ABNT – Associação Brasileira de Normas Técnicas Proibida a reprodução sem autorização Todos os direitos reservados</small>	DEZ 2005	Projeto 21:204.01-012
	Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos	
Projeto de Revisão de Norma		
Folha provisória – não será incluída na publicação como norma		

Apresentação

I) Este Projeto de Revisão de Norma:

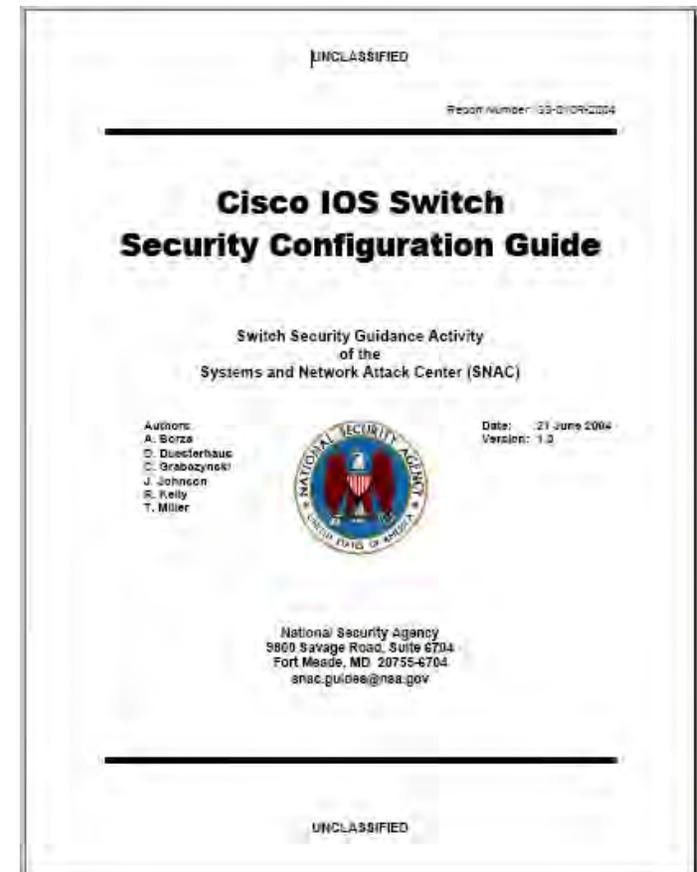
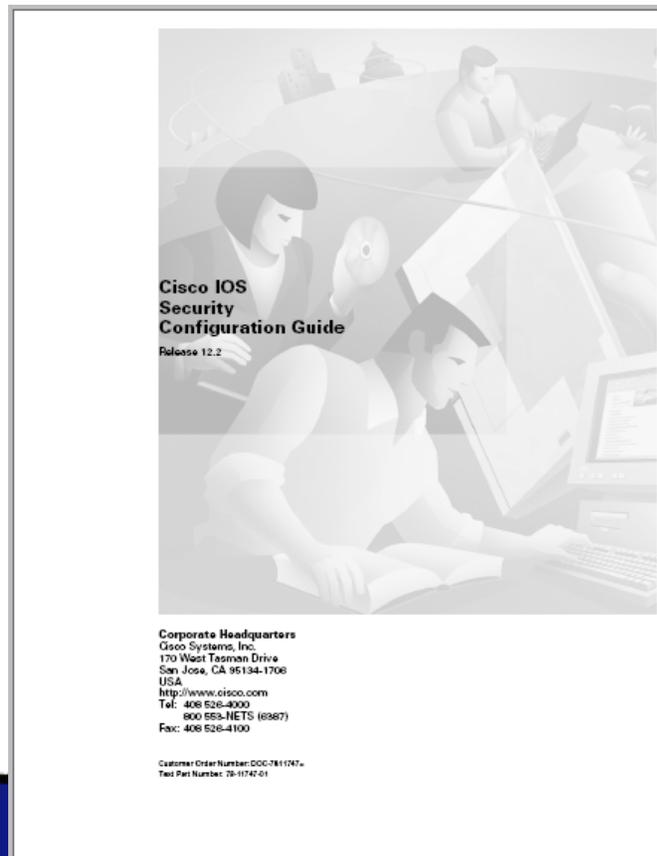
- 1) foi elaborado pela CE-21:204.01 – Comissão de Estudo de Segurança Física em Instalações de Informática do ABNT/CB21-Comitê Brasileiro de Computadores e Processamento de Dados;
- 2) é equivalente a ISO/IEC 27001:2005 e quando da sua homologação receberá a seguinte denominação: ABNT NBR ISO/IEC 27001;
- 3) recebe sugestões de forma e objeções de mérito, até a data estipulada no edital correspondente;
- 4) não tem valor normativo.

II) Tomaram parte na elaboração deste Projeto:

CGBI	Aristo Farias Jr
POLIEDRO	Larissa Prado
SERASA	André Novaes Frutuoso
	Denise C Menoncello
PWC	Andréa Thomé

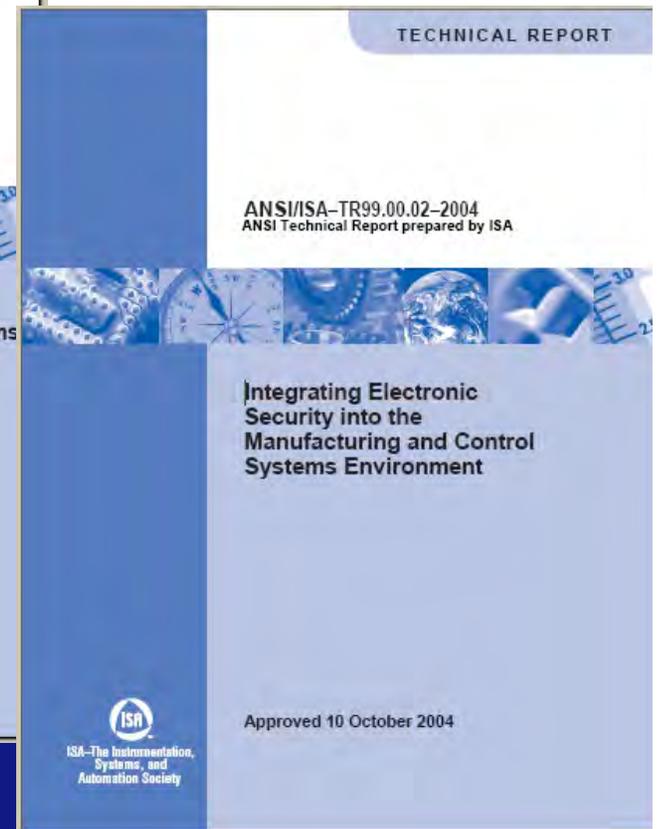
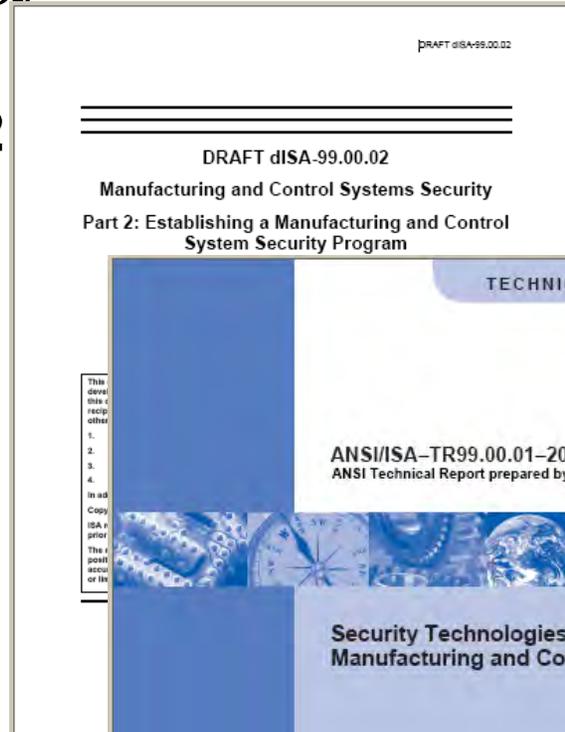
Methodology – Norms and References

- ◆ Manufacturers Security Guides
- ◆ NSA Security Guides



Methodology – Norms and References

- ◆ dISA-99.00.02
- ◆ TR99.00.01
- ◆ TR.99.00.02



Methodology – Norms and References

◆ ISA 99 Support and Recommendations

- General Recommendations
 - Cyber Security Policies and Procedures;
 - Inventory;
 - Detailed Security Assessment;
 - Training ...
- Specific Recommendations
 - What to do (antivirus, patches, firewall, network segmentation, ...)
 - How to do
 - Simple Network Diagrams;
 - Account Administration (e.g. process users accounts);
 - Remote Access Policy;
 - Access Policies (e.g. Restrict Internet and e-mail access – s99 Activity 16).

Methodology – Norms and References

ISA 99 Recommended Technologies and Practices Adopted	Reference
Network Segmentation to contain cyber security threats spreading	S99 7.14.4
Group the devices and systems and develop an inventory	S99 7.10.2
Develop Simple Network Diagrams	S99 7.10.2.1
Conduct a Detailed Security Assessment	S99 7.12
Recommendations how to Conduct the cyber security vulnerability assessment	S99 7.12.2
Develop Detailed M&CS Cyber Security Policies and Procedures	S99 7.13
Rules for Account Administration	S99 7.14.3.1
Rules for Authentication for Local Users	S99 7.14.3.2.1
Recommended Security Tools (antivirus, patch management)	S99 7.14.5
Restrictions on Internet and E-mail Access on Operator Stations	S99 6.16
Patch Management Rules and Recommendations	S99 7.19.1

Methodology – Norms and References

ISA TR99 Recommended Technologies Adopted	Reference
Dedicated Network Firewall Deployment and Recommendations	TR.99.001 6.1
Password Authentication Deployment and Recommendations	TR.99.001 5.2
Virtual Networks (VLAN) Deployment and Recommendations	TR.99.001 6.3
Virus and Malicious Code Detection Deployment and Recommendations	TR.99.001 8.2
Industrial Automation and Control Systems Computer Software (Windows systems Recommendations and Guidance)	TR.99.001 9.2

Challenges and Lessons Learned

Challenges and Lessons Learned

◆ Challenges

- The Schedule of the **production stops** (preventive repairing, etc.) is **instable** requiring strong Project Management monitoring;
- Applying new Security Controls requires **Cultural Changes**;
- A well structured and well understood **security policy** is necessary to warrant that the new technologies and practices **will not be forgotten**;

◆ Lessons Learned

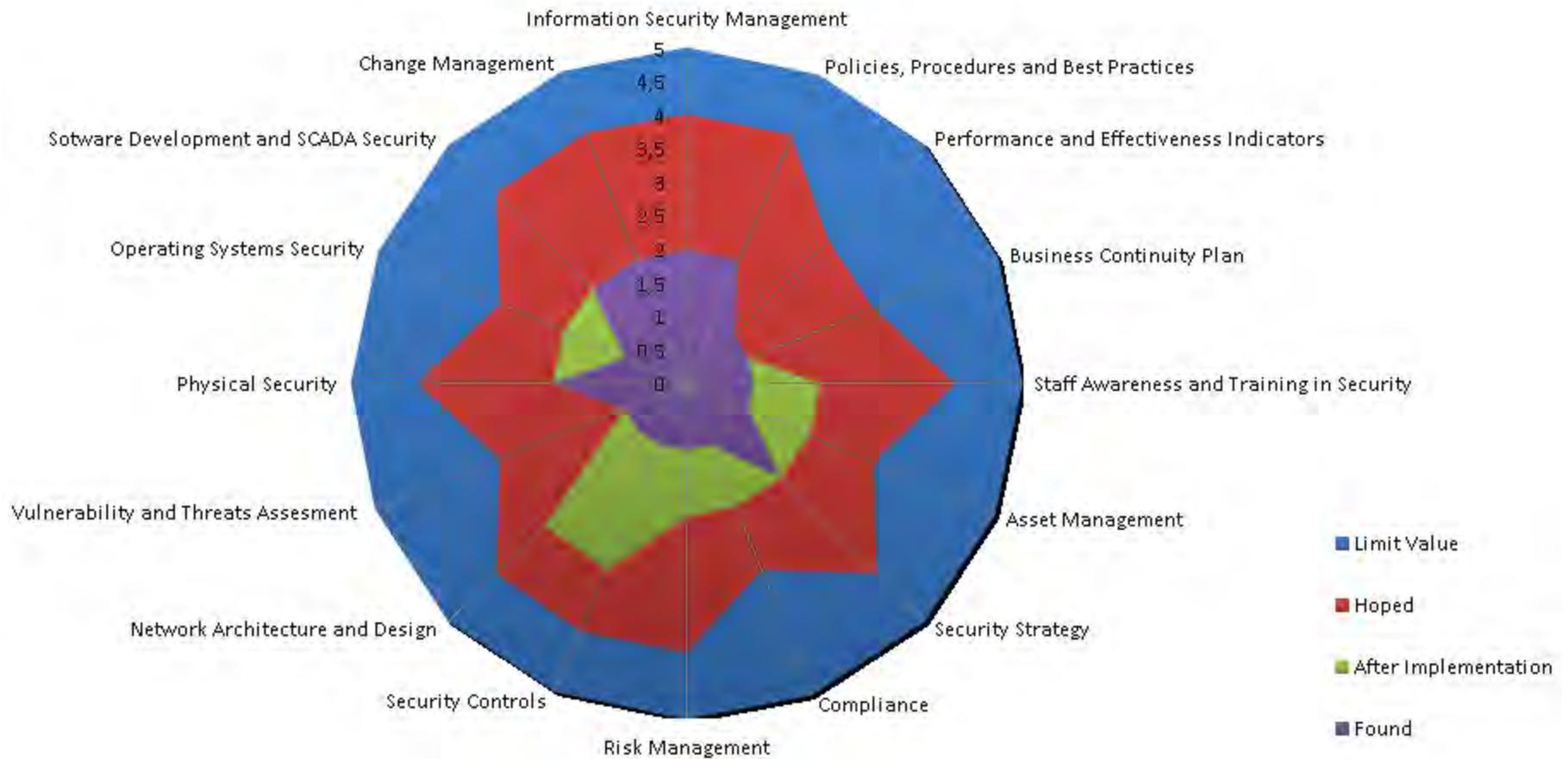
- **Automation Managers involvement** is very important to prevent mistakes and to warrant that new technologies and practices will be used correctly;
- Preparing **detailed plans** helps identifying mistakes;
- **ISA S99 and TR99** are good support tools for knowing what **features are not feasible** for automation environment;
- **ISA S99 and TR99** are good support tools for **cultural changes** (while adopting security new technologies);
- Microsoft **Security Templates must be strongly tested** in lab before migrations.

Results and Future Directions

Results

- ◆ **New Network Model:**
 - High Availability;
 - High Performance;
- ◆ **New Security Controls and Practices, including:**
 - Network Traffic Control with Firewall;
 - Operating Systems Security Improvements;
 - Malicious Code Detection;
 - New set of Policies and Practices to follow;
- ◆ **Well Known environment:**
 - Vulnerabilities and Risks;
 - Network Documentation;
 - Inventory;
- ◆ **No Production Stops.**

Results – GAP Analysis



Future Directions

◆ Improvement of Network Management Practices

- Improving availability management skills;

◆ Automation Security Policies Improvement

- Well defined Backup Policy;

◆ Risk Mitigation Projects

- As suggested by S99, continuing to mitigate;
- Following Operational Risk Report;

◆ Improvement of Authentication Model

- e.g. Digital Certificates (Smart Card);

Questions?

CHEMTECH – A Siemens Company

Leandro Pflieger de Aguiar

Computer Systems Analyst / Security Specialist

Phone: +55 (31) 3289-4437

Cel.: +55 (31) 9331-5803

leandro.aguiar@chemtech.com.br

