Security for IT Assets in Oil & Gas Industry

By

Hari Prasad Chitikala

R060104008

Guided By

Prof. B.G.Gupta

A Dissertation Report Submitted In Partial Fulfillment of the Requirements for Master of Technology (Petro-Informatics) Of University of Petroleum and Energy Studies, INDIA

College Of Engineering

University of Petroleum & Energy Studies, India

A1, Kailash Colony, New Delhi 110048

Acknowledgement

I take this opportunity to extend my sincere gratitude to my Guide Prof. B.G.Gupta for his constant guidance, critical appraisals, valuable suggestions, and supervision, which have made the completion of this dissertation possible well within stipulated timeframe.

I am pleased to extend my sincere gratitude to my friends for their enormous amount of support and encouragement.

UNIVERSITY OF PETROLEUM & ENERGY STUDIES

Certificate of Originality

This is to certify that the dissertation report on "**Security for IT Assets in Oil & Gas Industry**" submitted to the *University of Petroleum & Energy studies*, New Delhi by **Hari Prasad Chitikala** (Regd. No: R060104008) in partial fulfillment of the requirement for the award of the degree of **Masters of Technology (Petro Informatics)**, is a bonafide work carried out by him under my supervision and guidance.

Place: New Delhi

Date: 15/05/06

Prof.B.G.Gupta

Contents **Pg No**

1. Introduction:

A breach of information security within the Oil and Gas industry has the potential to bring down the entire power system for your city, state or country – regardless of whether the incident was the result of a malicious act, negligence, or simply an accident. For this reason, Oil and Gas organizations worldwide have been subjected to greater scrutiny of their information security practices. Governments are establishing tighter controls and want regular proof of Information security controls.

Traditionally, legacy and other energy industry applications have been stand alone systems accessible to a limited number of users mostly within the corporate itself. Like other industries, companies in the utility industry have fragmented security implementations across the organization with no integrated information security mechanisms, processes or systems in place to implement or manage information security. The task of ascertaining the level of security and the need for enhancement is therefore a difficult one.

Information Security Threats and Vulnerabilities:

Deregulation is breaking the industry into smaller independent units, driving the need for increased working. The new environment of de-regulation and increased competition means that companied need to open up their information systems for sharing of information with multiple parties as suppliers, vendors, customers etc. Examples include internet based billing presentment and payment systems, energy trading systems etc.

This will involve an integration of disparate application and infrastructure systems belonging to multiple organizations as well as providing online access top a large user based over the internet. Systems which were previously closed and in many cases, proprietary, now need to be inter-connected for information exchange. Many of these systems are now connected to the Internet making them vulnerable to cyber-attacks.

The traditional approach of building security mechanisms within the applications has resulted in multiple duplicated user and access data stores and poses a significant challenge for integration.

Information Security:

Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize Return on Investment & business opportunities.

It is the prevention of unauthorized Access, Destruction, Modification and Disclosure of information Assets.

2. IT Security Policy

This is to describe the IT Security Policies. The policies are aimed at providing reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as to assure availability, integrity, utility, authenticity and confidentiality of information applicable to all systems that generate, gather or store electronic data.

The following are the major components of the IT Security Policy:

- IT Assets Security Management Policy
- Asset Ownership, Identification and Classification Policy
- Asset Protection Policy
- Individual Use Policy
- Network Security Policy
- Disaster Recovery Policy
- Incident Reporting Policy
- Education, Training, and Awareness Policy
- Additional Instructions/Guidelines.

The three basic considerations while defining the policy elements are:

Appropriateness: to business needs, yet comprehensive in coverage

Justification: to the extent that it will reduce perceived risks to the level that business continuity is ensured and

Effectiveness: against actual threats

Definition of "IT Asset": IT Assets include all physical assets like computers, peripherals, network devices, communication devices, data media, and information assets like software, production data, e-mails, databases, any type of files stored in computers relevant to the Company's business and information displayed on computer screens.

3.0 Objectives

The primary objectives of the Information Security Policies are:

- To effectively manage the risk of security exposure or compromise within the systems under the scope of the IS Department
- To communicate all concerned, the responsibilities for the protection of information
- To establish a secure and stable processing environment
- To encourage understanding and compliance with all applicable laws and regulations
- To define a set of instructions and guidelines towards acceptable use of the IT Assets
- To protect the Company's reputation from actions in contrast to the code of conduct and ethics
- To protect the management and preserve its options in case of/during the event of an IT Asset misuse, loss or unauthorized disclosure

The relative importance of an objective depends on the nature of the asset. In majority of the cases, the emphasis will be on availability of the asset followed by integrity, and confidentiality.

4.0 Applicability

The policies, instructions and guidelines are applicable to all the categories of employees, anyone who is carrying out activities on behalf of the company, anyone who has been provided with access privileges to the network locally or remotely and any third party who is connecting to the network by virtue of any contract in force.

5.0 Policies in Detail

5.1 IT Assets Security Management Policy

5.1.1 Purpose and Objectives

The purpose of this policy is to define and clarify the policies, principles, standards, instructions, guidelines, and responsibilities related to the security of the Company's IT Assets.

IT Assets Security Management Policy is necessary to serve as a goal pertaining to the functions and operations related to the IS Department. These include:

- ensure continuity of information systems and services
- safeguard the safety and integrity of information assets
- prevent unauthorized access to the computer network
- ensure proper use of IT facilities
- assign responsibility for handling IT equipment and information assets

5.1.2 Policy Statement

The owners of IT Assets shall determine how critical and sensitive the asset is and correspondingly shall adopt appropriate security measures that offer a level of protection commensurate with the value and sensitivity of the assets. The security measures shall provide reasonable protection against unauthorized physical and logical access, disclosure, modification, or destruction, as well as assure the availability, integrity, utility, authenticity and confidentiality of information applicable to all systems that gather, generate and store data.

5.1.3 Explanation of Statement

IT Assets take many forms. It may be hardware of any kind, media or information stored in computers or transmitted across networks. Information technology systems are assets of vital importance to the Company. These assets are central to the business operation and may impact each one who relies on the Information Systems and Services.

The IT Assets Security Management Policy provides guidance for establishing effective security measures. The goal of this policy is to ensure the confidentiality of information systems, the continued availability of information systems to support critical activities, and the implementation of appropriate technologies.

Information security has the following main components:

- ***Confidentiality:*** Protecting sensitive information from unauthorized disclosure or interception
- ***Integrity:*** Safeguarding the accuracy and completeness of information and Processing methods
- ***Availability:*** Ensuring that information and services are available as and when required

5.1.4 Core Principles

• The IT Assets Security Management Policy provides guidance for establishing effective security measures.

• IT Assets are of immense value to the organization and need to be suitably protected.

• Information resources must be available when needed. Continuity of information resources supporting critical services must be ensured in the event of a disruption to business or a disaster, which makes critical systems unavailable.

• Information Services security must support the core functions of the organization. It should be an integral element of the management of the organization. It requires a comprehensive and integrated approach, which has to be periodically reassessed.

5.1.5 Policy Elements

IT Assets Security Management Policy includes the following elements:

• Identification and classification of assets for determining the appropriate level of security.

• Organizational responsibilities for implementing the security program, including security organization, security administration within the organization with authority over all aspects of security

• Security framework for identification and authentication, authorization and access control, accountability, integrity and availability, security of communication, and security administration

• Physical and environmental security

• Disaster recovery

• Incident reporting

• Compliance, including consequences of violations

• Training and education

• Security audits

5.1.6 Security Organization

Security organization creates an administrative infrastructure defining roles and responsibilities of various functionaries who are entrusted with the responsibility of implementing and monitoring various aspects of information security.

Security committee is headed by the Head of Administration Department. The Head of IS Department is a member of the committee. All aspects related to IT Assets Security are the responsibility of the Head of Department (IS).

5.2 Asset Ownership, Identification and Classification Policy

5.2.1 Purpose

The purpose of this policy is to distinctly identify an IT Asset and assign the ownership for subsequent classification and activities and to decide the level of security requirement.

5.2.2 Policy Statement

Each IT Asset shall have a designated owner within the Company.

Custodians of the physical assets shall identify and distinctively label all such assets and maintain an updated database. Owners/custodians of electronic data, which is a distinct and definable piece of information that is stored in electronic media, shall store and maintain a hierarchical structure in the respective storage areas.

IT Asset of any kind is classified as soon as its identification and appropriate security measures are adopted by the owner/custodian.

5.2.3 Policy Standards

Even if the ownership of a specific asset is identified with a function description, ownership does not occur automatically during staff rotation. When staff turnover occurs, ownership of the assets becomes the responsibility of the supervisor

of the designated information owner until such a time that ownership is delegated to the new/ another staff member.

IT Assets are classified by the owner/custodian based on the nature of the asset and its business value according to the following scheme:

• Restricted

Contains information whose unauthorized exposure or disclosure could have substantial negative impact on the business of the Company or causes it major public embarrassment.

Access and distribution is restricted to designated persons with an explicit need to have access to the asset.

The word RESTRICTED or a code of equivalent meaning to be displayed explicitly on the asset appropriately.

• Confidential

Contains information whose unauthorized exposure or disclosure could cause damage to an individual or would be prejudicial to the interests of the Company

Distribution is limited to employees who need to know it to perform their functions.

The word CONFIDENTIAL or a code of equivalent meaning to be displayed explicitly on the asset appropriately.

• Internal Use only

Contains information which itself, or in published form, has personal, technical or administrative sensitivity and is intended for internal use only, and should not be published or communicated externally except for official purposes.

• Public

Any asset that can be shared freely and unconditionally with anybody is classified as Public.

Any asset until its classification shall have default classification as "Restricted".

5.3 Asset Protection Policy

5.3.1 Purpose

The purpose of this policy is to set standards and guidelines for ensuring protection to the IT Assets of the Company from unauthorized access and thus ensuring safety and integrity.

5.3.2 Policy Statement

Asset Protection Policy aims at protecting IT Assets from unauthorized access by managing access to all entry and exit points, both logical and physical. Adequate perimeter security and logical security measures shall protect against unauthorized access to sensitive information of the Company. These measures shall ensure that only authorized users, as determined by the asset owner, have access to specific computer resources, networks, data, applications or any other IT Asset.

5.3.3 Policy Explanation

In this era of electronic collaboration, new technologies and greater automation are increasing opportunities for resources sharing. The Company shall seek a balance between the need to protect IT Assets and allowing greater access to equipment, data and applications. Multiple factors will affect how an asset owner chooses to control access to the asset. This includes some calculation of risk and consequences of unauthorized access vis-à-vis collaborative work and geographically distributed teams.

5.3.4 Physical Access Control

Control of physical access is the primary step for protecting of IT Assets. This is achieved by restricting entry to areas where equipment or media containing information is placed.

Control of physical access is under Administration Department's scope. However, access to the server room and UPS room is restricted to only a designated person as approved by Head of IS Department.

In any of the areas where IT Assets are stored, visitors and temporary staff are not left alone.

5.3.5 Logical Access Control

Logical access controls are protection mechanisms that limit users' access to information and restrict their privileges of access on the system to only what is appropriate for them. Logical access controls are often built into the operating system, or may be part of the "logic" of application programs or major utilities, such as Database Management Systems. They may also be implemented by add-on software packages that are installed upon an operating system. Additionally, logical access controls may be present in specialized components like network equipment that regulate communications between computers and networks.

Access to the operating systems of any computing device is restricted to only system administrators of IS Department and in exceptional cases to the supplier or maintenance contractor.

Security settings based on NTFS are applied to the file system of the computer. Security passwords are enabled in case of other devices depending on availability of such features.

Access to organizations WAN is strictly controlled and monitored.

5.3.6 Dial-up Access Control

Dial-up access to the network is provided through the network service provider, authenticated by organization. Policies and procedures as enforced shall be applicable to users.

5.3.7 Internet Access

Internet access is provided to the users strictly on need-basis. All equipment connected to the Internet is behind Firewalls. All users are guided by the relevant sections of "Individual Use Policy".

5.3.8 Access to/from other Entities

Network access to/from other entities is controlled by the managed equipment in the WAN as per organizations applicable policies. Access to Software resources is controlled by the defined Access Control List and file system security settings.

5.4 Individual Use Policy

5.4.1 Purpose and Objectives

The purpose of this policy is to define and clarify the principles, standards, procedures, guidelines, and responsibilities related to the security and proper usage of the Company's IT Assets.

The primary objectives are:

- To establish specific requirements for acceptable use of IT Assets
- To define the responsibilities of users in storage of production data and other soft information asset as per the disaster recovery policy
- To reduce exposure to security risks associated with use of internet and e-mail
- To reduce exposure to legal liability because of wrongful acts committed by employees using IT resources of the Company
- To protect the Company's and Group's reputation from actions in contrast to the code of conduct and business ethics

5.4.2 Policy Statement

The Company shall adopt policies governing the use of computer and communication facilities and other IT Assets by individuals. Like all communications conducted on behalf of the Company, users shall exercise ample judgment in Internet, e-mail and other use of computing and communication facilities. Use of the Internet, email, and other actions shall always be able to withstand scrutiny by the authorized personnel of the Company or any external agency without losses, legal liability or embarrassment to the individual or the Company.

5.4.3 Policy Explanation

Information System & Services has become a mission critical function for the Company. As such, it must be operational 24x7x365. In order to achieve this it must be operated in a secure and managed environment. It is also important to ensure that all the computers are running legal software. Careless use of e-mail and the Internet can subject other users to security problems such as viruses and denial of IT Services.

5.4.4 Policy Standards

Companies have a set of instructions/ guidelines regarding acceptable use of e-mail, Internet, and other IT Assets.

A message will be displayed on the screen at the first login by a user to the effect that the user would agree to read and abide by the IT Security Policies of the Company.

5.5 Network Security Policy

5.5.1 Purpose and Objectives

A policy on network security is intended to support IT security by reducing exposure to security threats when providing access to external computer networks,

allowing connections to the Internet, using the Internet or an Intranet to receive or deliver information or services.

The primary objectives of the Network Security Policy are:

- To protect the integrity of the Company networks from unauthorized access and fraudulent use and /or abuse
- To communicate responsibilities implementing the network security policy
- To reduce exposure to security risks identified with remote access, Internet use, and Wide Area Networks
- To monitor network use

5.5.2 Policy Statement

The Company shall manage networks in a manner that ensures their proper use, prevent unauthorized access or use, maintain availability and protect the security and integrity of IT Assets. The Controls shall also reflect the security needs of other entities connected to the network.

Internet and Intranet sites shall be protected so that an unauthorized individual cannot alter data and information or compromise the integrity. Classified information on these sites shall be further protected by user-IDs and passwords or other effective mechanism so that access by unauthorized individuals is not allowed.

5.5.3 Policy Explanation

Networks allow sharing of equipment, information, applications, and other computer resources. Dependence on networks requires availability 24x7x365. Integrity and confidentiality are paramount in a shared environment. Networks also represent major points of vulnerability to a large range of security problems. Remote access, connections between networks and Internet access by workstations make the network security a complex problem.

Internet, Intranet or Extranet connections pose a risk of unauthorized access to the Company's data by compromising the integrity and privacy of data. Potential consequences of unauthorized access include altering, erasing, or otherwise rendering the information invalid or unavailable by manipulating the data or the underlying programs.

TCP/IP has become the universal communications protocol for all computer systems. This exposes any connected computer to potential malicious attacks from anonymous persons located anywhere in the world. Sufficient and effective security controls are essential to provide access to those who have the need and privilege and keep out those who do not.

5.5.4 Policy Standards

Network resources participating in providing access to sensitive information or critical systems shall assume the security level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk. All network components must be identifiable and restricted to their intended use.

Specific standards and guidelines include:

- ✓ Password protected screen savers, terminal lock and key or terminal software locking options should be enabled on each terminal so that access can be controlled by locking the terminal while it is unattended
- ✓ All network nodes should be located in secured areas
- ✓ Switches, hubs and other important network devices must be protected from unauthorized physical access
- ✓ Procedures should be implemented which ensure that access to data or information is not dependent on any individual. There should be more than one person with authorized access
- ✓ The network manager must periodically monitor sharing and trust relationships for connecting with other networks to ensure they are still valid
- ✓ An audit of network security must be conducted periodically

Perimeter security protects a network by controlling access to all entry and exit points. It must be managed as a mission critical infrastructure. Specific standards concerning the Internet gateway include:

- The Company shall manage the security for all points of entry to and from the Local Area Network Appropriate access controls such as identification, authentication, certification, and authorization shall be implemented to control entry to the network
- Security for a connected network should reflect the security requirements of the highest risk elements on the network
- Remote access shall be provided to a user based on specific requirement and for a specified period
- Management approval is required for providing remote access
- The workstations should not be configured for automatic login by storing the password in the computer

5.6 Disaster Recovery Policy

5.6.1 Purpose and Objectives

The purpose of this Disaster Recovery Policy is to define and clarify principles, standards, procedures, guidelines, and responsibilities related to the safety and security of the IT Assets, especially information assets of the Company against disaster of any kind.

The primary objectives of the policy are:

• To reduce the risk of disruption of operations or loss of information

• To communicate responsibilities for the protection of information and continuity of business operations

• To establish a plan for restoration of information and operations following a disaster

5.6.2 Policy Statement

The essence of disaster recovery is business resumption. A company shall have a disaster recovery plan that identifies and minimizes risks to critical systems and information in the event of a disaster. The plan shall provide for contingencies to restore information assets after a disaster occurs.

5.6.3 Policy Explanation

Business Continuity Planning is one of the most important functions of any organization. Traditionally, disaster recovery is the responsibility of the Information Systems Department. It focuses primarily on assuring data integrity and applies strategies for recovering information assets from disasters that affect business processes.

5.6.4 Policy Elements

Disaster recovery plans must include the following elements:

- Identification of critical assets
- Mitigation strategies and safeguards to avoid disasters. Safeguards
- Data backup strategy
- Business resumption plan
- Contingency plans for different types of disruption to information systems
- Organizational responsibilities for implementing the disaster recovery plan
- Procedures for reporting incidents and implementing the disaster recovery plan

5.6.5 Policy Standards

- ***Data Backup Strategy:*** The primary responsibility of safety and security of data lies with its owner. All users shall follow the Company's procedures and guidelines for backing up of data for ensuring business continuity.

- ***Power Backup System:*** IS implementing multilevel power backup system for IT Assets. However, responsibility of ensuring mains supply from the public services agency is with the Administration Department.

• ***Physical Security of Servers:*** Server room is locked and keys are controlled by IS Department. In addition, electronic access control system is installed with access to limited persons.

• ***Responsibilities:*** Head of IS Department shall be responsible for implementing the disaster recovery plan.

• ***Reporting:*** Any disaster should be informed to the Head of IS immediately.

5.7 Incident Reporting Policy

5.7.1 Purpose and Objectives

The policy on security breaches and incident reporting is intended to support IT security by documenting security violations and taking actions to discourage or apprehend those who are responsible. The ultimate goal of this policy is the protection of IT Assets, containment of damage, and restoration of services. Secondary goals are dependent on the category of violation.

The primary objectives of the Incident Reporting Policy are:

• To document security violations and incidents

• To share information on security problems with other responsible people in the Company or authorized state agencies

• To fix any loop holes in the security procedures

5.7.2 Policy Statement

The company shall prepare procedures for monitoring, investigating and reporting security breaches and incidents. Security breaches shall be investigated promptly and documented. If criminal action is suspected, the Company shall contact the appropriate law enforcement and investigative authorities as quickly as possible.

5.7.3 Policy Explanation

Collective and timely action is required to counteract security violations and activities that lead to security breaches. All concerned must know the extent of security problems. Quick reporting of some incidents, such as new viruses, is essential to stop them from spreading and affecting other systems.

5.7.4 Policy Standards

- All users of information technology resources must receive education on security issues, obligations, procedures, and consequences of violations
- Reporting and documenting security incidents to the appropriate level of management
- Implementing procedures for documenting or logging information on intrusion attempts and storing that information in a manner for later analysis or use by law enforcement agencies
- For catastrophic disasters such as fire, floods or destructive storms, the goals of employee safety and damage containment apply. Notification procedures will include the appropriate public service departments (Fire, Police etc.)
- Any disaster should be reported to head of IS Department immediately
- For physical intrusion of secured areas, the goals of employee safety, intruder identification, and if warranted, the intruder's removal from the premises apply. Notification procedures will include building security or local police.
- For cases involving deception and fraud, the goal of identifying the perpetrator applies

5.8 Education, Training, and Awareness Policy

5.8.1 Purpose and Objectives

The primary objectives of the Education, Training and Awareness Policy are:

- To communicate responsibilities of IT Assets security policies and procedures

- To provide adequate skills for IS staff responsible for implementing security procedures
- To establish specific requirements for achieving the goals
- To communicate the consequences of violations of security procedures

5.8.2 Policy Statement

The IT Security Policies and Procedures of the Company will be communicated to all those who are covered under "Applicability". These will also be available for a limited number of reviewers who are in position to influence the security policies. A mechanism to maintain effective awareness of IT Assets Security Policy, standards and acceptable use will be in place. Persons responsible for information technology resources shall have adequate training on implementing proper security controls for the IT Assets under their control.

5.8.3 Policy Explanation

Established security policies and standards must be followed to achieve the intended level of IT security, control and integrity. Security policies and standards are ineffective if individuals at any level of the organization are unaware of the importance of them, do not understand established standards or fail to perform required practices for any reason. Failure to follow policy or procedures for any reason negates the very purpose of protective intent for which the security policy and procedures exist. Information Security is not a one-time event. To have maximum effectiveness security standards must be known, understood, believed, and appropriately and consistently practiced.

5.8.4 Policy Standards

⇒ All users must be informed of security policies and procedures and their responsibilities in writing. This should include knowledge of the consequences of violations of security procedures.

⇒ All users must be informed that any actions taken under their assigned identification (e.g., user-id) are their responsibility

⇒ Persons responsible for information technology resources must be aware of the information security policies and must be knowledgeable about effective security practices for the technical environment under their control

⇒ Head of IS Department will develop and disseminate procedures, guidelines and illustrations for users to assist them in maintaining good security practices

6.0 Additional Instructions/Guidelines

Additional Procedures and Guidelines are

A. Acceptable Use of IT Assets
B. IDs and Passwords
C. Email
D. Internet Access
E. Antivirus
F. Software Authorization

A. Acceptable use of IT Assets

All IT resources are assigned exclusively for Company purposes and as per the job requirements. No user shall use any IT Asset for any other, including recreational purposes.

Users shall not tamper with hardware or software configurations. Users shall not install any software legal or otherwise in their computer on their own.

Individuals shall not monopolize system resources. Shared devices should not be engaged beyond reasonable duration. Users may request IS for exclusive use of a resource in exceptional cases.

Any type of offensive or inappropriate material (programs, files, data, images etc.) that could be considered in contrast with the rules of the codes of conduct and ethics must not be stored in the Company's storage areas.

Users should not make unauthorized changes to the contents of any workstation, delete or modify data in an unauthorized manner.

Each user is responsible for ensuring that the hardware assigned to him/her is in a secure state when left unattended by taking one or more of the following guidelines as applicable:

- Do not leave confidential company information displayed on the screen
- Store media containing data in a safe place
- Lock workstation after saving open files wherever possible
- Close all open files and log off if workstation is not lockable
- Use password protected screen saver with activation after a maximum of 5 minutes of inactivity
- keep the equipment in lock and key where feasible
- Laptop computers must always be carried as hand baggage while traveling by air

Workstation must be switched off at close of work, unless used for tasks that run overnight.

Loss, theft or damage to hardware must be immediately reported to the IS department. Relocation of any hardware must be authorized by IS Department.

B. IDs and Passwords

All users shall have a unique user ID and password not less than 6 characters long for logging on to the computer network.

It is the responsibility of the concerned user to keep the secrecy of the password. In case the password is disclosed, the user must change it immediately.

The initial password assigned by IS must be changed on first login.

Obtaining, possessing, using or attempting to use someone else's password shall warrant disciplinary action regardless of how the password was obtained.

The password should be constructed in such a manner that is not easily guessable.

Some characteristics of a weak password are:

• Names of family members, friends, co-workers, pets, movie or cartoon characters, etc.

• Birthdays and other personal information such as initials, addresses and phone numbers, registration number of vehicles etc.

• Word or number patterns like aaabbb, qwerty, zyxwvuts, abcd1234, 123321, etc.

Characteristics of a strong password are:

• contains both upper and lower case characters in random sequence

• have digits and punctuation characters e.g., 0-9, !@#$%^&*()_+|~ \` {}[]:";'<>?,./)

• is at least six alphanumeric characters long

• is not a word in any language, slang, dialect, jargon, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered by you. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "My Cat's Friend is a Dog Named Tom Aged 2 Yrs" and the password could be: "McFisDnT-9" or a variation.

User passwords must be changed at regular intervals but not later than 90 days. Administrator level passwords must be changed in every 30 days.

Password Protection Standards

Do not use the same password for accounts as for other access (e.g., personal ISP account). Wherever possible, use passwords for various Company access needs.

For example, select one password for the Windows login and separate passwords for Intranet and Lotus Notes.

Do not share Company passwords with anyone, including assistants or secretaries.

Don't:

- reveal a password over the telephone/email to ANYONE
- reveal a password even to the supervisor
- talk about a password
- Hint at the format of a password (e.g., "my family name")
- reveal a password on questionnaires or forms
- reveal a password to colleagues while on vacation
- use the "Remember Password" feature of applications (e.g., Internet Explorer)
- write down passwords and store them anywhere in the office
- Store passwords in a file on ANY computer system

If someone demands a password for any reason, refer them to this document or have them call IS Department.

If a user account or password is suspected to have been compromised, report the incident to IS Department.

Software Development Standards

Software developers must ensure their programs contain the following security precautions:

- Support authentication of individual users, not groups
- Not store passwords in plain text or in any easily decryptable form
- Provide for role management, such that one user can take over the functions of another without having to know the other's password

C. E-mail

The purpose of these guidelines is to ensure the proper use of companies email system and make the users aware of what the Company deems to be acceptable and unacceptable use of its email system. These guidelines do not grant the users any contractual rights to use the email system.

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply as far as accountability is concerned. Therefore, it is important that users are aware of the inherent risks of email:

- If you send emails with any defamatory, offensive, racist or obscene remarks, YOU and the Company can be held liable
- Any email forwarded by you will be treated as an email sent by you
- If you unlawfully forward confidential or sensitive information, you and the Company can be held liable

By following the guidelines in this policy, the user can minimize the legal risks involved in the use of email. If any user disregards the guidelines, the user will be fully liable and the Company will disassociate itself from the user as far as legally possible.

Best Practices / email etiquette

Employees are strictly forbidden from using email accounts other than those provided by the Company for official purposes without prior approval from the Head of concerned Cluster. Any such account has to be in the IS records.

Users should take extreme care in drafting an email as they would for any other communication. Company demands users to adhere to the following guidelines:

- do not end unsolicited email messages
- do not forge or attempt to forge email messages
- do not disguise or attempt to disguise identity when sending mail
- do not send email messages using another person's email account

Writing emails:

- Be concise and to the point. Write well-structured emails and use short, descriptive subjects.
- Send a different message for each topic of discussion.
- Do not write emails in upper case. It's hard to read. More over this can be highly annoying and might trigger an unwanted response from the recipient.
- Only stamp emails as important if they are really important.
- Do not send unnecessary attachments. Compress attachments larger than 500K before sending them. Please respect the receiver's resource constraints and comfort also for receiving your mail.
- Keep the number of recipients as low as practical. E-mails with a long list of recipients in the To: or Cc: fields may not be seen as urgent as e-mails directly addressed to an individual.
- Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware what action, if any, to take. It is advisable to write what the cc: recipient is expected to do at the bottom of the mail. If not specified the cc: bcc: mail may be treated as "For Information only".
- While forwarding mails, state clearly what action the recipient is expected to take.
- Be careful with formatting. Remember that when you use formatting in your emails, the sender might not be able to view them, or might see different fonts and colours than you had intended. As far as possible, use plain text for the body of an e-mail as it can be read by all e-mail client software.
- A corporate disclaimer will be added automatically underneath the signature for all e-mail addressed outside domain.

Replying to emails:

As far as possible, emails should be answered on the same day of receipt. If a detailed reply would take time, one must acknowledge the email saying that the mail has been received and that it will be replied later.

Priority emails like emails from customers and business partners should be replied as quickly as possible.

Do not overuse "Reply to All". Only use "Reply to All" if you really need your message to be seen by each person who received the original message.

Don't reply to spam. By replying to spam or by unsubscribing, it is confirmed that the email address "exist'. Confirming this will only generate even more spam. Therefore, just delete the mail.

News groups:

Users need to request permission from their supervisor before subscribing to a newsletter or news group, even if it is for official purposes.

Maintenance:

Delete any email messages that need not be preserved. Archive the mails and compact the mailbox periodically to keep the mailbox healthy.

Personal Use

Companies email system is meant for business use. But the Company allows short and incidental use of its email system for personal purposes without contradicting the provisions in others parts of this document. Use of personal emails should not interfere with the work.

However, spamming, sending of chain letters, junk mails, jokes and executables is prohibited. Do not give out your official e-mail address to any website

or anybody unless you are confident that it would not be used for spamming or sending unsolicited mails.

All messages distributed via the company's email system are Company's property.

System Monitoring

The Company can monitor emails without prior notification. If there is evidence that users are not adhering to the guidelines the Company reserves the right to take appropriate action against the concerned.

D. Internet Access

Internet connections are given to employees only on the basis of a specific requirement and for official business purposes for a specific period. The requirement will be reviewed periodically.

It is strictly prohibited to use Internet for:

- Any purpose violating the Laws of the Land
- Accessing sites that contain defamatory, offensive, insulting, racist or obscene material
- Unlawful or unethical conduct
- Instant messaging for purposes other than official or with contacts other than official
- Deliberately propagating any virus, worm, Trojan horse, or trap-door program code

System Monitoring:

The Company can monitor the usage of Internet connections without prior notification for the purpose of enforcement of guidelines. If there is evidence that users are not adhering to the guidelines the Company reserves the right to take appropriate action against the concerned

E. Antivirus

Antivirus activities are centrally managed by IS Department. Suitable antivirus software is installed in all computers and servers.

Virus definitions are updated on critical servers automatically from the Antivirus Vendor's website. In addition a distribution copy is downloaded and distributed automatically to client computers at user logon. (An appropriate updation and distribution method is decided based on the specific antivirus product in use.)

Following are some guidelines to be adhered to:

•Do not uninstall the software or disable the auto protect shield

• keep a watch on the status of antivirus software and updation status of the computer

• do not open any file attached to an email from an unknown, suspicious or untrustworthy source

• Do not open files attached to an email if the subject line is questionable or unexpected

• Do not open files with a double file extension, (e.g. document.txt.vbs). Under normal circumstances one should never need to receive or use these

• If in doubt, always ask for advice, do not open the file or email

• Inform the IS Department of any abnormal system behavior suspected of being virus related

Notebook users, after using it on a network outside organization or Internet, shall run a full system scan if a new antivirus patch is released after the last update. The antivirus distribution tool displays a message on the screen while a new patch is being installed.

Be aware that an infected computer in the LAN can infect any computer connected to the Network anywhere in the world!

F. Software Authorization

It is forbidden to use software disregarding the terms specified in the end user license and standards. Users are not allowed to download or/and use software from Internet in violation of license agreements.

No user shall install any software in any of the Company's computer even if the user owns necessary licenses for the same. In case users require to install such software, freeware or shareware, they must bring the software and license agreement, if applicable, to the IS Department for necessary action.

Users must not permit others to copy software for which the Company possesses the license. Users shall not intentionally develop programs that harass other users or infiltrate a computing system and/or damage or alter the software components of a computer or computing system.

7. Backing up, Archival and Retrieval of Production Data

Preamble

The term "Production Data" covers all "electronic files" generated in-house, received from clients, vendors or through any other source as part of a project, as required for carrying out an official work or as reference material.

The various aspects of safety and security of our production data and guidelines for ensuring business continuity. Names of servers mentioned in this document may change or new servers may get added.

Strategy

The strategy for data safety is formulated to enable:

- IS to take ownership of the production data after it is stored as per the guidelines
- Storage of production data in a well-organized and pre-defined manner at a central place so that complete data pertaining to a project or a cluster/department /section is available at a single location and is traceable

- Access to production data is independent of the availability of the owner
- reconstructing the storage server to the status of one day prior to a possible disc crash
- Making the generation files of project data available for a specific period of time (at present 1 year)
- Provide limited additional backup space with private access only to the concerned user, or any data stored in a user computer, in addition to the general space provided for storage of production data
- Archiving the data pertaining to completed projects
- Providing a mechanism for retrieval of backed-up/archived data

Local Storage

As a convention, working files are stored in the local hard disk of user computers under "*Driveletter*\users*username*" (eg. C:\users\alt) while the central storage is in the storage server as described in detail below.

Storage Servers

The storage server stores the complete production data and is available online to the user. Name of our main storage server is "STRGSRVR". All storages except "Transit" are here. "NTMAC" is being used for "Transit" shares as described elsewhere in this document.

The storage server has the following three major partitions:

a) Home

All users are given independent personal shares, namely \\STRGSRVR*userid.* For example, user abc's personal share is \\STRGSRVR\abc. Each personal share has 100MB of storage space. Only the concerned user (and administrator) can access files in the personal share.

These folders should ideally contain backup of selected data stored in the local computer of the user. However, backup of all production data should be available in

"Projects" or "Clusters" as described in other paragraphs. Personal folders are created along with creation of user's windows account when a new employee joins. This is deleted on separation of the concerned user after his/her last working day in the Company.

b) Projects

This location contains separate subfolders for each project. The folder name shall be based on organizations project number. Project folders can have a structure suitable to the project organization in terms of disciplines/working groups and applicable security system. The project folder is created on request of the project manager. NTFS security system will be applied to the complete folder, giving necessary permissions to the project manger or his representative. Management of the project folder is the responsibility of the project manager.

These folders are expected to contain all project related files, finished and unfinished. No other file should be kept in project folders. In case some team members are not given access to the project folder, the project manager must make arrangements to ensure that files from such users also reach the project folder every day, may be through an intermediate person. In any case such users can keep backup of their files in their personal share. There shall be no directory on individual names in the project folder.

c) Clusters

Each cluster will have a separate folder, in which department folders will reside. Reference materials etc, which do not pertain to a specific project, but used frequently, can be stored in these folders. A nominee of the HOD or HOS will be given necessary permissions for the folder who shall be responsible for managing the access rights. The concerned department/section, as per the requirement, shall decide the structure of the subfolders. There shall be no directory in the name of an individual. These folders will also have NTFS security system.

d) Public

This folder will contain information relevant to all employees like, Backup log, templates, reference materials like telephone directory (Public telephones), yellow pages etc. This is accessible as \\strgsrvr\public. The users will have only "Read" permission. Any material to be made available through Public share has to be routed through IS.

e) Backup

This partition is in STRGSRVR, but not accessible to common users. This is to store daily backup of Notes databases, PDS data etc as described under "Special Backups".

f) Transit

"Transit" is available on NTMAC. The share name is \\ntmac\transit. This folder, as its name suggests can be used to transfer data between two computers if they cannot be connected to each other due to security reasons. This can also be used for making data available to multiple users. Maximum retention time or latency of files in transit will be 15 days. Read, Write and Delete permissions are given to all users in the transit folders. The users should not delete files stored by others. Ideally, files to be deleted by the users after the intended use.

Backup Procedure

User's Responsibility:

Primary responsibility of the safety of the production data is with the owner of the data. The user should ideally work in his/her local machine only, checking the necessary file out from the storage server. The user is responsible for taking backup of his/her day's work at close of work to the appropriate location in the storage server. The files have to go to either "Projects" or "Clusters", as mentioned in detail above.

Project Manager's / HOD/HOS's Responsibility:

Ensure that the team members take backup of their data systematically. They are also responsible for managing data and access rights in the backup areas.

IS Responsibility

IS oversees the folder structures, contents and security settings of the folders. The "Daily Backup Server" takes a daily incremental backup of the production data from the Storage Server automatically. This is not directly accessible to users. Off-line backup of the Daily Backup Server is taken in duplicate on a monthly basis to tapes/ other suitable media. The second copy of the backup will be stored in a place other than the office. This is stored for a period of 1 year. The logs will be available in Public Folders. Full off-line backup of the File Server is taken in duplicate on a monthly basis. The second copy of the media will be stored in a place other than the office. The logs will be available in Public Folders. This backup will be available for 1 year. Data pertaining to closed projects are archived in duplicate in two different media and stored eternally. The second copy of the media will be stored in a place other than the office. The logs will be available in Public Folders. Media of archival set are checked for retrieval every year, and changed, if required. All media will have a unique ID as per a standard labeling scheme described separately.

Special Backups

1. Lotus Notes Databases

Daily full backup of notes databases are taken automatically to \\strgsrvr\backup. This will be available for 7 days (subject to availability of space). In addition, databases of completed projects are archived along with the rest of the project data.

2. Intranet/SQL Databases

Daily incremental backup of Intranet and all services under Intranet and full backup of SQL databases related to intranet are taken automatically to DAILYSRVR. This will be treated like the daily back up of Projects/ Clusters data.

Full backup of other SQL databases are taken automatically on STRGSRVR, which will be available for 7 days. In addition, databases of completed projects are archived along with the rest of the project data.

3. PDS Data

Daily full backup of project data from PDS servers are taken automatically to \\strgsrvr\backup. This will be available for 7 days (subject to availability of space). Monthly full backups are taken and stored for one year. In addition, data of completed projects are archived along with the rest of the project data.

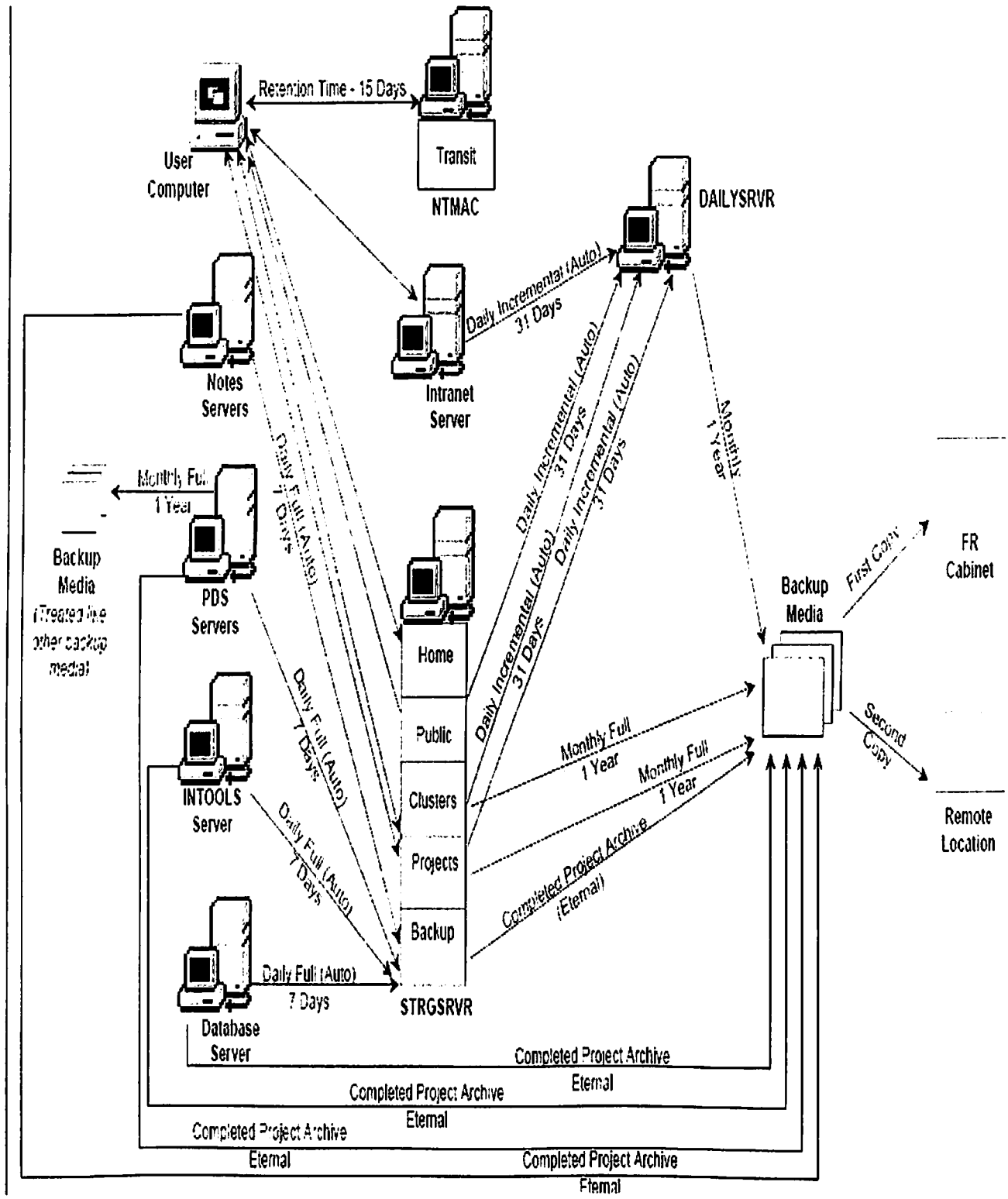
4. Intools Data

Daily full backup of project data from Intools server are taken automatically to \\strgsrvr\backup. This will be available for 7 days (subject to availability of space). In addition, data of completed projects are archived along with the rest of the project data.

Retrieval Procedure

In case any data has to be retrieved from the backup set, the user has to approach IS with the unique ID of the media, and the file details. The required files will be retrieved to an appropriate location.

"Archival" refers to copying the data files pertaining to closed projects to multiple sets of media, which will be available only offline. In this case the files are removed from the server after archival. A graphical depiction of the data flow is attached as Exhibit-1


Retention Time - 15 Days
Transit
NTMAC
User Computer
DAILYSRVR
Daily Incremental (Auto) 31 Days
Notes Servers
Intranet Server
Monthly 1 Year
Daily Full (Auto) 7 Days
Daily Incremental (Auto) 31 Days
Monthly Full 1 Year
Backup Media
PDS Servers
Home
Public
Clusters
Projects
Backup
Backup Media
First Copy
FR Cabinet
Second Copy
Remote Location
INTOOLS Server
Monthly Full 1 Year
Completed Project Archive (Eternal)
Daily Full (Auto) 7 Days
Database Server
STRGSRVR
Completed Project Archive Eternal

8. BS 7799

8.1. About the Standard BS 7799

British Standard BS 7799 represents an internationally recognized basis for the evaluation of IT security management practices.
The standard BS 7799 contains a comprehensive set of best practices for IT security management and consists of two parts:

- The first part BS 7799-1 "Information security management. Code of practice for information security management" forms the reference model for an Information Security Management System (ISMS). The standard contains guidance for establishing an Information Security Management System (ISMS). BS 7799 has meanwhile reached the Status of an ISO-Standard and has been published as ISO/IEC 17799 (identical with BS 7799-1).

- The second part BS 7799-2 "Information security management. Specification with guidance for use" contains the requirements for effective application and documentation of an Information Security Management System (ISMS). BS 7799-2 is the basis for our assessment and certification.

8.2. Content of BS 7799

BS 7799 covers the following topics:

- Security Policy
- Organizational Security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control

- Systems development and maintenance
- Business continuity management
- Compliance (legal aspects, internal procedures, compliance with the standard itself)

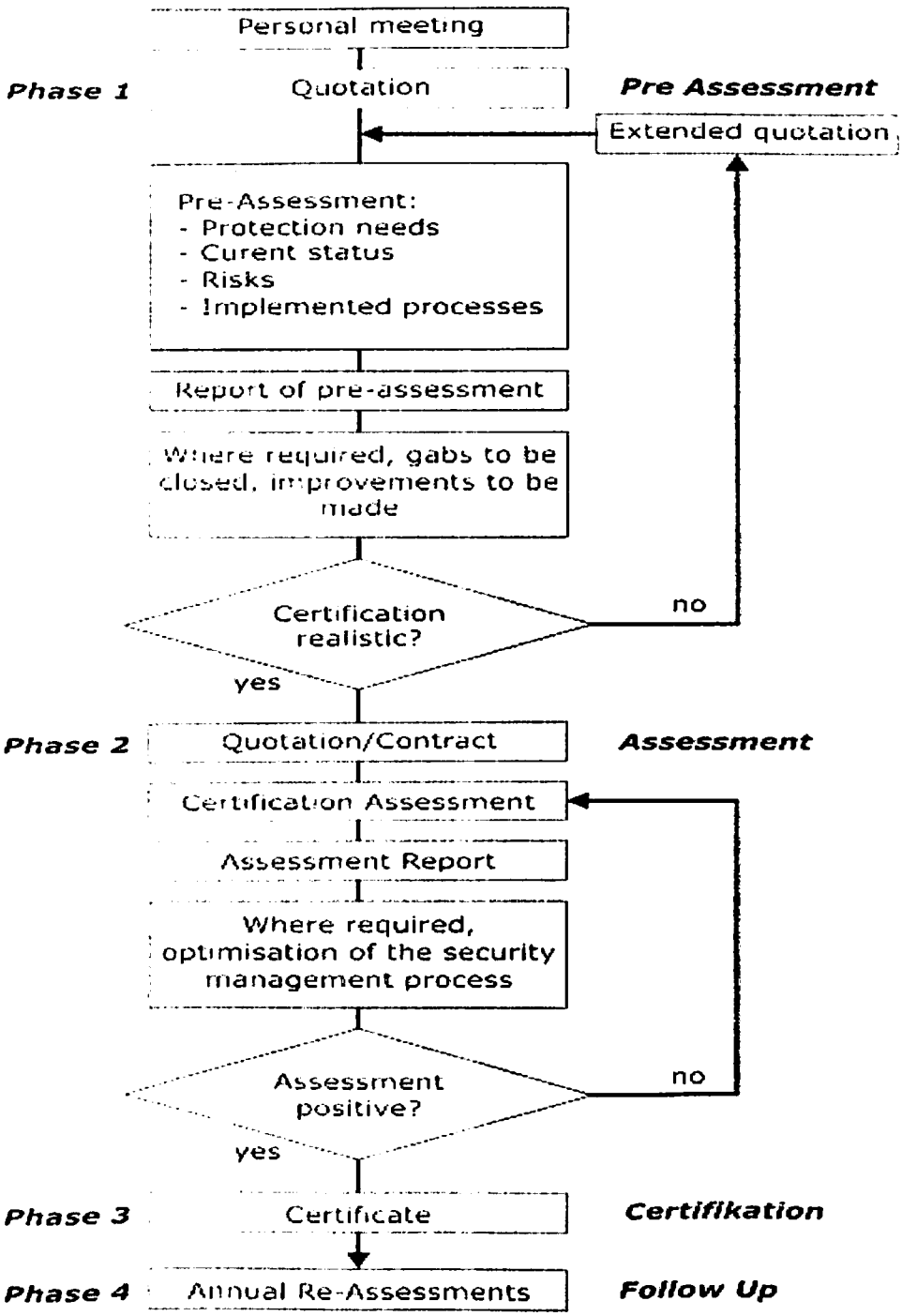
8.3. Advantages of a BS 7799 Certification

The application of BS 7799 enables your organization to establish a security management process, which maintains a defined security level in a systematic and controlled manner. Such a controlled and certified security management process leads to the following advantages:

- Effective security management system
- Market advantage through certificate issued by independent experts
- Cost reduction through transparent and optimized structures
- Security management is integrated in the business processes
- Measurement and control of IT related risks
- Documentation of security relevant structures and processes
- Staff with enhanced security consciousness
- Evaluated organizational processes with regards to IT security aspects
- Effective Business Continuity Management
- World wide accepted IT security system
- Likelihood of reduced costs for security related insurances
- Security-specific compliance with ITIL (Standard for IT Service Management)
- Integratability with ISO 9001:2001

8.4. The steps to BS 7799 certification

The following diagram illustrates our certification procedure.



The following steps lead you to a BS 7799 certification

Initial analysis:

The first step is a discussion with one of our experts in order to determine the adequate scope for the certification (size and business purpose of your organization and certification-relevant areas) in order to produce a differentiated quotation for you.

Phase 1: Pre-Assessment

As part of a pre-assessment, first identify deficiencies and open issues within your existing IT security management process, which need to be identified and covered before a certification assessment can sensibly take place. The pre-assessment is not compulsory, however it is highly recommended in order to ensure an efficient certification process.

Phase 2: Certification Assessment

Once all deficiencies and open issues have been covered by your organization, our certification assessment will take place. As part of an intensive onsite-assessment by two of our experienced IT security assessors, analyze all relevant areas within your organization. The goal of the certification assessment is to prove, that you have successfully implemented the IT security management as specified in BS 7799. The outcome of the assessment is a detailed assessment reports which details our findings. As far as deficiencies are identified, they need to be removed before the certification takes place.

Phase 3: Certification

A soon as the assessment report is being issued and the assessment results are positive, this assessment report is being forwarded to the certification body and approved. The certificate will be processed and sent to you.

Phase 4: Follow Up Process

Annual re-assessments of IT security management will be carried out in order to ensure that the achieved IT security level is being maintained and the certification statement.

8.5. Requirements for BS 7799 certification

As part of the BS 7799 certification process, your organization needs to complete a set of tasks:

- Completion of a risk analysis with analysis of threads and deficiencies as well as expectable extent of damage and likelihood of occurrence
- Establishment of a risk management system
- Establishment of a process for identification, control and cost-effective removal or minimization of risks

Furthermore, a complete Information Security Management System Documentation needs to be produced. Compliance with BS 7799 requires the following composition of documents:

- Security Policy
- Definition of the scope of the Information Security Management System and the implemented procedures
- Documentation of a systematic risk assessment
- Risk treatment plan to operationalize the security goals taking into account financial and personnel resources
- Documented procedures required by the organization to ensure the effective planning, operation and control of all information security processes
- Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the Information Security Management System (e.g. visitors' books, audit records and authorization of access)

- Statements, specifying which required activities of BS 7799 have been found to be applicable / not applicable including the rationales.

On top of the BS 7799 specific documentation, our assessors require the following documents:

- Documentation of the activities of the management forum
- Documentation of responsibilities for the protection of individual assets and for the operation of specific security processes
- Documentation of a management authorization process for new information processing facilities
- Documentation of (process-)independent reviews of implemented measures
- Documentation of security aspects regarding sub contractors and outsourcing

8.6. The standard has 10 Domains, which address key areas of Information Security Management.

1. **Information Security Policy for the organization.**

   This activity involves a thorough understanding of the organization business goals and its dependence on information security. This entire exercise begins with creation of the IT Security Policy. This is an extremely important task and should convey total commitment of top management-. The policy cannot be a theoretical exercise. It should reflect the needs of the actual users. It should be implementable, easy to understand and must balance the level of protection with productivity. The policy should cover all the important areas like personnel, physical, procedural and technical.

2. **Creation of information security infrastructure**

   A management framework needs to be established to initiate, implement and control information security within the organization. This needs proper

procedures for approval of the information security policy, assigning of the security roles and coordination of security across the organization.

3. **Asset classification and control**

One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, which is appropriate for copy, store, transmit or destruction of the information asset.

4. **Personnel Security**

Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities. Various proactive measures that should be taken are, to make personnel screening policies, confidentiality agreements, terms and conditions of employment, and information security education and training.

Alert and well-trained employees who are aware of what to look for can prevent future security breaches.

5. **Physical and Environmental Security**

Designing a secure physical environment to prevent unauthorized access, damage and interference to business premises and information is usually the beginning point of any security plan. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables are some of the activities. Cost

effective design and constant monitoring are two key aspects to maintain adequate physical security control.

6. **Communications and Operations Management**

Properly documented procedures for the management and operation of all information processing facilities should be established. This includes detailed operating instructions and incident response procedures.

Network management requires a range of controls to achieve and maintain security in computer networks. This also includes establishing procedures for remote equipment including equipment in user areas. Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks. Special controls may also be required to maintain the availability of the network services.

Exchange of information and software between external organizations should be controlled, and should be compliant with any relevant legislation. There should be proper information and software exchange agreements, the media in transit need to be secure and should not be vulnerable to unauthorized access, misuse or corruption.

Electronic commerce involves electronic data interchange, electronic mail and online transactions across public networks such as Internet. Electronic commerce is vulnerable to a number of network threats that may result in fraudulent activity, contract dispute and disclosure or modification of information. Controls should be applied to protect electronic commerce from such threats.

7. **Access control**

Access to information and business processes should be controlled on the business and security requirements. This will include defining access control

policy and rules, user access management, user registration, privilege management, user password use and management, review of user access rights, network access controls, enforcing path from user terminal to computer, user authentication, node authentication, segregation of networks, network connection control, network routing control, operating system access control, user identification and authentication, use of system utilities, application access control, monitoring system access and use and ensuring information security when using mobile computing and tele-working facilities.

8. **System development and maintenance**

Security should ideally be built at the time of inception of a system. Hence security requirements should be identified and agreed prior to the development of information systems. This begins with security requirements analysis and specification and providing controls at every stage i.e. data input, data processing, data storage and retrieval and data output. It may be necessary to build applications with cryptographic controls. There should be a defined policy on the use of such controls, which may involve encryption, digital signature, use of digital certificates, protection of cryptographic keys and standards to be used for cryptography.

A strict change control procedure should be in place to facilitate tracking of changes. Any changes to operating system changes, software packages should be strictly controlled. Special precaution must be taken to ensure that no covert channels, back doors or Trojans are left in the application system for later exploitation.

9. **Business Continuity Management**

A business continuity management process should be designed, implemented and periodically tested to reduce the disruption caused by disasters and security failures. This begins by identifying all events that could cause

interruptions to business processes and depending on the risk assessment, preparation of a strategy plan. The plan needs to be periodically tested, maintained and re-assessed based on changing circumstances.

10. **Compliance**

It is essential that strict adherence is observed to the provision of national and international IT laws, pertaining to Intellectual Property Rights (IPR), software copyrights, safeguarding of organizational records, data protection and privacy of personal information, prevention of misuse of information processing facilities, regulation of cryptographic controls and collection of evidence.

Information Technology's use in business has also resulted in enacting of laws that enforce responsibility of compliance. All legal requirements must be complied with to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

8.7. COBIT

Control Objectives for Information and related Technology (COBIT) was created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI). It is a framework that outlines information technology control objectives to ensure that technology is properly governed and that it maps and supports business processes. COBIT is process oriented but IT driven, which means that it focuses on the success of business processes through the proper use of IT resources.

COBIT has been used mainly by the IT industry and in 1998 Management Guidelines were added, which expanded its relevance and use to today's business needs. It contains four domains, 34 processes, 318 control objectives, and close to 1,600 control practices. The four domains are groupings of processes that map to the following organizational responsibilities:

- Planning and Organization
- Acquisition and Implementation
- Delivery and Support
- Monitoring

Each domain has a list of processes that should be followed, for example under the plan and organize domain the following processes are provided:

- Define a strategic IT plan
- Define the information architecture
- Determine the technological direction
- Define the IT organization and relationships
- Manage the IT investment
- Communicate management aims and direction
- Manage human resources
- Ensure compliance with external requirements
- Assess risks
- Manage projects
- Manage quality

The IT resources addressed in COBIT are data, application systems, technology, facilities and people. COBIT provides performance metrics to measure control effectiveness, necessary success factors for each IT process, and maturity models to allow for clear lines of continual improvement.

It is considered a true framework that allows for IT governance and is in its fourth edition. The main goal of COBIT is to accomplish business needs, through processes using IT resources in a controllable and measurable manner. It provides a criteria of key performance indicators (KPI) to evaluate the success of identified processes:

- Effectiveness
- Efficiency
- Confidentiality

- Integrity
- Availability
- Compliance

Information Technology Infrastructure Library (ITIL)

Although this framework was not asked about, it is an important component when comparing and contrasting current industry best practices. It is considered the de facto standard for IT service management and concentrates on how to provide consistent, documented, and repeatable processes to ensure quality.

None of these frameworks are in competition with each other, in fact, it is best if they are used together. Although they may seem at first to have overlaps, they do have distinct differences, pros and cons:

- ISO 17799 outlines security controls, but does not focus on how to integrate them into business processes
- ITIL focuses on IT processes, not on security
- COBIT focuses on controls and metrics, not as much on security

So, a combination of all three is usually the best approach. COBIT can be used to determine if the company's needs (including security) are being properly supported by IT. ISO 17799 can be used to determine and improve upon the company's security posture. And ITIL can be used to improve IT processes to meet the company's goals (including security).

8.8. BS 7799 (ISO 17799) and "It's" relevance to Indian Companies:

Although Indian companies and the Government have invested in IT, facts of theft and attacks on Indian sites and companies are alarming. 261 Indian Government sites were hacked in 2001* * Attacks and theft that happen on corporate websites are high and is usually kept under "strict" secrecy to avoid embarrassment from business partners, investors, media and customers.

Huge losses are some times un-audited and the only solution is to involve a model where one can see a long run business led approach to Information Security Management.

BS 7799 (ISO 17799) consists of 127 best security practices (covering 10 Domains which was discussed above) which Indian companies can adopt to build their Security Infrastructure. Even if a company decides not go in for the certification, BS 7799 (ISO 17799) model helps companies maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. Additional benefits of an ISM are improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact. Ultimately leads to increased profitability.

9. PCS/SCADA

Automation systems often referred to as process control systems (PCS) or supervisory control and data acquisition (SCADA) systems are critical to the safe, reliable, and efficient operation of many physical processes. PCS and SCADA are used extensively in petroleum and natural gas infrastructures, as well as in various manufacturing operations, and their use is growing in this sector. The government's interpretation of the term "SCADA" includes the overall collection of control systems that measure, report, and change the process. Essentially any subsystem that electronically measures state, alters process control parameters, presents/ stores/ communicates data, or the management thereof, is subsumed in the consideration of SCADA.

Given SCADA's pervasive use throughout the critical infrastructure, it is imperative in the near-term that security vulnerabilities in deployed systems be identified and subsequently mitigated; in parallel, longer-term basic must be conducted to design and implement next-generation secure SCADA systems. The SCADA research project addresses this pressing need through a multi-institutional effort to identify risk

management strategies for existing SCADA systems and to develop inherently secure designs for future SCADA systems.

The problem and its importance to the nation is the present state of cyber security and information assurance for SCADA is not commensurate with the threat or potential consequences. Security assessments of SCADA have identified troubling vulnerabilities in these systems.

The reliance of infrastructure on SCADA for operation and control is pervasive, and furthermore SCADA is increasingly used as a means of communication with customers. Cyber vulnerabilities place SCADA systems at risk and adversely affect not only the directly controlled infrastructure, but also other interconnected and interdependent critical infrastructures. These include gas and oil storage and transportation. For, example, during and after the 11 September 2001 attacks on the World Trade Center when information technologies of all kinds were indirectly affected, and in turn, affected the ability of other critical infrastructures to function.

SCADA systems are important for the safety of infrastructure systems and for economic production. The dependence of SCADA on conventional IT elements and its increasing use of the Internet causes it to inherit the known and emerging cyberspace risks, such as network hacking and cyber attacks (e.g., computer viruses and malicious code). To enhance security and trustworthiness of SCADA systems, it is imperative to comprehensively identify, assess, and manage the vulnerabilities inherent in their hardware and software composition, architecture, and configuration, along with the human supervision that controls and operates the system and the environment within which they operate.

The SCADA project is organized into six tasks in order to execute effectively. The six tasks are follows:

Task 1: Assess dependence on SCADA and its security

Task 2: Account for the type and magnitude of SCADA interdependencies

Task 1: Develop metrics for the assessment and management of SCADA security

Task 4: Develop inherently secure SCADA systems

Task 5: Develop cross domain solutions for information sharing

Task 6: Transfer technology of these solutions into industry

Each task will be performed by a team from several of the participating institutions, and each will have a Task Leader to coordinate the associated with the task. SNL will coordinate activities and facilitate technical exchange across the tasks to realize the synergistic potential of this multi-institutional effort.

The six tasks will enhance SCADA security through a combination of security engineering and basic science research, which will be grounded where appropriate to focus on SCADA issues within the oil and gas sector. The first task will bring together SCADA stakeholders — vendors, industry personnel and government officials — through workshops and working groups to aggregate information about the current state of SCADA systems. This characterization of the vulnerabilities, threats, consequences, and risks for SCADA security in the oil and gas infrastructure's facilities and operations will help shape the requirements of subsequent tasks. The second task extends this risk analysis to identify the indirect risks of cyber attack to SCADA systems of the oil and gas sector through an improved understanding of the sector's interconnectedness with other critical infrastructures. Recognizing that we must be able to measure the efficacy of cyber security to build a business case for investment in cyber risk management, the third task will develop metrics for the systemic quantification of the value of risk prevention, mitigation and correction. SCADA vulnerabilities remain in deployed systems because of insecure configuration of physical security, network design and weaknesses in the host systems. The fourth task addresses this problem by leveraging the team's existing cyber security capabilities to develop tools to make current SCADA system configurations more secure, while in tandem performing basic to

develop inherently secure designs for the SCADA systems of the future. The fifth and final task will develop technologies to improve cross-domain information sharing, which could lead to economic efficiencies for operators through optimized supply chain management, and would enhance infrastructure security by enabling the development of new system-level intrusion detection systems and regional and national infrastructure monitoring capabilities for emergency response management.

10. PCS Security Risk Assessment:

Process control systems (PCS) are crucial to many critical infrastructures, notably those in the oil and gas (O&G) sector. In the past, such systems were effectively isolated from sources of cyber threats external to their owners/operators. However, as enterprise systems evolve towards increasing integration, the need has increased for inherently secure process control systems: those that have been designed, implemented, and configured to minimize vulnerabilities to cyber threats.

Technical security risk analysis – the identification and assessment of risks associated with cyber threats that exploit vulnerabilities in a system's design, implementation, and/or configuration – is key to improving the security of systems throughout the system life-cycle. Technical security risk analysis is performed by technologists, but the results inform risk management decisions by upper management, who must view technical security risks in the larger context of business risks. This implies that connections between risks to processes supporting business operations and vulnerabilities inherent in the underlying process control system be recognized and understood. These connections can be difficult to understand and as a result, recommendations for mitigating vulnerabilities are often disregarded.

Keys to a better understanding of the relationships between vulnerabilities in PCS components and the business processes they support lie in how risk is assessed and how risk is communicated. The American Petroleum Institute (API) Standard 1164 and the National Petrochemical & Refiners Association (API/NPRA) Security

Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries address the security assessment problem space defined by environments where process control systems are used. Targeted and specific refinements to components of these security assessment methods will aid upper management in understanding how technical risks could manifest as adverse impacts to their company's operation and business objectives.

Based on analysis of these and other security risk assessment methodologies, it can be concluded that a PCS technical security risk assessment methodology should:

a) Draw upon and be consistent with overall IT risk assessment methodologies, but avoid the biases of such methodologies towards confidentiality as the primary security goal
b) Address PCS architectures, technologies, components, and configurations as sources of technical vulnerabilities
c) Be consistent with the differently-scoped risk models being developed under the project
d) Be consistent with the Security Vulnerability Assessment (SVA) or Instrumentation, Systems and Automation Society (ISA) methodology (that is, the correspondence between such risk modeling constructs as threats, vulnerabilities, and assets should be clear and comprehensive)
e) Be useful to those organizations that employ the SVA or ISA methodology, as a drill-down for the analysis and assessment of technical vulnerabilities and risks
f) Focus on technical risks to process control systems (including process control
g) systems that are interconnected with or interdependent on IT systems), rather than on risks to IT systems
h) Facilitate the evolution of process control systems toward more inherently secure systems

10.1 Need to Understand Technical Security Risks

Energy company owners/operators need a better understanding of the connection between risks to the production and distribution processes for energy products and vulnerabilities inherent in the process control systems controlling those processes, before they can make the commitment necessary to improve PCS security. No return-on-investment (ROI) case can usually be made; rather, enhancing cyber security serves to manage business risks associated with the second-order effects of cyber threats: loss of critical data, equipment malfunction, degraded or denied production or distribution. However, the relationship is typically subtle and complex, especially for large and multi-faceted operations. This often renders even the strongest connections all but invisible to anyone but a trained risk assessment professional.

As a consequence of this connection being difficult to understand, recommendations for mitigating vulnerabilities, or for applying sound design principles to architectures and systems, are frequently discounted, prioritized low, or even disregarded. Further, lack of an approach to illuminating cause-and-effect relationships, i.e., of exploited vulnerabilities, to resultant physical or business consequences, makes it more difficult for front line risk analysts to convey to corporate decision-makers risks to production and distribution operations in terms they would find useful.

Security of process control systems used in the oil and gas industry needs to be improved to safeguard production and distribution operations from intentional harm. Cyber attacks on process control systems, from master terminal units (MTU) in control centers down to the field end devices they manage (e.g., RTUs, PLCs, IEDs), could lead to:

- Endangerment to human life and/or the environment
- Loss of profitability for the affected company
- Harm to the nation's energy production infrastructure

An owner/operator of an oil or natural gas company will appreciate a business case for investing in security when persuaded that without the investment, human life, the

environment, or profitability could be harmed—this as a result of vulnerabilities in their process control systems being exploited. Better communication of the impacts compromised process control systems could have on corporate objectives will enable managers to better protect their interests from threats and minimize consequences should PCS vulnerabilities be exploited.

10.2 Keys to Understanding: Risk Assessment and Risk Communication

Understanding technical security risks involves two closely aligned activities—Assessment and Communication. The technical risk assessment involves all the hardware and software associated with the monitoring and control of a system, where, for example, that system could be defined as broadly as being an entire oil refinery, or as narrowly as being a single sensor or actuator attached to a PLC. Risk assessment problems in this dimension are suitably addressed by methods that take into account hardware/software vulnerabilities, threats in the form of exploits to systems possessing vulnerabilities, and consequences stemming from vulnerabilities that are exploited.

Risk communication between groups involves preparing and presenting risk information that is both convincing and motivating in terms that are directly applicable to them. Risk communication between assessment teams and corporate officers is greatly enhanced by risk assessment methods capable of translating technical risk into business risk, where that translation is via an industry-accepted algorithm and where risk to operations is expressed as potential business consequences both in financial terms and in terms that reflect an endangerment to human life and/or the environment. Potential solutions, acknowledging both the benefits and costs they will bring, must be a part of risk communication so that decision makers will have options that can be exercised.

Communication of risk involves effectively informing stakeholders at all levels. From the technician performing the most fundamental tasks to the corporate officer charged with maintaining commercial viability, each audience has their own goals and concerns. The risk information must be clearly presented to them in those terms, and must also be consistent, well-founded and defensible.

10.3 The PCS Technical Security Risk Assessment Problem Domaim:

The PCS technical security risk assessment problem can be stated as follows:

> How can technical risks to PCS security be assessed, and how can the results of the assessment be communicated meaningfully to corporate decision-makers, so that enterprise process control systems can evolve toward greater inherent security?

Several aspects of the PCS technical security problem domain must be considered, to enable the definition of a methodology, and development of a supporting tool, to address this problem:

- The relationship between PCS technical security and information technology (IT) security
- PCS technologies
- The evolution of security risk assessment methodologies for PCS environments
- Sources of technical security risk in PCS environments

10.4 Relevance of IT Risk Assessment Methods

An approach frequently taken to address PCS technical security is to apply concepts and technologies for information technology (IT) security. Risk assessment methods and techniques have been devised and developed over the years, primarily within government and academia, in response to security risk management challenges facing IT enterprises. Three such methods are listed below for illustrative purposes. They are

- The National Security Agency (NSA) InfoSec Assessment Methodology (IAM) (NSA undated)
- The National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems (NIST 2002)
- The Carnegie Mellon University (CMU) Software Engineering Institute Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Alberts 1999)

Each of these methods, and other similar methods not listed, has been used in different Department of Defense (DoD), national level agency, and industry settings with varying degrees of usefulness. They attempt to determine the amount of risk faced by enterprises, expressed in the traditional terms of information unavailability, corruption, and disclosure. Also considered by these assessment methods, albeit selectively, is the prospect of unauthorized physical access and its role in facilitating cyber attacks. However, the consequences from attacks on PCS components go beyond damage to information; they include physical process alteration, which could have dramatic operational, financial, and safety ramifications.

10.5 Risk Communication Issues

Because risk concepts of the IT domain are difficult to understand, they are also difficult to communicate effectively to non-IT professionals. Expanding the IT enterprise to now include computerized, network-ready physical control devices unfamiliar to IT risk professionals (e.g., physical sensors and actuators connected to programmable logic controllers) only compounds the risk communication problem. It is difficult for an organization to manage risks without everyone fully understanding what they are.

When assessing risk in PCS networks, the end focus should not be on abstract consequences such as a denial of service, but rather on tangible consequences from cyber attacks (e.g., the intentional malfunction of a PLC and its sensor and how that would affect an oil refining production step). There is a difference between the temporary unavailability of a network information server and a maliciously manipulated plant process that allows a volatile material to enter an unstable state. The difference between these two types of consequences is not lost on plant operators and must be effectively communicated with a credible basis for all assertions and consequences.

The seriousness of potential consequences from cyber attacks on process control systems argues that technical vulnerabilities in process control system components be unambiguously mapped to specific physical consequences that could manifest themselves should those vulnerabilities be exploited. Development of

inherently secure process control systems will be facilitated by use of risk assessment tools and techniques that express risk in terms of impact on operations and then on business objectives. Communicating a better understanding of the likely consequences, given the prevailing threat environment of not developing inherently secure process control systems, will motivate greater consideration of recommendations for making these systems more secure. Obstacles to effective risk communication, such as the use of technical terms and abstract concepts when presenting assessment results to upper management, and not adequately explaining cause-and-effect relationships involving exploited components and their resultant impacts on operations, must be overcome in order to help justify needed security investments indicated through risk assessment and analysis.

10.6 PCS Technologies

A PCS technical security risk assessment methodology must facilitate analysis of a process control system throughout its life-cycle. It must identify and facilitate the identification of vulnerabilities in the PCS architecture and its underlying technologies and components, as designed, built, and operationally configured. The PCS architecture includes specification of the functionality of PCS components (increasingly in terms of standards) and of how components are assembled in interdependent ways. Within oil and gas sector enterprises, process control systems evolve (rather than being replaced by new turn-key systems); changes are implemented gradually to minimize operational impacts. An organization's PCS architecture can be expected to change slowly. Therefore, in the near term, evolution toward inherently secure process control systems must focus on addressing vulnerabilities in components, their configurations, and their interdependencies.

Considerable guidance exists for security of IT components. However, that guidance is frequently irrelevant to the PCS environment in which real-time response is crucial to safety and operational performance. Security configuration guidance for the PCS environment is limited (see, for example, (NISCC 2005)). However, the development of more guidance can be expected. A PCS technical security risk assessment methodology must thus be capable of including or using such guidance.

Table 1 below identifies major PCS hardware and software components typically used in the monitoring and control of equipment within energy producing enterprises. Their likelihood of presence/use in control centers, remote stations, and plants is noted in the table. Together, they represent a core of potential sources of vulnerabilities and must be considered when modeling risk in energy production operations that use process control systems.

Table 1 PCS Technologies/Components

PCS Technology/ component	*PCS Point of Service*		
	Control Center	**Remote Station**	**Plant**
PCS / WAN interfaces	***D***	***D***	***D***
HMI/MMI (MTU/RTU)	***D***	***M***	***D***
Alarm Subsystems	***D***		
Data archiving (database server)	***P***		
Links to operation's business network	***P***		
FEPs (front end processor/local data storage)	***M***	***M***	***M***
Internet connectivity	***M***		
Global control loops	***M***		
RTUs/IEDs/PLCs		***D***	***D***
Sensors		***D***	***D***

Control equipment and actuators		***P***	***D***
Local control loops		***P***	***D***
Communication protocols (e.g., ModBus, TCP/IP)	***D***	***D***	***D***
SCADA/PCS system software	***D***	***P***	***D***
Business network interface			***M***

Source: Sandia National Laboratories

Key: D = definitely have, P = probably have, M = may have

The PCS components described in Table 1 are used for monitoring and controlling business objects. A business object, as defined in the Oil and Gas sector, is typically hardware in substance (equipment) and is used to facilitate business objectives of an organization. In the case of an oil production enterprise, high-level business objects include

- Platforms (sea-based)
- Wells (land-based)
- Pipelines (well to tanker/refinery, refinery to distributors/outlets)
- Tankers (transportation of oil (crude))
- Facilities (petroleum terminal (dock), storage, refinery, pumping/distribution)
- Retail outlets (gasoline, heating oil, jet fuel)
- PCS network

Business processes that rely on the availability and correct operation of these high-level business objects could be adversely affected through the exploitation of vulnerabilities in process control systems. Together, these objects represent potential

business-level areas of impact that must be considered when constructing a process control system-centric model of business risk.

High-level business objects are not directly monitored and controlled by process control systems; rather, it is the underlying electro-mechanical business objects such as pumps, valves, switches and heaters that are. These objects are representative of the class of objects that mechanically instrument platforms, wells, refineries, etc., and are essential to production operations. Thus, they must also be considered when modeling risk in process control systems and to the high-level operations they support. These lower level business objects are what interface to PCS end devices (e.g., IEDs, PLCs, RTUs) and are therefore susceptible to malicious manipulation.

10.7 Security Risk Management Methodologies for Process Control Systems

Existing and emerging industry standards for PCS security address risk management to varying degrees.

- o Security Vulnerability Assessment (SVA) Methodology for the Petroleum and Petrochemical Industries (API 2004c), which is an adjunct to the vulnerability assessment process defined in the Security Guidelines for the Petroleum Industry (API 2005)
- o Risk analysis methodology described in Appendix B of API 1164 (API 2004b)
- o Risk analysis methodology for integrating electronic security into the manufacturing and control systems environment (ISA 2004b)

Each of these methods is based, explicitly or implicitly, on IT security risk management methods. The National Institute of Standards and Technology (NIST) Risk Management Guide for Information Technology Systems (NIST 2002) serves as a risk assessment/risk management framework from which the assessment/analysis methods cited above draw some of their techniques.

The Security Guidelines for the Petroleum Industry (API 2005) identify the following security vulnerability assessment methodologies, but allow for the use of other methodologies:

→ The SVA methodology (API 2004c)

→ API RP 70 Security for Offshore Oil & Natural Gas Operations (API 2003)

→ API RP 70I Security for International Oil and Natural Gas Operations (API 2004a)

→ USCG NVIC 11-02, relevant solely to specific types of facilities (USCG 2004)

→ The American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS®) "Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites"; and

→ The Sandia National Laboratories Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF).

No guidance is given on selecting a methodology, and these methodologies are scoped more broadly than cyber security. However, the Chemical Industry Data Exchange (CIDX) has defined a process for comparing cyber security vulnerability assessment (CSVA) methodologies, and applied this to nine methodologies (CIDX 2003). The comparison is based on 17 basic criteria, 11 desirable properties, and four nice-to-have properties for the methodology. One of the basic criteria is that the CVSA be "applicable to all types of computer systems (DCS, PLC, SCADA, Enterprise Network, Business LAN/WAN), and their support systems (Utilities, rack room, fire protection, environmental control and network connections), used at process plants." While some of the methodologies CIDX compared met this criterion, the focus is not on technical security risks. Thus, it is unclear whether the existing methodologies compared by CIDX could be used to guide the development or evolution of process control systems toward inherent security.

Overall, the API Security Guidelines and SVA provide a useful structure for security risk assessment. The Security Guidelines (API 2003) focus on assessing risks

associated with possible terrorist attacks. However, The SVA methodology defines four classes of threat sources:

- "Terrorists (international or domestic);
- Activists, pressure groups, single-issue zealots;
- Disgruntled employees or contractors;
- Criminals (e.g., white collar, cyber hacker, organized, opportunists)."

The SVA methodology also defines three threat types:

- "Insider threats
- External threats
- Insiders working as colluders with external threats"

The SVA methodology identifies critical assets; identifies, for each asset, critical functions and interdependencies; and assesses asset attractiveness to adversary. The SVA methodology provides blank forms for identifying and assessing assets, threats, asset attractiveness to threats, and for vulnerability identification, risk ranking, and countermeasure identification.

The scope of the SVA methodology is broad; cyber security is addressed as one area. Cyber countermeasures involve application of good IT security practices and do not address the cyber security concerns specific to process control systems. The SVA methodology "has been used extensively at a wide variety of facilities involving all aspects of the petroleum and petrochemical industry." (API 2004a) Thus, a PCS technical security risk assessment methodology should

- ✓ Be consistent with the SVA methodology (that is, the correspondence between such risk modeling constructs as threats, vulnerabilities, and assets should be clear and comprehensive); and
- ✓ Be useful to those organizations that employ the SVA methodology, as a drill-down for the analysis and assessment of technical vulnerabilities and risks.

In addition, however, a PCS technical security risk assessment methodology should

- ✓ Focus on technical risks to process control systems (including process control systems that are interconnected with or interdependent on IT systems), rather than on risks to IT systems
- ✓ Facilitate the evolution of process control systems toward more inherently secure systems.

ISA Technical Report 99.00.02, Integrating Electronic Security into the Manufacturing and Control Systems Environment (ISA 2004b) presents an asset-based methodology for performing security vulnerability and risk assessment for such systems. This methodology like the accompanying technical report on security technologies (ISA 2004a) focuses on IT security technologies and vulnerabilities. However, a PCS technical security risk assessment methodology could use, or draw from, the assessment measures defined in this methodology.

The Natural Gas Security Committee of the American Gas Association (AGA) references the NIPC Risk Management Guide (NIPC 2002) for an overall framework. The AGA's specific security guidance (AGA 2004) describes a high-level risk assessment process, consisting of Three Layer Analysis, Security Architecture Analysis, and Successive Compromise Analysis. However, this guidance does not address assessment or risk communication.

The risk models (risks to the infrastructure due to potential vulnerabilities in process control systems, risks of cascading effects resulting from system interdependencies and cyber attacks) being developed under other I3P tasks (Lindqvist 2005) are not focused on technical security risks alone. However, a PCS technical security risk assessment methodology should be consistent with these models.

10.8 Sources of Technical Security Risk in Process Control Systems

Process control systems used in past decades to instrument energy production facilities were by today's standards less prone to cyber attack. This was due largely to the use of proprietary communication methods to exchange information between field locations and the operations center as well as the PCS LAN's isolation from the corporate business LAN. Modern process control systems use open (i.e., standards-based rather than proprietary) technologies. While open technologies have helped improve oil and gas operations, they have also made those same operations less secure due to their newly acquired exposure to vulnerabilities exhibited by the open technologies being embraced.

Internet Protocol (IP) -based networks are examples of open technologies currently being used within a number of critical infrastructure sectors. Because IP-based PCS networks can be implemented easily and interconnect with corporate networks, they, in some cases, allow business users and corporate clients to gain access to field data directly. However, the connection of PCS networks to corporate networks and the Internet also exposes them to many more risks of attack and sabotage through viruses and other forms of malicious code. (Zonneveld 2004)

10.9 Process Control Systems Remain Vulnerable to Physical and Cyber Attacks:

- Process control systems were not built with security in mind companies use a complex mix of hardware and software systems, often without any basic security (authentication, intrusion detection, encryption, and logging).
- The prevalence of old technology and the real-time environment limit security options – shutting down process control systems upon suspicion of an attack is often not possible.
- The oil and gas infrastructure is vulnerable to physical attacks due to the wide distribution of assets and volatility of the material.

- Safe and reliable operation of the oil and gas industry depends heavily on other critical infrastructures, such as telecommunications, electric power, water and transportation.

10.10 Threats Against Process Control Systems Are:

⇒ Process control system operators should consider serious threats like professional hackers and organized cyber-terrorism.

⇒ A coordinated attack along several threat vectors is a serious long-term threat. A thorough analysis of the real risks (vulnerabilities, threats and probability of occurrence) and consequences (damage restoration time and costs) is critical.

⇒ Access to information about control systems and software tools to compromise them is readily available, often on the web. These industrial automation technologies are used worldwide in the oil and gas industry.

10.11 Security Issues from the Industry Perspective:

- ✓ How does it help Us Make Better Oil? Process control system security is all overhead – asset owners need a business case for implementing security to convince senior management.
- ✓ In the oil and gas industry, safety (not security) is always the primary concern. Security strategies must fit into this framework.
- ✓ Dependability, reliability and redundancy are critical for SCADA – the availability of systems trumps everything else.
- ✓ Control systems are often remotely accessible and increasingly connected via the Internet or through wireless networks.
- ✓ In many cases attackers can access critical control systems through non-critical corporate networks.
- ✓ Insider attacks from disgruntled employees with detailed system knowledge are one of the most serious security challenges.
- ✓ The high cost of patching and constant software security fixes puts a strain on the oil and gas industry and reduces security.

- ✓ The increasing use of commercial software and networking technologies introduces known vulnerabilities.
- ✓ Inadequate information sharing within the industry and with government may contribute to an apparent dearth of incident and threat information.

10.12 Problems Can Be Addressed at the National Level:

- ❖ Solutions require close collaboration between oil and gas operators, vendors, the research community and the government.
- ❖ Widely-accepted security standards, best practices and metrics for the oil and gas industry are urgently required.
- ❖ Inherently secure SCADA systems and technologies need to be developed.

11. Cryptographic Protections of SCADA Communications

The details for retrofitting serial communications links with cryptographic protection, such as the hardware design, the general functionality, and the description of the communications protocols and key management procedures, will be finalized based in part on your submitted comments.

SCADA Serial Line Operational Constraints

The following is a description of the general SCADA equipment characteristics and operating environment for transferring SCADA messages over asynchronous serial links as described in AGA 12 Annex C. When SCADA communications are to be cryptographically protected the equipment characteristics and the operating environment combine to produce constraints of which system designers and operators must be aware.

This is structured to be a list of the environmental realities (identified below by a letter and number in the form E*n*, where *n* is an integer designated to identify the particular environmental or equipment characteristic. Following each characteristic,

the corresponding constraint(s) is(are) listed; these constraints are identified with an index number of the form C*n.m*, where the C indicates a constraint, *n* is an index that is the same as the index E*n* corresponding to an environmental characteristic, and *m* is an index to distinguish different constraints arising from environmental characteristic E*n*. Thus, each environmental characteristic E*n* has one or more constraint implications, C*n*.1, C*n*.2, etc. The acronym **SCM designates a SCADA Cryptographic Module**, the component of the system that provides cryptographic protection to the communication channel used by the SCADA system.

11.1 General

E1: SCADA system operators want to deny unauthorized access to their system, including access as a result of malicious or inadvertent insider operations.

C1.1: Without existing methods, a new method needs to be developed to protect SCADA systems from unauthorized uses. This includes providing confidentiality, integrity, and authentication.

C1.2: A system for managing the SCADA protection mechanisms should address protecting data-in-transit, data-at-rest, and authorized operators.

C1.3: The system for managing the SCADA protection mechanisms should be designed with an operating model of "separation of duties", i.e., no one individual shall have total control over the management system.

C1.4: The system for managing the SCADA protection mechanisms should be designed as a single system or interoperable modules to address all forms of SCADA protection, including configuration of cryptographic modules; provisioning cryptographic material for cryptographic modules; monitoring forensic and usage information from cryptographic modules; managing operators, their authorized roles and privileges; managing operator two-factor authentication hardware tokens; provisioning cryptographic materials for operators and their two-factor authentication hardware tokens; monitoring usage and actions taken by operators; and creating and managing cryptographic materials for protection of data-at-rest.

11.2 Business & Operational Issues

E2: Utilities have significant investment in SCADA equipment, in terms of capital investment (hardware and software) and training of operational personnel (SCADA operators, engineers, maintenance technicians, etc.).

C2.1: Protection methods shall not be developed that require major replacement of existing equipment or software/hardware modifications requiring the re-certification of the existing SCADA equipment in the near term.

C2.2: Integration of protection methods shall not be prohibitive in terms of cost, complexity, or operations.

E3: Operating under time & funding limitations, utility SCADA operators would like the option of selecting from multiple vendors equipment and techniques to protect their systems that are low cost, and easy to install and operate.

C3.1: SCADA protection products shall have a minimum level of interoperability, both between different products by the same manufacturer and products made by different manufacturers.

C3.2: Management systems of the SCADA protection mechanism should be designed to leverage and interoperate with existing security management systems, including directory structures, key management systems, and intrusion detections systems.

E4: Utility communications (including SCADA, EMS, DMS, and DER) can occur between multiple entities which interact for business and operational purposes, including market trading and ISO, RTO, or DER Aggregator relationships.

C4.1: Protection mechanisms shall support at least limited interoperability, both between different products by the same manufacturer, and products made by different manufacturers.

C4.2: Protection mechanism should address multi-domain issues, such as designated roles and responsibilities including owners, operators, field maintenance technicians, control center management/provisioning, data access privileges, etc., and interoperable credentials to allow access without creating vulnerabilities.

11.3 Equipment

E5: SCADA and similar control equipment are designed to have significant lifetimes.

C5.1: Protection methods shall not be developed that assume that replacement of SCADA equipment will happen in the near term, e.g., that new equipment with additional capabilities will replace existing equipment any time soon.

C5.2: Protection methods should be designed to provide for compatibility between near-term and long-term solutions.

E6: The processors traditionally used in remote SCADA units (e.g., RTUs, IEDs) have limited capabilities and low processor speeds compared to current desktop computers, and have little additional memory for programmable functionality.

C6.1: Because testing with typical hardware (such as the effort in a previous GTI project) has shown, in general, that adequate cryptographic functionality cannot be provided by the limited capabilities of legacy remote SCADA processors, protection methods should be implemented as a retrofitted add-on device.

C6.2: Existing SCADA systems should be able to operate without knowledge of any add-on protecting devices.

C6.3: Control communication with external devices shall not be interrupted, e.g., modem commands should be detected and sent "in-the-clear".

E7: SCADA communications occur over wired lines and wireless channels that may have various levels of protection afforded by existing measures. Some are protected within buildings and fences; some are exposed through/by third parties such as the telephone company, while others are relatively unprotected.

C7.1: Potential attackers can access exposed communications links. Such attacks include listening to or altering SCADA messages, generating new SCADA messages, or blocking the flow of data.

E8: SCADA systems operate in harsh environmental conditions.

C8.1: Protection mechanisms should operate in traditional SCADA environments, including both substation environments and control center environments.

E9: SCADA equipment is typically housed in substations, protective enclosures, or control center equipment rooms.

C9.1: Protection mechanisms should be designed, at a minimum, to exhibit evidence if the mechanism is tampered with.

C9.2: Protection mechanisms may rely upon physical protection (i.e., limited operator access) for some of its security requirements.

11.4 Channel topology

E10: The majority of remote SCADA communication is over leased lines, dial-up connections, or radio links.

C10.1: The communication links to field devices (e.g., asynchronous serial) do not provide either virtual or physical concurrent connections to multiple entities. If an SCM is placed on a particular communication link (e.g., in-line); the SCM cannot contact another entity to obtain information or services (e.g., to acquire an encryption key or to verify the status of a partner's credentials).

E11: In some cases, secondary, or backup, communication links are present, e.g., dial-up connections are often used as backup for leased lines.

C11.1: Alternative connections may require different types of SCADA message protection and may require protection equipment to be able to differentiate between the primary and secondary channels.

E12: Many SCADA networks are designed for the possibility of multiple SCADA hosts that communicate with SCADA field units, e.g., primary and backup center.

C12.1: Protection mechanism management should be designed to operate in one or more control centers, for disaster recovery and distributed management purposes.

C12.2: Protection methods shall not interfere with the ability of a utility to switch between the primary and the backup SCADA host(s), e.g., support for "cold" backup control centers (normally off, and must be started before use).

C12.3: SCMs should support multiple addresses so backup control centers can monitor traffic between the primary control center and field devices, e.g., support for "hot" (actively monitoring or aware of all message traffic) or "warm" (active but not monitoring message traffic) backup control centers.

C12.4: Protection mechanism should support both local and remote (in-band) management (including configuration, forensics, and key management).

11.5 Channel characteristics

E13: Most communication is low speed serial (300-2400 bps, with newer units using 9600 and 19,200 bps), and uses either byte- or bit-oriented protocols, with a trend toward byte-oriented in new equipment.

C13.1: Little additional bandwidth is available in which to perform functions related to the cryptographic protection (e.g., session establishment).

C13.2: Protection mechanisms shall support both hardware and software flow control to minimize the potential for data loss.

E14: In many instances, SCADA message times are short compared to the time to open and close communication channels. Many SCADA operators have stated that they thought higher baud rates require more time for modems to negotiate than the entire time it takes to issue a SCADA command and receive a reply using modems operating at the lower baud rates.

C14.1: SCADA systems are designed for frequent (near real-time) status updates. Incorporation of cryptographic functions should not reduce the reading frequency of an existing system below an acceptable level (nominally 20%).

E15: The serial connection ensures that the order of messages received matches the order of the sent messages. There is no packet re-ordering or multiple delivery path issue as may be present on packet networks.

C15.1: Any protection method shall preserve message ordering to accommodate the existing equipment and software.

E16: SCADA units can communicate over shared or unshared channels, i.e., a SCADA host may use a particular channel to communicate with one or more field units.

C16.1: Protection methods shall be selected/ designed to be able to properly direct protected SCADA messages to the appropriate SCMs, for those instances in which the exposed channel is shared amongst multiple SCADA units (also described as a multi-drop, multipoint, or daisy-chain configuration). Note: SCADA units connected by radio communications can be seen as operating in this fashion.

C16.2: SCMs shall be able to associate multiple SCADA units with target SCMs, for those instances in which only one exposed channel connects multiple SCADA units with the host.

E17: SCADA units on a shared channel may have SCMs installed on only some of the RTUs as needed (determined by priority/security), the SCMs may be gradually deployed in a staged fashion, or some may be out-of-service for maintenance.

C17.1: Protected equipment may need to share a communications channel with unprotected equipment, without causing interference between protected and unprotected equipment.

C17.2: Protection methods need to be able to differentiate between SCADA units that are protected and those that are not, and send the appropriate encrypted or unencrypted message.

C17.3: Protection methods need to be designed so that protected SCADA messages cannot be inadvertently recognized as unprotected SCADA messages.

E18: SCADA units on a shared channel (e.g., daisy-chained) may have multiple segments of the line externally exposed between field units, requiring protection mechanisms at each connection point along the line.

C18.1 Protection mechanisms shall be designed to permit recognition of SCADA addresses to properly identify SCADA units, and to associate SCMs with SCADA units to direct the protected messages.

E19: Communications may be implemented as store-and-forward, where one SCADA unit receives a message as an intermediary, then re-transmits it to the intended unit.

C19.1: Protection methods need to be designed to not interfere with the store-and-forward function as implemented by some SCADA protocols.

11.6 SCADA messages

E20: Short message lengths are common for many commands and responses; most messages are in the range of 16-32 bytes. Almost all messages are less than 256 bytes.

C20.1: Implementation of methods to protect messages needs to ensure that transmission is not significantly delayed by the additional information required for

protection, e.g., adding 32 bytes or more of overhead to an 8 byte message should be avoided.

E21: Responses to queries may be as short as the query, or they may be significantly longer. In some instances a single query can prompt a response of multiple messages (e.g., a request for historic information or range of data).

C21.1: SCADA message protection shall not be based the assumption of 1:1 message flows, i.e., one response for one query.

11.7 SCADA error handling

E22: Noise can interfere with integrity of messages (especially on radio links). Typically integrity is checked using a checksum or CRC as part of the SCADA message.

C22.1: Protection methods shall be designed to not interfere with existing SCADA protocol integrity checks.

C22.2: Protection methods should not be potentially weakened by the presence of SCADA integrity checks.

E23: SCADA systems are designed to handle damaged or un-received messages due to noise and other interference with timeouts and retries in the SCADA application.

C23.1: Protection methods should not interfere with normal problem identification and handling by the SCADA application, e.g., implementing secure transport involving retries may interfere with the natural SCADA retrial.

C23.2 Protection methods should not add additional traffic on the line for error handling that may interfere with the normal operation (i.e., poll cycle or scan rate) of the SCADA system

11.8 SCADA protocols

E24: There are estimated to be between 100 and 250 SCADA communications protocols in the field.

C24.1: Independence of the SCADA message format is desirable. Incorporation of a method to recognize (parse) all or most SCADA protocols is not considered necessary

for protecting the SCADA messages. Protection methods that require minimal or no understanding of the SCADA protocol are desired.

E25: SCADA protocols use various methods to identify messages and message lengths. This can include message length values embedded in the SCADA message, special values used as markers (e.g., End-Of-Text), and/or timing values (e.g., period of silence indicates message end).

C25.1: Protection methods need to be able to handle, at a minimum, the three identified methods of recognizing SCADA start-of-message and end-of-message to be able to properly encapsulate messages.

C25.2: Overhead latency should be kept to a minimum so that time-based end-of-message detection is not adversely impacted (i.e., a long SCADA message broken into multiple parts by the SCM is decrypted and reassembled in a reasonable amount of time such that the SCADA protocol is not fooled into believing it has received multiple messages, rendering the original SCADA message unusable).

E26: Multiple SCADA protocols can be transmitted on the same channel. The differences between protocols permit units to recognize their own messages while ignoring the others with the different protocol, usually treating them as noise.

C26.1: Protection methods need to be designed so that protected SCADA messages are not inadvertently recognized as any of the existing SCADA protocols on a channel.

C26.2: Protection methods may need to be configurable to differentiate between (multiple) SCADA protocols that exist on the same channel.

E27: Most SCADA messages are repetitive (e.g., status requests) or are very similar (e.g., status responses).

C27.1: Protection methods shall to be designed to recognize that few unique messages are sent. If a unit sends the same (unprotected) message repeatedly, the protected form of the message shall be different. C27.2 Protection mechanisms shall protect against message replay.

E28: Although most SCADA systems operate on the poll-response model, some SCADA field units can initiate a message to the host (i.e., report by exception).

C28.1: Protection methods should not interfere with the basic operation of each SCADA unit to initiate messages, if the SCADA protocol permits such function.

C28.2: SCMs at either end of the link should be able to initiate (request) a cryptographic session.

C28.3 Protection mechanisms shall protect against message spoofing.

11.9 SCADA broadcast/multicast capabilities

E29: Some SCADA protocols provide for a broadcast (all units) or multicast (range of units) address.

C29.1: Protection methods should be able to accommodate broadcast or multicast transmission to multiple SCADA field units. (Note: SCADA protocols that do not implement this feature natively will not have it provided by the SCMs.)

C29.2: Broadcast/multicast messages that are encrypted should be intelligible to all protected SCADA units on the SCADA system that are intended to receive them without the necessity of sending the broad/multi cast message to each unit separately.

C29.3: Broadcast/multicast messages shall be sent in the clear to unprotected SCADA units.

C29.4: SCMs should support multiple broadcast addresses or subscription groups.

C29.5: Protection methods should be designed to minimize the timing differences in the availability of the SCADA message between encrypted broadcast messages and unencrypted broadcast messages; important in "set time" functions.

C29.6: Protection methods should be designed recognizing that sending both plaintext and ciphertext of the same SCADA message makes analysis to derive the encryption key "easier". For example, separate keys should be used for broadcast message versus unicast message, and broadcast and multicast keys should be changed frequently.

11.10 SCADA field device maintenance ports

E30: Many SCADA field devices support dial-up maintenance ports, which permit remote access for authorized technicians to modify settings, programming, etc., as required for support functions.

C30.1: Protection mechanism shall recognize there may be a potentially large number of technicians authorized to perform maintenance on field devices.

C30.2: Protection mechanism shall identify technicians uniquely due to the potentially transient nature of technicians (e.g., temporary employees, contractors, vendors, etc), and for auditing purposes.

C30.3: Protection mechanism shall recognize the technicians may be authorized to perform maintenance on specific devices, or perform maintenance for a limited period of time.

C30.4: Protection mechanism may not be able to establish a concurrent connection to a centralized host to offload authentication and authorization processes, i.e., authentication and authorization may need to be performed locally by the protection mechanism.

E31: SCADA maintenance port interaction is defined by the speed of the technician, instead of the real-time needs specified for the SCADA host.

C31.1: Communication timing periods can be relaxed in comparison to those for the primary control and reporting channel needs.

E32: Typical SCADA maintenance port interaction is via dialup mechanisms.

C32.1: Protection mechanism should provide support for multiple types of dialup topologies, including: field devices with external modems; field devices with internal modems; a single modem interacting with a single field device; and a single modem interacting with multiple field devices.

C32.2: Protection mechanism should not interfere with the ability of the field device to dial out, such as to report an alarm or alert condition.

C32.3: Protection mechanism should not significantly interfere with the field device's existing maintenance mechanisms or procedures.

12. Security Solutions for the Oil and Gas Industry

Protect corporate, pipeline, and refinery networks against cyber attacks and vulnerabilities

Overview

Oil and gas companies are accustomed to dealing with physical security and safety issues to achieve a safe and operationally efficient environment. But in today's world, these companies must consider the security and availability of both their corporate IT and process control networks (PCNs) to reach that goal. Fortunately, many security and availability best practices have been developed and applied to oil and gas corporate IT networks to protect them from unexpected cyber attacks and outages. But these best practices cannot be automatically applied to PCNs because of the unique security and availability issues associated with oil and gas PCNs.

Customer Benefits

• Achieve required levels of availability and reliability for PCNs in the interconnected environment

• Avoid penalties, financial losses, and safety issues associated with supply disruptions

• Achieve regulatory and industry standards compliance

• Assess security risks, identify vulnerabilities, and respond immediately to emerging threats

Key Advantages

- Enables pipelines and refineries to create a security framework with products tailored to the specific needs of oil and gas industry
- Enables reliable and secure interconnections between corporate, SCADA, and DCS networks
- Includes security measures specific to SCADA and DCS networks—such as Modbus and ICCP signature support

12.1 Cyber Security for Process Control Networks

Solution for the Oil and Gas Industry comprises a number of products and services that help protect process control networks against cyber attacks and vulnerabilities and that is aligned with the four-step cyber security process shown below.

SCADA/DCS Security Assessment Services

The first step in determining one's risk profile is to assess where the security gaps lie. Security Services experts have unparalleled knowledge of SCADA/DCS systems and protocols such as ICCP and Modbus, and have worked with dozens of oil and gas and electric power companies to identify vulnerabilities and recommend remediation steps. This evaluation is performed in a comprehensive and safe manner, with no disruption to system operations.

12.2 Security Solutions for the Oil and Gas Industry

This service often extends beyond the evaluation of SCADA/DCS systems, resulting in a comprehensive evaluation of the network at large that encompasses network discovery, vulnerability detection, system penetration, and applications testing. It can also perform technical control reviews for a comprehensive assessment—beyond just the view of an external intruder. Concluding the assessment, It offers vendor-agnostic recommendations in network design and operational procedures.

Perimeter Security

Strong perimeter security is one of the first steps to effective PCN security. Whether the result of intentional attacks, accidents, or oversights, many threats start from within the organization. The following are best practice services and technologies for protecting SCADA and DCSs against both external and internal cyber attacks and vulnerabilities.

While perimeter firewalls provide an important first measure for separating the control system environment from the corporate network, they usually do not address application-level attacks, intrusions, or viruses. At the same time, certain technologies

and protocols are able to bypass typical firewall configurations. Traditional firewalls also cannot protect against blended threats which typically combine the characteristics of different types of malicious code (such as viruses, worms, and Trojan horse programs) and are able to exploit vulnerabilities. Traditional firewalls can even become the launch point for an attack.

Gateway Security is a comprehensive solution that includes full-inspection firewall technology, protocol anomaly-based intrusion prevention and intrusion detection engines, award-winning virus protection, URL-based content filtering, antispam technology, and IPSec-compliant virtual private networking technology with hardware-assisted high-speed encryption. When placed at the gateway between the Internet and the corporate network or control network, or between network segments, this appliance protects mission-critical systems against intrusions, viruses, worms, and other malicious code and threats.

Network Security

Once strong perimeter security is in place, the next step is to implement an intrusion detection/intrusion prevention system to protect the network against internal and external threats that may have been introduced from within the PCN segment. Network Security appliance is an Intrusion Detection/Prevention System (IDS) featuring both protocol anomaly and signature-based detection techniques that enable oil and gas companies to detect an attack that a firewall may miss. IDSs that use protocol anomaly detection along with attack and vulnerability signature based detection and prevention, are able to recognize standard SCADA and DCS protocols—such as Modbus and ICCP—and identify zero-day attacks, helping organizations stay abreast of even the newest threats, while ensuring that legitimate data is not misidentified as a threat. What's more, because IDSs do not block traffic, they do not introduce unwanted latency into the system.

Security Monitoring and Management

As oil and gas companies deploy security technologies throughout their networks, the challenge of properly managing and monitoring these resources on 24x7 bases becomes increasingly complex, especially in highly distributed environments that often lack easy physical access to security software and devices. Employing Managed Security Services—which provide 24/7 centralized management and monitoring of protection technologies along with early warnings, incident response, and decision support—is a key step in improving an organization's security posture. Written incident reports and trend reporting help organizations assess their overall security posture, while at the same time simplifying audits.

Complementary Security Products and Services

The following complementary offerings further protect the PCN while also safeguarding the corporate network.

Enterprise Security Manager

After establishing security policies, oil and gas companies need a policy compliance tool that measures the current state of security, compares it with the state needed to comply with specific regulations as well as company policy, and recommends measures to accomplish such compliance. With Enterprise Security Manager, oil and gas companies can address effective password management – disabling invalid accounts and access rights, disabling unused ports, securing modem connections, firewall management, updating antivirus software, and identifying vulnerabilities.

Antivirus

Antivirus Corporate Edition provides industry-leading, real-time virus and spyware protection and automatic virus removal for enterprise workstations and network servers.

Client Security

Client Security provides threat protection through integrated antivirus, firewall, and intrusion detection for remote, mobile, and networked client systems.

DeepSight

DeepSight Threat Management System tracks security on a global basis, providing early warning of active attacks specific to customer's systems and applications. With personalized notification triggers, expert analyses, and industry-specific reporting capabilities, the solution enables utilities to prioritize resources in order to better protect critical information assets against a potential attack.

LiveState Patch Management

On SCADA and DCS systems, patch management is complicated by difficulty in removing critical systems from service without impacting system reliability. In addition, companies often lack the necessary physical access to geographically distributed SCADA and DCS systems in order to effectively manage system patches. LiveState Patch Manager allows oil and gas companies to reliably protect their infrastructure from vulnerabilities. Its intuitive interface allows organizations to scan, identify, and install missing patches on hundreds of clients and servers in minutes. By centralizing and automating these tasks, LiveState Patch Manager

13. Vulnerability Assessment Vendors:

The energy sector represents a union between cyber control and monitoring systems, physical facilities, and the people that have the sector-specific knowledge base.

The oil infrastructure consists of oil production; crude oil transport; refining and processing; transport, holding, and distribution of refined products and petroleum-derived fuels; and control and other external support systems. The natural gas industry consists of exploration and production, storage, transmission, and local distribution. For both oil and natural gas, many miles of pipeline span the Region and

move a variety of substances, including crude oil, refined petroleum products and natural gas.

Common Vulnerability Assessment Tools Owners:

Methodologies currently available to Oil & Gas asset owners include the following:

1. AGA (American Gas Association)/INGAA (Interstate Natural Gas Association of America) Security Guidelines
2. ANL (Argonne National Laboratory) Checklist – screening tool
3. API (American Petroleum Institute) /NPRA (National Petrochemical and Refiners Association) SVA (Security Vulnerability Analysis)
4. Coast Guard Security Risk Guidelines
5. ExxonMobil SVA
6. IORTA (Information Operations Red Team Assessment) – external team from SNL will perform comprehensive physical and cyber analysis
7. LLNL (Lawrence Livermore National Laboratory) VA Capability – external team from LLNL will perform comprehensive physical and cyber analysis

Methods that can potentially be tailored to oil & gas assets include:

AS/NZS (Australia/New Zealand) Risk Management Guideline 4360:2004

1. CARVER + Shock VAM – widely-used screening tool
2. CCPS (Center for Chemical Process Safety) SVA or its computerized version SVA-Progeared towards facilities that handle hazardous chemicals
3. North Carolina Terrorism VSAT (Vulnerability Self-Assessment Tool)
4. RAMCAP (Risk Assessment Methodology for Critical Asset Protection)
5. VAM-CF (Vulnerability Assessment Methodology – Chemical Facilities)

14. STANDARDS

This section provides a brief description of an international information security standard and the two oil and gas segment security standards used in this study. Table 2 shows the major sections of each standard. This study can help identify the similarities and differences between standards, which can contribute to selecting the best security practices and help strengthen sections of the standards in future revisions.

14.1. **ISO/IEC 17799.** ISO/IEC 17799, First edition 2000-12-01, standard titled "Information Technology – Code of Practice for Information Security Management," gives recommendations for information security management. It is high level, broad in scope, conceptual in nature and intended to provide a basis for an organization to develop its own organizational security standards and security management practices.

The standard states: "This code of practice may be regarded as a starting point in developing organization specific guidance. Not all of the guidance and controls in the code of practice may be applicable. Furthermore, additional control not included in this document may be required."

ISO/IEC 17799 is a widely recognized, comprehensive information security standard. It is organized into ten major sections or topics. The sections are listed in Table 1, along with the major sections from the other standards covered in this report. Although it was not written specifically for the oil and gas sector, ISO/IEC 17799 offers guidelines and voluntary directions for information security management and is meant to provide a general description of the areas considered important when initiating, implementing, or maintaining information security in an organization. It addresses the topics in terms of policies and general good practices but does not provide definitive details or "how-to's."

14.2. **API 1164.** American Petroleum Institute (API) Standard 1164, First edition September 2004. API represents more than 400 members involved in oil and natural gas industry. Oil and natural gas utilities are part of the nation's critical infrastructure. They rely on SCADA systems to control their operations.

The objective of API 1164 is to provide "a means to improve the security of the pipeline SCADA operation by:

- Listing the processes used to identify and analyze the SCADA system vulnerabilities to unauthorized attacks
- Providing a comprehensive list of practices to harden the core architecture
- Providing examples of industry best practices."

"This standard on SCADA security provides guidance to the operators of oil and gas liquid pipeline systems for managing SCADA system integrity and security. The use of this document ... should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA system."

This standard is targeted at small to medium pipeline operators with limited Information Technology security resources. While the recommendations are not as comprehensive as those in ISO/IEC 17799, they are applicable to any SCADA system and their implementation could significantly improve the cyber security of a SCADA system. The two appendices in the specification add a significant amount of detail. Appendix A is a checklist to be used as a guide when reviewing the cyber security of SCADA systems. Appendix B is an example of a SCADA Control System Security Plan. It is intended to be used when developing an operator specific SCADA security plan. The example plan is not all-inclusive or intended to cover all possible vulnerabilities but it is a useful starting point.

14.3. **AGA-12**. American Gas Association (AGA) "Cryptographic Protection of SCADA Communications General Recommendations" Draft 3, AGA Report No. 12 dated August 14, 2004. The AGA represents 192 local utilities that deliver natural gas to homes, businesses, and industries throughout the United States. AGA member companies account for roughly 83 percent of all natural gas delivered by the nation's local natural gas distribution companies. The AGA "encourages and assists members in sharing information designed to achieve operational excellence by improving their security, safety, reliability, efficiency, and environmental and other performance."

Natural gas utilities are part of the nation's critical infrastructure. They rely on SCADA systems to control their operations. The AGA asked the Gas Technology Institute to research encryption methods that could lead to a standard industry encryption system for both new and existing SCADA systems.

AGA 12 is the first of an expected series of documents recommending practices designed to protect SCADA communications against cyber attacks. It is the product of a cooperative effort by AGA and the Gas Technology Institute in coordination with associations representing the gas, water, and electric industries; manufacturers; SCADA operators; U.S. Government Agencies (National Institute of Standards and Technology and Department of Transportation); and security experts. The intent of the recommended practices is "to provide confidential SCADA communications that are known to be unaltered by potential attackers and that can be authenticated as having originated from valid authorized users."

The AGA 12 series of documents focus on securing the communications link between field devices and the control servers or control center. AGA 12 "contains the background, security policy fundamentals, and a test plan that apply generally to all areas of cryptographic protection of SCADA systems." Planned addendums to AGA 12 are expected to address cryptographic key management, and protection of data at rest. Additional planned documents in the AGA 12 series include:

AGA 12-1: Retrofit link encryption for asynchronous serial communications of SCADA Systems

AGA 12-2: Protection of IP-based, networked SCADA systems

AGA 12-3: Protection embedded in SCADA components.

AGA 12 Draft 3 contains a number of informative sections as well as normative (required) sections. The major normative sections are listed in Table 1. Major informative sections include: SCADA fundamentals, Cryptography fundamentals, Challenges in applying cryptography to SCADA communications, and Classes of attacks against SCADA systems. As mentioned above, the main body of AGA 12 focuses on securing the communications link between field devices and the control servers or control center using encryption. However, Annex F provides a discussion on security practice fundamentals. Annex H provides a Cryptographic system test plan.

Table 2: Major Security Sections in Oil and Gas Standards

ISO/IEC17799 Information Technology Code of Practice for Information Security Management	**API 1164 Pipeline SCADA Security**	**AGA Cryptographic protection of SCADA Communica--tions General Recomm--endations**
Security Policy	Access Control	Steps to define Security Goals
Organizational Security	Communication	Cryptographic System Requirements
Asset Classification and Control	Information Distribution	
Physical Security	Physical	

Physical & Environmental Security	Network Design and Data Interchange	
Communications and Operations Management	Management System	
Access Control	Appendix – A (SCADA System Security Checklist) 1. Application and Database 2. Authentication 3. Change and Problem Management 4. Computer, Telephone, and Network Usage 5. Contractors, Vendors, Consultants, and Third Party 6. Information Classification and Application Criticality 7.Information Retention/ Archive/ Backup 8.Network Connectivity 9.Personnel Security 10. Physical Security	Annex F Security practice Fundamentals 1. Recommendations for staffing an InfoSec team 2. Awareness of security assurance 3. Recommendations for writing security policies 4. Recommendations for performing assessment and analysis 5. Auditing

Systems Development and Maintenance	Appendix B (Example) SCADA/Control System Security Plan 1. Identification and Documentation 2. Risk Analysis 3. Preventive Action 4. Oversight 5. Security Management	Annex H Cryptographic System Test Plan 1. Test requirements and evaluation criteria 2. Interoperability testing 3. Special test setup requirements 4. Test reports 5. Test Architecture and Environment
Business Continuity		
Compliance		

15. CONCLUSION

A number of recent events have raised the risk profiles of corporate information systems making them more vulnerable. Energy companies are therefore forced to renew their focus on information security to provide enhanced security in a cost-effective manner. By following a holistic approach to enterprise security detailed above, organizations can mitigate these risks, reduce operating costs and meet regulatory compliance deadlines.

Table 3: Energy and Utilities: Security Benchmarks

(Percentage of response from energy and utility executive)

	2005	2004
Security spending (as % of IT budget)	**8.7%**	**8.4%**
Will increase security budget next year	**48%**	**64%**
Reports Zero security events in past 12 months	**35%**	**17%**
Conducts penetration testing	**41%**	**27%**
Employs a Chief Information Security Officer (CISO) or Chief Security Officer(CSO)	**46%**	**35%**

Additionally, the increasingly competitive deregulated environment has also meant that companies need to focus on operational efficiencies and cost-savings. The increasing number of mergers and acquisitions requires that the security infrastructure be scalable and flexible to support the unpredictable business environment. The streamlining of security management processes and technologies and the creating of robust security frameworks should therefore receive renewed attention.

16. LIST OF FIGURES

17. LIST OF TABLES

18. ACRONYMS AND ABBREVIATIONS

AGA	American Gas Association
AIChE	American Institute of Chemical Engineers
API	American Petroleum Institute
COBIT	Control Objectives for Information and related Technology
CCPS	Center for Chemical Process Safety
CIDX	Chemical Industry Data Exchange
CMU	Carnegie Mellon University
CSVA	Cyber Security Vulnerability Assessment
DCS	Distributed Control System
DHS	Department of Homeland Security
HMI	Human Machine Interface
I3P	Institute for Information Infrastructure Protection
IAM	InfoSec Assessment Methodology
IEC	International Engineering Consortium
IED	Intelligent Electronic Device
IP	Internet Protocol
IS	Information Security
ISA	Instrumentation, Systems and Automation Society
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Standard for Organization
ISP	Internet Service Provider
IT	Information technology
ITGI	IT Governance Institute
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
MMI	Man Machine Interface
MTU	Master Terminal Unit
NIST	National Institute of Standards and Technology
NPRA	National Petrochemical & Refiners Association

NTFS	New Technology File System
O&G	Oil and Gas sector
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PCN	Process Control Network
PCS	Process Control System
PLC	Programmable Logic Controller
ROI	Return on Investment
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SVA	Security Vulnerability Assessment
VAM-CF	Vulnerability Assessment Methodology for Chemical Facilities
WAN	Wide Area Network

19. References

http://www.computersecuritynow.com/

http://www.gammassl.co.uk/bs7799/

http://www.dnv.com/certification/

www.mitsue.co.jp

http://17799.denialinfo.com/

http://www.iwar.org.uk/comsec

www.aga.org

www.securityfocus.com

www.ins.com

www.iso.org

http://csrc.nist.gov

www.cert.org

http://api-ep.api.org

http://www.gtiservices.org

www.sans.org

http://www.gammassl.co.uk/bs7799/works.html

http://www.gammassl.co.uk/bs7799/history.html

http://www.ukas.com/information_centre/technical/technical_bs7799.asp

http://enterprisesecurity.symantec.com/industry/

http://praxiom.com/iso-17799-2000.htm

http://www.informationstandards.com/

http://www.tech-faq.com/bs7799.shtml

http://www.itgovernance.co.uk/page.bs7799

www.rusecure.co.uk

http://17799-news.the-hamster.com/issue05-news9.htm

www.csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf

http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

http://www.gammassl.co.uk/bs7799/works.html

http://www.csrc.nist.gov/policies/FISMA-final.pdf

http://www.itil.co.uk/

http://www.ogc.gov.uk/index.asp?id=2261

www.tuv-acchi.cl

www.network-and-it-security-policies.com

http://www.us-cert.gov/control_systems/

www.information-security-policies.com

www.centerforsecuritypolicy.org

http://www.digitalbond.com/SCADA_Blog/2004/08/api-1164.html

http://www.digitalbond.com/SCADA_security/AGA%2012.htm

http://www.sandia.gov/iorta/docs/SAND2003-
1772C_Common_Vulnerabilities_CI_Control1.pdf

http://www.responsiblecaretoolkit.com/