Security Measures for Computer Networks in
Large-Scale Industrial Facilities

Preparing Vital Systems to Deal with Cyber-Terrorism and System
Cracking

March 1998

Interim Report

Ministry of International Trade and Industry

Large-Scale Plant Network Security Committee
# Table of Contents

**Introduction** .................................................................................................................................................. 1

**Prologue: Background and Summary of Studies** ......................................................................................... 8
1. From Control Systems to Large-Scale Plant Networks ........................................................................... 9
2. Objectives of This Committee .................................................................................................................. 18
3. Study Areas of Subcommittees ................................................................................................................ 19

**Chapter 1: Current Status and Future Potential of Cyber-Terrorism and "Cracking"** ................................. 22
1.1 Overseas Cases of Cyber-Terrorism and Cracking .............................................................................. 23
1.2 Cases in Japan of Cyber-Terrorism and Cracking ............................................................................... 25
1.3 Anticipated Future Threats ................................................................................................................... 27

**Chapter 2: Current State of Plant Networks** ............................................................................................ 30
2.1 Overview of System Configuration Models .......................................................................................... 30
2.2 Current Security Measures of Companies in Japan and Evaluations .............................................. 32
2.3 State of Affairs in the U.S. and Evaluations ......................................................................................... 38

**Chapter 3: Urgently Needed Measures to Prevent Cyber-Terrorism and "Cracking"** ................................. 40
3.1 Establishment of Security Policies ....................................................................................................... 40
3.2 Threat Analysis Using HAZOP and FTA ............................................................................................. 43
3.3 Threat Analysis by Route of intrusion ................................................................................................. 53
3.4 Security Measures by Route of Intrusion ............................................................................................ 71

**Chapter 4: Proposals to Reinforce Security** ............................................................................................. 82
4.1 Institution of Plant Security Guidelines ............................................................................................... 82
4.2 Development of Methodologies for Analysis of Threats to Network Security ..................................... 85
4.3 Research and Development of Preventive Technologies .................................................................... 85
4.4 Publicity and Education on Network Security ..................................................................................... 87
4.5 Summary ................................................................................................................................................ 88

**In Conclusion** .............................................................................................................................................. 90

**:Attached Materials**

* Glossary ...................................................................................................................................................... 92
Security Measures for Computer Networks in Large-Scale Industrial Facilities: Preparing Vital Systems to Deal with Cyber-Terrorism and System Cracking

Introduction

Advances in information technology in recent years have been accompanied by a growing dependence, in many areas of economic and social activity, on computer networks and systems. As a result, stoppages or failings of the functions of computer networks have serious consequences not only for economic activity, but for many other aspects of the lives of citizens. More recently there has been a growing awareness of threats posed by actions via networks which are hostile to governments and industry--acts of so-called "cyber-terrorism." Hence in order to ensure the smooth functioning of the advanced information-based society of the future, sufficient measures must be implemented to ensure the security of computer networks and systems.

Among other areas of computer network security, studies have already begun on measures for security of electronic authentication, electronic payment and other electronic commercial transaction systems. However, to date there has not been sufficient consideration paid to issues of security in the computer and network systems of large-scale plants and other industrial facilities. Yet problems of network security in large-scale plants can be said to be an area of system security, of vital importance to society, which requires urgent study. As a result of advances in network technology in the last several years, there has arisen the possibility of a decisive competitive advantage of firms capable of exploiting such technology over firms which cannot. Because of this, there has been a rush to connect enterprise systems to open networks. But in promoting such open systems, if there has been inadequate study of the security issues
related to connection with outside networks, then systems may be vulnerable to willful attacks by outside parties—what has been called "cyber-terrorism." And even closed systems may be invaded by malicious code during software maintenance or on other occasions, so that risks cannot be entirely discounted.

In light of this situation, in September 1997 the Ministry of International Trade and Industry established a Large-Scale Plant Network Security Committee (chairman: Tomio Umeda, professor, Department of Project Management, Chiba Institute of Technology), which assembled experts from various fields to study approaches to dealing with cyber-terrorism and system cracking in the large-scale and wide-ranging socio-economic infrastructure. This committee is the first instance of an assembly of persons from user, vendor and engineering firms for computer systems and networks in such energy- and manufacturing-related fields as petroleum refining, petrochemicals, electric power, steel, and paper & pulp. Studies were conducted on security measures for large-scale plant networks, and the results were summarized in an interim report, completed in February 1998, which made proposals for technologies and system operation necessary to deal with the threat of cyber-terrorism.

I believe there is great significance in the results of the committee's studies, including the adoption of security standards for large-scale plant networks, development of methods for analyzing the risks posed by different intrusion routes, development of encryption and authentication techniques for plants and facilities, examine through mock attack test, and the clarification of specific problems for system operation and management during remote maintenance and wireless LAN use. I am confident that this interim report will be useful to companies as guidelines or a kind of manual for ensuring the security of large plant networks; but these study results are similarly applicable to general-purpose computer networks and systems. They should also be of
interest to persons studying network security measures for systems used in financial settlement, airway control, railway operation, disaster prevention, maintenance of public order, and defense.

Finally, I would like to thank all the committee members for their unstinting efforts in conducting studies on countermeasures to cyber-terrorism and system cracking, as well as those persons at the Japan Users Association of Information Systems who served in administrative capacities. In addition to thanking these persons, I hope to receive their continuing support and cooperation.

March 1998

Machinery and Information Industries Bureau

Katsusada Hirose
Schedule

The initial meeting was held on September 2, 1997; thereafter eight meetings were held by the end of January of the following year, at intervals of about three weeks.

Summaries of the meetings follow.

First Meeting: September 2 (Tues)
"The Threat of Cyber-Terrorism to Vital Facilities"
"Approaches to Security Measures for Plant Control Systems"
"Current Status of Oil Refining Systems from a Security Standpoint"
"Cases of Requests for Security at Overseas Plants"

Second Meeting: September 19 (Fri)

Third Meeting: September 30 (Tues)
"Current State of Security Measures in U.S. Power Control Systems"
"Cyber-Terrorism Countermeasures in the U.S."
"Current Status of Networks and Security in Japanese Oil Companies"
"Current Status of Networks and Security in Japanese Paper Companies"
"Current Status of Networks and Security in Japanese Chemical Companies"
"Current Status of Networks and Security in Japanese Electric Power Companies"
"Current Status of Networks and Security in Japanese Steel Companies"
"Current Status of Networks and Security in Japanese Telecommunication Companies"
"Recent Trends in Unauthorized Access and Viruses in Japan"

Fourth Meeting: October 17 (Fri)
"Current Status of Security Measures by Control System Vendors in Japan"
"Current Status of Security Measures by Plant Engineering Firms in Japan"
"On Security Management"

Fifth Meeting: November 5 (Wed)
"On the Future Direction of the User Company Subcommittee"
"On the Future Direction of the Vendor Company Subcommittee"
"On the Future Direction of the Engineering Company Subcommittee"
"Report by a U.S. Committee for Protection of Vital Infrastructure"

Sixth Meeting: November 20 (Thurs)

Seventh Meeting: December 11 (Thurs)

Eighth Meeting: January 27 (Tues)

"Establishment of Security Policies by Users and Studies of Operation and Management Standards"
"Analysis of Anticipated Threats and Intrusion Routes in Control Systems"
"Study of Necessary Technology and Operation Countermeasures for each Network Intrusion Routes"
"Analysis of Communication Difficulties Using the HAZOP Procedure"
"Future Areas for Study and Proposals"
Committee Members

Chairman:

Tomio Umeda, professor, Department of Project Management, Chiba Institute of Technology (process systems engineering); chairman, Management Information Committee, The Japan Petroleum Institute

Subcommittees:

User Company Subcommittee

13 members

Vendor Company Subcommittee

10 members

Engineering Company Subcommittee

6 members

Observers:

Shin Yasunobe, manager, Information Processing Promotion Section, Machinery and Information Industries Bureau, MITI

Masaaki Kobashi, head of Information Security Policy Office, Machinery and Information Industries Bureau, MITI

Hiroshi Suzuki, assistant manager, Information Processing Promotion Section, Machinery and Information Industries Bureau, MITI

Kenichiro Mukai, assistant manager, Information Processing Promotion Section, Machinery and Information Industries Bureau, MITI
Hiroshi Sawano, officer in charge of safety guidance, Information Processing Promotion Section, Machinery and Information Industries Bureau, MITI

Executive Office:
Kazuo Okuda, managing director, Japan Users Association of Information Systems
Kingo Iketani, manager in charge of planning, Japan Users Association of Information Systems
Chiharu Tsunoda, manager in charge of surveys and public relations, Japan Users Association of Information Systems
Kayo Hirata, in charge of surveys and public relations, Japan Users Association of Information Systems
(titles omitted)
Prologue: Background and Summary of Studies

With recent advances in information technologies, we have come to rely increasingly on computer networks and systems for improved productivity and greater efficiency in many socioeconomic areas. Because of this, stoppage or disturbance of the functions of computer networks can have grave effects on all aspects not only of economic activity, but of the lives of citizens as well. Thus it is essential for the future well-being of our society, based as it will be on sophisticated information and communication technologies, that adequate security measures be devised to counter "cyber-terrorism" and other threats.

The information systems\(^1\) and control systems\(^2\) which comprise the computer network systems in industrial facilities have been gradually extended, from individual isolated computers to closed networks using dedicated communication lines and protocols, and thence to interconnectable "open" systems using standard protocols. With respect to network security measures for information systems, there is already an "Standard Countermeasures to Unauthorized Computer Access" (11/15/96) and other guide lines. Hence this committee primarily addressed control systems in studying measures to ensure network security, and particularly countermeasures to system "cracking."

In conducting this study, a model was adopted based on control systems used in energy and manufacturing industries. However, we believe that the study results of this committee can be applied to the cases of other industries as well, in dealing with control and other systems which have ordinarily existed independently of general open-type information systems, but in which

---

\(^1\) Information system: Used for processing relating to the accounting, personnel, sales and other activities of a company.

\(^2\) Control system: Used primarily to process data for controlling facilities and equipment.
interconnection is expected to proceed apace. Such industries include finance, air control, railway operation, disaster prevention, public safety, and defense.

1. From Control Systems to Large-Scale Plant Networks

In the past, the control systems used in plants have been independent, closed systems; but recently there have been movements to interconnect multiple control systems, and to connect them to information systems both within and outside the company, to form a large-scale hierarchical network. Figure 1 is a model of the system configuration of such a large-scale plant network. In this committee, experts and learned persons from various fields have conducted deliberations based on the model diagram shown below.
Figure 1. Model of the system configuration of large-scale plant networks

Explanation of Figure 1

System configurations and names will differ with the industry and the company. The model serving as the basis for discussion was modified a number of times, upon agreement by the committee members.

[1] Control System

"Plant" refers to production equipment; where oil, chemicals, water, fuel, gas or other fluids are handled, control equipment known as a distributed control system (DCS) is used for control.

The DCS is based on a controller, which directly controls the production equipment ("plant site" in the figure), and consoles used by operators to monitor and operate plant equipment. It also includes an engineering console for engineering support, and a gateway used for data exchange between the DCS and a higher-level system.

As a consequence of system design policy and in accordance with the plant scale, plant site location, applications and other factors, several controllers may be used and may be in a distributed layout; for this reason the system is called a "distributed control system".

Controllers read electric signals (measurements) from production equipment (sensors) corresponding to flow rates, temperatures, pressures, and other physical quantities, and send other electric signals (output) to valves and other operation terminals in the plant to control equipment according to the control logic.

Consoles display various kinds of information necessary for operation, monitoring and manual control on a graphic screen which indicates the plant
operating state. The screens are designed for intuitive operation. For reasons of plant scale and ease of operation, multiple consoles are used, connected by a Control System LAN.

The network within the DCS is called a Control System LAN. Control information flows in this LAN, and so it must meet requirements for speed (responsiveness) and reliability. Vendors meet these requirements through redundant configurations and by using protocols proprietary to the vendor rather than TCP/IP.

Above the DCS is a process computer which handles production information (planning and management), manufacturing information (recipes) and achievement information (as a data server). In the past, process computers have been dedicated systems based on a minicomputer; more recently, servers which use UNIX or WindowsNT as the operating system have been employed. Multiple process computers may be used, depending on the plant scale and operating conditions.

Recently, computers ("EWS" in the figure) have also been added which are capable of multivariate forecasting and control and other sophisticated control, which was not possible using previous control equipment, and able to analyze the causes of disorders.

On the right side of the figure, "PLC" stands for programmable logic controller. Whereas the DCS mainly handles analog value, the PLC is principally concerned with digital signals (on/off signals); because it is programmed in a language used for control procedures (sequences), it is also called a sequencer. PLCs are frequently used in machining and assembly industries (automobiles, electric equipment, etc.), but are also used to handle solid products in process industries.
The Control System Information LAN connects the DCS and process computer. Because the computers and equipment of different manufacturers must be connected, Ethernet has been used. This LAN carries data which, while not used for control, is directly related to production; and in some cases it connects plants the control range of which extends to multiple plants. Hence this LAN transmits information necessary to the control system, and so as a name describing its function, it is called a Control System Information LAN.

Other systems which fall within the definition of "control systems" include gateways for connection to the DCS of other plants, and wireless communication systems used for equipment inspections, site information collection, and other site patrol tasks. There are also external dialup connections for remote maintenance, used to perform services to maintain computers and equipment within the control system from a remote site at the vendor's location.

All equipment below the process computer is thus referred to collectively as the control system, and is considered to be the main object for protection by the security measures studied by this committee. Especially detailed studies were conducted on the consoles which are the core of plant operation and the controllers which output direct control data.

[2] Information System

The information system is shown in a form which is typical for manufacturing industries. The Information system LAN serves as the backbone of the network within the plant; to it are connected equipment management systems, office systems and other subsystems. In some cases, the networks for these subsystems extend to instrumentation or control rooms in which the DCS is installed, where operators may make use of them. In the case of small-scale systems, PCs for office use may be connected to the Control System Information
LAN, so that the LAN is shared with the office system; and in some cases the Information system LAN and the Control System Information LAN are not separated.

In some cases the Information System of Factory may be connected to public communication circuits or the Internet for the purpose of exchanging data on materials, products or other matters with outside companies. The Information System of Factory is connected with enterprise-wide systems including the main office via a WAN.

Each companies build systems in which necessary functions are added as the need arises. As a result, these have typically grown into enormous systems which directly link production and information, with DCS and plants existing as components.

(1) History of Control Systems

Among the large-scale computer network systems in electric power, oil, gas, transport, finance, telecommunications and other fields which are directly linked to the lives and welfare of citizens, information networks used primarily for clerical tasks are rapidly being opened up to broad access.

On the other hand, the control systems used in the operation and control of plants and other facilities have in the past normally been based on proprietary systems, used in an environment isolated from external systems. Compared with control systems, the plant service lifetime is relatively long, and so the three generations of control systems described in the table below coexist. However, as explained below, it is only a matter of time before a more "open" design is adopted in this area as well.
Table 1 Transitions in control systems

<table>
<thead>
<tr>
<th>Generation</th>
<th>Period</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First generation</td>
<td>1970's to late 1980's</td>
<td>• Both consoles and controllers use the vendor's proprietary OS. • Communication between control system and information system used low circuit capacity; for example, point to point connections using PIO transfers and RS232C synchronous transfers. Data exchange and other communication protocols in the application layer were either vendor-specific or were determined upon each connection.</td>
</tr>
<tr>
<td>Second generation</td>
<td>Late 1980's to early 1990's</td>
<td>• Consoles mainly ran on UNIX; controllers used the vendor's proprietary OS. • In the 1990's, systems with the configuration shown in Fig. 1 emerged. However, Ethernet connections were limited to just a few Information system LANs and Control System Information LANs, PC networks were not yet widespread, and there were almost no &quot;open&quot; connections with the Internet or other outside entities. Control System LANs adopted communication protocols specific to the vendor. • Persons well-versed in UNIX versions and in the TCP/IP protocols were capable of intrusion up to consoles. However, cracking of controllers was not possible without adequate knowledge of the plant's control system architecture.</td>
</tr>
<tr>
<td>Third generation</td>
<td>Late 1990's (recent systems)</td>
<td>• Consoles run on open OSes such as UNIX and WindowsNT. Controllers use proprietary OSes. • Systems are being made more open by exploiting the networking features of open OSes. • Persons with extensive knowledge of the networking features of open OSes can intrude as far as consoles with relative ease; with the spread of networks both within and outside companies, including PCs, the threat of system &quot;cracking&quot; is growing.</td>
</tr>
</tbody>
</table>

In the past, plant control systems, typified by DCS, have been computer systems predicated on the assumption of a vendor-specific control network. This was both because a proprietary protocol was needed to ensure
responsiveness, given that process control was a special application, and
because of the need for redundancy in the system configuration, in order to
ensure network reliability (avoid system down time). For these reasons, open
OSes were not employed.

When DCS systems were developed 20 years ago, limitations on
communication capacity meant there was little data exchange between control
systems and higher-level information systems. Recently, however, more tightly-
woven intercommunication as typified by integration of production and sales
activities has come into demand as a result of the need for faster data flow,
improved efficiency and reduced manpower requirements. In addition, slowing
economic growth has produced demands for reduced expenditures on new
control systems, maintenance and management, as investments in plant
equipment have themselves fallen off. For these reasons there has been less
financial latitude for the construction of dedicated redundant systems. On the
engineering side, with recent advances in computer and network technologies,
open OSes have acquired sufficient functionality to enable use in control
systems as well.

For all these reasons, control systems have moved from the proprietary
high-reliability systems of the past to DCS systems adopting open OSes. And,
they have come to be connected closely with production management servers
and enterprise-wide systems.

However, the use of open OSes in such control systems has purchased
improved cost-performance and greater convenience at the price of potential
security risks: individuals with sufficient knowledge of the open OS may be
able to gain intrude to the control system.
(2) Prospects for Distributed and Open-Architecture Control Systems

At present open-protocol networks are used in Control System Information LANs, and PCs running on open OSes are also coming to be used as the consoles which govern plant operation and monitoring. This trend is expected to accelerate in future.

On considering trends in customer requests accompanying plant construction overseas, in addition to the construction of control systems, there are also cases which include construction of an information system intended to govern all basic corporate activities, such as management, personnel, accounting, sales, and production management. Such cases reveal a need among users for connection of information systems with process computers and DCS systems via networks, to utilize a wide range of data for production planning, cost accounting, energy management and other activities.

Hence future trends in control systems may be summarized as follows.
Table 2 Future trends in control systems

<table>
<thead>
<tr>
<th>Connections with enterprise-level information systems</th>
<th>Application of ERP (enterprise resource planning)(^1) packages, sharing of information with existing information systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection with plant information systems; faster operation, distributed architectures, integration</td>
<td>Application of PIMS (plant information management systems)(^2)</td>
</tr>
<tr>
<td>Open architectures</td>
<td>Adoption of general-purpose technologies (field buses, TCP/IP)</td>
</tr>
<tr>
<td>General-purpose components</td>
<td>Shift from proprietary OSes to open OSes</td>
</tr>
</tbody>
</table>

As another factor intensifying these trends, recently the ISA (International Society for Measurement and Control) formed an Enterprise-Control System Integration committee for the purpose of creating standards related to instrumentation and control. The ISA committee plans to adopt a business model which emphasizes the control domain and establish standards for the details of system functions in each area, input/output specifications for each domain, terminology and other matters.

2. Objectives of This Committee

In order for a "malicious intruder" to be able to inflict critical damage on a large-scale plant through a network, special knowledge relating to the plant is

\(^1\) ERP (Enterprise Resource Planning): Information systems created primarily with the objective of integrating enterprise-wide activities. The salient characteristic of such systems is the shared use throughout the company of data specific to each area or activity. Recently such systems have been commercialized as ERP packages.

\(^2\) PIMS (Plant Information Management Systems): Information systems which perform integrated management and processing of information related to plant construction and operation, production management, laboratory systems, inventory management, shipments, and maintenance.
necessary. Hence at the present time this danger is thought to be minimal, but in the near future it is clear that such threats will appear.

In particular, we cannot disregard the possibility of explosions, stoppages and other incidents and malfunctions at plants resulting from the destruction or falsification of the OS, application software, data or other components by a malicious intruder, particularly given that such large-scale plant networks represent infrastructure of vital interest to society, and from which high reliability is required.

Based on an awareness of the foregoing problems, this committee has studied approaches to security measures intended to protect large-scale corporate computer network systems from "cyber-terrorism" (hostile acts committed against governments and industry through networks, and other attacks perpetrated by malicious intruders), in accordance with the needs of the petroleum refining, petrochemical, electric power, steel, pulp and paper, and other industries. The purpose of the committee's activities is to make proposals regarding technologies necessary to counter threats to such systems from outside, the preparation of security measures for system operation, and the development of new technologies.

3. Study Areas of Subcommittees

Each committee member was assigned to one of three subcommittees--the User Company, Engineering Company, or Vendor Company subcommittee--based on his experience in planning, designing, developing, constructing or operating control systems, for the purpose of sharing related knowledge and promoting the lively exchange of opinions. In addition, persons knowledgeable in network security issues dispersed to participate in the studies of each of the subcommittees.
(1) User Company Subcommittee

In order to promote discussions by the entire committee on a common basis, this subcommittee established a model system configuration (cf. Fig. 1 above) closely approximating the configuration of systems currently in actual use at user companies within Japan, and also attempted to define consistent terminology (see the appendix) in order to expedite mutual understanding among committee members, including more detailed matters. Following this, a list of areas requiring prevention against threats both internal and external (elucidation of security policy) was created. In addition, issues of operation management expected to become essential for users in future, as well as requests to vendor and engineering companies, were also examined.

(2) Engineering Company Subcommittee

This subcommittee was charged with the task of analyzing network security risks in control systems, as one aspect of plant design engineering. Another task was to establish the flow of process security engineering, and to attempt to apply HAZOP, FTA, JRAM and other plant risk analysis techniques to the analysis of network security risks (cf. Fig. 2 below).

---

1 HAZOP (Hazard and Operability Studies): A technique for evaluating plant (chemical process) safety. A deviation from design concepts is supposed, and the cause of the deviation and its effects are studied, as a means of examining the appropriateness of safety measures. HAZOP is executed by a team of specialists.

2 FTA (Fault Tree Analysis): The nature of the malfunction or accident and its causes are assumed, and a tree-structure diagram describing the causal relations between the phenomenon and its causes is created. Through qualitative and quantitative analysis of occurrence of top-level phenomena, the phenomenon in question is averted.

3 JRAM (Jipdec Risk Analysis Method): A technique for analyzing actual system risks through FTA, and at the same time using JRAM questionnaires to collate and evaluate subjective assessments of risk by responsible persons in units using the system, combining both in a comprehensive report. This method
(3) Vendor Company Subcommittee

This subcommittee analyzed the relation between methods of intrusion from outside, and security violations. FTA was used to analyze threats by different intrusion routes, and security measures were proposed for different intrusion routes requiring immediate action. Proposals were also made regarding development of new security technologies expected to be necessary in future.

was developed in 1984 by JIPDEC (Japan Information Processing Development Center).
Chapter 1: Current Status and Future Potential of Cyber-Terrorism and "Cracking"

"Cracking" is a term used to refer to attempts at access with malice to a computer network system without obtaining proper authentication. "Cyber-terrorism" refers to hostile acts directed at governments and industry via networks, with attempts at large-scale and organized unauthorized access. American specialists have defined cyber-terrorism as a "global information war"; the aim is to intrude the computer network systems used in areas such as government, finance, air traffic control and electric power, in order to induce malfunctions, shutdown and destruction of the system itself as well as to illegally acquire or falsify important documents or to inject viruses, with political or economic motives.

The following are threats relating to computer security. In light of recent trends toward increased cyber-terrorism, redoubled efforts to thwart purposeful threats will be needed.

• Threats of natural disasters: Damage caused by fires, lightning, earthquakes, flooding, other events
• Threats due to chance events: Damage due to human actions such as erroneous operation or software bugs
• Intentional threats: Damage caused by industrial spies, terrorists, criminals, " crackers," "hackers"¹

The objectives of persons in this last category may be broadly categorized as follows.

¹ Hackers: Refers to persons with deep knowledge of the internal logics of computer network systems; normally distinguished from " crackers" and "cracking."
(1) To overthrow the government or cause social disorder
(2) For monetary gain through intimidation or blackmail
(3) For business purposes, as in the case of industrial spies
(4) For revenge, motivated by enmity
(5) For recreation  (to obtain a sense of achievement or superiority)

1.1 Overseas Cases of Cyber-Terrorism and Cracking

Even abroad, there are not yet so many cases of what could clearly be defined as cyber-terrorism. However, in locations around the world there have occurred instances of intrusion, eavesdropping, data falsification and other events targeting the computer systems of governments, corporations, research laboratories and universities. Among these, the following may be cited as examples of cyber-terrorism.

(1) Intrusion into U.S. Air Force's Rome Laboratory

In March 1994, a 16-year-old British boy and a second unknown assailant launched over 150 attacks against 30 computers over a period of 26 days, from Internet sites at ten locations in eight countries. The details of the damage suffered are a military secret, but in addition to the theft of important information, the Rome Laboratory facilities were used as a springboard for further attacks on systems at various important U.S. military installations, NASA, NATO headquarters, and NATO High Command for Europe.

(2) Intrusion of Citibank Computers and Movement of Funds

In June 1994, a Russian group intruded Citibank's cash management system at least 40 times. An Argentine investment firm discovered that its funds
had been transferred from its Citibank account to an unknown account in San Francisco. In fact, Citibank had been investigating similar occurrences of intrusion for more than one year. One member of the group was arrested in Great Britain, and another in Russia.

(3) Theft of $500 Million by Cyber-Terrorists from Banks in the U.S., U.K., Other Countries

According to an issue of the British Sun-Times newspaper for June 1996, European and American financial institutions have paid approximately $500 million to cyber-terrorists since 1993 in response to threats. Terrorists had intruded the computer systems of financial institutions more than 40 times over the three-year period. The paper reports that nearly all banks prefer to handle such matters internally in a desperate effort to avoid publication of such affairs, and that almost none reported the incidents to the police.

(4) Intrusion of U.S. Military Computer Systems

On February 25, 1998, the deputy defense secretary of the U.S. Department of Defense announced that American military computers had been intrude from outside a number of times over the previous two weeks. The compromised computers were unclassified systems containing personnel and payroll records for the army, navy and air force; there was no loss of classified information.

There have not yet been any reported cases of cyberterrorist attacks on large-scale plants. However, U.S. power utilities fear that crackers and discontented parties may try to intrude energy management systems and power grid control systems via phone lines or wireless channels, in order to falsify
data and cause power outages and other problems. There is also a growing awareness of the threat posed by system cracking with a profit motive, in which power systems are intentionally disrupted or crippled in order to induce a huge demand for power-related stocks and other products carried by financial brokers.

An appendix introduces some U.S. publications which classify the features of crackers, criminals (spies, swindlers, system abusers), disruptive elements (both outsiders and system users) and other unlawful elements and organizations according to the nature of attacks, operation used, actions, and resources. There are also publications which summarize attackers by types of attack, methods of detection, and records to be used as evidence of attacks (see Reference Material 5: "Features of Criminal Organizations" and Reference Material 6: "Methods for Detection of Attacks").

1.2 Cases in Japan of Cyber-Terrorism and Cracking

As examples of phenomena in Japan attributed to cyber-terrorism, there have been cases of intrusion the systems of major corporations by a religious organization. Apart from cyber-terrorism, there have also been reports of attempts to intrude organizations starting from companies and network service providers with inadequate security measures, in order to sell commercial secrets to rival companies, as well as instances of shutdown of financial securities systems and railway operation systems. It cannot be denied that similar occurrences in future may result from cyber-terrorist acts.

In information systems, there has been an increase in the number of incidents of attacks on computers connected via networks (the number of cases brought for consultation to JPCERT/CC, an organization for emergency response to unauthorized computer access, increased from 61 to 107 and then to 122 cases in successive three-month periods beginning April 1, 1997), as well as increasing
damages sustained by computer viruses (with the number of incidents reported to the IPA (Information Technology Promotion Agency, which receives reports of damages) increasing from 755 in 1996 to 2391 in 1997). Moreover, incidents are tending toward greater maliciousness and criminality.

Major instances of "cracking" within Japan are as follows.

(1) Fund movements within Tokai Bank

In 1995, an employee of Tokai Bank and two computer operators together intruded a cash management system and unlawfully transferred approx. 140 million yen.

(2) Intrusion of Service Provider (Oita prefecture)

In April 1996, an unknown person or persons gained intrusion into the system of a service provider in Oita prefecture, stealing the passwords of some 2000 members and corrupting personal data and system information.

(3) sendmail Attack Incident

From December 1996 to January 1997, attacks targeting a security hole in the "sendmail" e-mail transfer program occurred at well over one hundred sites in Japan in a short period of time. There was no damage to sites where the security hole was removed, but password files at a number of sites were stolen.

(4) E-mail Bombings

Around April 1997, several hundred e-mail messages were sent to multiple sites by an unknown person, paralyzing computer systems.

(5) httpd Attack Incident
Around June 1997, there was a spate of attacks on a security hole in http (Hypertext Transfer Protocol Daemon). Passwords were stolen from computers which did not deal with the security hole.

(6) Other Recent Incidents

• Malicious data submitted to a government organization was not checked, and so appeared on that organization's web site.

• Business-use account names\(^1\), not protected by passwords, were used to send falsified e-mail as if from a service provider or computer communication firm (on a certain public facility network).

• A security hole in an NIS (Network Information Service) was intrude, and used to access international circuits to the U.S. for 17 minutes (on the laboratory network at a university).

• A MITI mail server was used as the intermediary for junk e-mail.

1.3 Anticipated Future Threats

If adequate measures are taken to reinforce management, then systems will remain relatively safe even as they are made more open. But if they are opened up without any security measures in place, then latent threats may emerge as actual menaces. For example, a person with specialized knowledge of plants may be able to intrude the control system of an energy plant, falsify management programs and data, and bring about serious disorder. If valves, pumps, compressors and other equipment are operated erroneously, plant shutdowns and misconnections may result.

---

\(^1\) Account names: Identifiers assigned to individual users of a system in order to identify them unambiguously. Also often referred to as login names, user names, or user IDs.
The following are conceivable latent threats to control systems.

(1) Unauthorized Acquisition of Confidential Information

There is the danger that unauthorized persons may gain intrude to a system and acquire confidential information unlawfully.

(2) Loss of Integrity or Reliability

Unauthorized updates of database information may cause errors in processing using the database. If certain data is unauthorized updated or falsified, abnormal operation may result in oil refining and chemical plants, with potentially serious consequences.

(3) Loss of Credibility

When exchanging data over a network, there may be concern that data has been falsified, or there may be some question as to whether data has actually been transmitted or received. There may be anomalies in which, for example, the quantities of production orders have been modified. Such occurrences may cause confusion in daily production activities, lead to marked declines in quality, and induce malfunctions in systems and equipment.

(4) Loss of System or Network Availability

Systems and networks must always be operated stably and under the conditions for which they were designed. If an abnormal quantity of data, exceeding design capacity, is transmitted over the network, communication failures or dramatic declines in responsiveness may occur. In systems where realtime control is required, control lapses may result.
The twisted-pair cables, microwave and satellite communications used in networks are susceptible to wiretapping; radio waves can easily be received by installing antennas, making them highly problematic from the standpoint of security.

Further, the information flowing in networks is transmitted and received as plain text in a format conforming to the communication protocol. Passwords, account names, and other confidential information is likewise transmitted over the network as ordinary data. If such data is intercepted, it becomes a simple matter for a third party intrude into the system.

The above threats are even today options, in theory, for cyber-terrorists. Hence there is a pressing need to conduct studies beginning with areas where measures to combat cyber-terrorism and other threats are viable.
Chapter 2: Current State of Plant Networks

2.1 Overview of System Configuration Models

A model was instituted with reference to the actual system configurations of user companies within Japan, in order to enable the members of this committee, with their various backgrounds, to be able to enter into deliberations using a common terminology and shared concepts.
Figure 1. Model of the system configuration of large-scale plant networks (also presented earlier).
2.2 Current Security Measures of Companies in Japan and Evaluations

Below, the actual security measures currently adopted by eleven user companies in Japan are summarized. Company networks adopt security measures to prevent intrusion from outside not only into control systems, but into the system as a whole. For example, only communications based on specified rules are allowed in connections with outside entities. But in all cases, companies are aware that as systems become more open, such measures will be inadequate to prevent intrusion with malicious intent by cyber-terrorists. Moreover, no one company is implementing all of the measures described below. And, there are few instances of a company adopting measures systematically according to a well-defined security policy.

(1) Security Measures in System Construction

Measures targeting connections between information systems and external entities are as follows. (cf. Fig. 1)

Table 3

<p>| Internet •Limit the number of points of connection (for example, one connection point at the main office) •Specify an Information system LAN for connection points within business locations •Specify terminals at which Internet use is possible Use firewalls to control access (protocol limitations etc.) authentication functions to proxy servers |  |</p>
<table>
<thead>
<tr>
<th>Access to consoles (for vendor-specific protocols)</th>
<th>Watchdog timers are used for management (see Glossary) (infrequent)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Address information, account names and passwords are not disclosed, and are used to control login</td>
</tr>
<tr>
<td></td>
<td>• Unique commands are established for remote login, and use of these commands is limited</td>
</tr>
<tr>
<td></td>
<td>• Connection from the process computer is forbidden (infrequent)</td>
</tr>
<tr>
<td></td>
<td>• Changing of parameters except from a console is forbidden; a human operator must always be present (infrequent)</td>
</tr>
</tbody>
</table>
Access to controllers (for vendor-specific protocols)  
- DCS tag names are not disclosed, and login is controlled  
- Limiting values for control settings are established, and large changes in settings are forbidden

(2) Operation Security Measures

a. Security measures include, in addition to the features of system architecture described above, measures concerning system operation. Companies are adopting specific rules for access rights, methods for managing computers, data, passwords and documents, and procedures for security management and monitoring, with the label "operation management rules."

In addition, there are cases in which rules have been established relating to computer hardware management, including locking computer housings, prohibition of external computer hard disks, and locking passages to computer rooms; obligating the storage in fireproof safes of backup tapes; and obligating users to limit software usage and to run anti-virus software.

b. The User Company Subcommittee conducted a questionnaire survey, and has summarized the rate of implementation in large-scale plant networks of various standards for information systems (standards for safety measures for information systems; standards for measures to prevent unauthorized computer access; standards for measures regarding computer viruses; system monitoring standards). Questionnaire surveys were also conducted on unnecessary items and on items to be added; these results are described below in Chapter 4, together with recommendations.

The state of execution of standards for information security measures, as revealed by the questionnaire responses, is as indicated in the table below. Here any items which have been implemented by five or more companies (a
majority of the companies represented in the User Company Subcommittee) were tallied as "implemented."

Table 5. State of implementation of information security standards

<table>
<thead>
<tr>
<th>Safety measure standards</th>
<th>Measures to counter unauthorized access</th>
<th>Standards for anti-virus measures</th>
<th>System monitoring standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate of implementation (5 or more companies)</td>
<td>66.7% 128/192 items</td>
<td>58.0% 49/85 items</td>
<td>51.0% 25/49 items</td>
</tr>
</tbody>
</table>

(Overall):

The overall rate of implementation of safety standards was 67%; companies have implemented a relatively large number of safety measures.

(Installation standards):

Standards for installation of power supplies, fire/disaster prevention equipment, crime prevention equipment, air conditioning and other equipment have been implemented by a high 72% overall. However, monitoring of control rooms or consoles is at 0%; no companies have adopted these measures. In addition, earthquake-proofing measures for control rooms and console rooms are a low 45%.

(Engineering standards):

The rate of implementation of engineering standards for disaster prevention, malfunctions, and maintenance and operation support is a low 23%. In particular, measures to counter intentional or negligent acts (access control,
prevention of malicious data processing, prevention of information leaks etc.) is 0%, with almost no implementation whatsoever. Functions for coping with disasters are at a low 33%; but considering that three of these items were deemed unnecessary, the actual rate of implementation of necessary measures is close to 50%.

(Operation standards):

The rate of implementation of operation standards pertaining to data, systems, users, personnel management, outside consignment, and other matters is an extremely high 76%, indicating that care has been exercised in these areas. Of the measures in question, only measures related to entry into buildings and entry into rooms is lacking in implementation, at 14%.


The rate of implementation overall was 36%, but this rose to 58% if standards for external businesses are excluded. The figure for system user standards was 55%, and for system manager standards (for management of users, information, equipment, logs and other records), 55%. Hereafter it will be necessary to increase the awareness of system managers for the need for security standards. Issues include the establishment of security policies, prevention of information leaks over communication channels, adoption of functions for detecting falsification or modification, distribution of access control for important information, management of logs of system operation, security checks when introducing new equipment or software and when making connections with outside entities, collection and analysis of security information, and security education.

Standards for outside businesses were tallied as having been implemented if the company is providing guidance. However, the actual state of
implementation was 0% for network businesses and for hardware and software businesses.


The overall rate of implementation is 37%, but this rises to 51% if external businesses are excluded. The results for this area are closely similar to those for standards to prevent unauthorized access. Rates of implementation for user system standards and system manager standards were nearly the same, at 50% and 52% respectively. The rate for software provider standards was just 5%. Following occurrence of an event, make clear of causes and actions to prevent reoccurrences are comparatively satisfactory; but no measures are taken to perform inspections using the latest vaccines or to monitor system operation.

[4] System Monitoring Standards

The overall rate of implementation was 66%. Of this, the rate for operation tasks was a low 32% (whereas rates for monitoring of planning and development tasks are high, above 90%). However, as many as nine measures related to operation tasks were deemed unnecessary; if these are excluded, the rate is 40%. Issues include information security education and training; control and monitoring of database access; network management, monitoring, and analysis of usage records; prevention of unauthorized access at consignment contractor sites; and understanding of the state of execution of measures to protect confidential information.

(3) Security Measures in the Development, Design, Manufacture, and Construction of Control Systems
At vendor sites, the following security measures are being implemented in product development environments.

- Security measures are being taken with respect to development areas, document management, software management, and communication management.
- Inspections for computer viruses are being performed either for each item, or on a random sampling basis. Only software products that have been verified are sold and delivered.

2.3 State of Affairs in the U.S. and Evaluations

The current state of security measures for electric power control systems in the U.S. was surveyed. For details see the attached Reference Material 2: “Status Quo of U.S. Electric Power Control Systems and Related Problems.”

The above report reveals that the control systems for plants, power generation systems and transformer substations are even more distributed and "open" in the U.S. than in Japan. There are also interconnections with energy management systems (EMS) and other public utility systems. And, relaxation of regulations for utilities, and policies for promotion of competition, are also having a major impact on the computer network systems of electric power companies. That is, the U.S. Federal Energy Regulatory Commission (FERC) has stipulated that information relating to the sale of electric power by public utilities be made public on the Internet. This means that crackers and viruses not only to individual systems, but also, through the Internet, to other interconnected systems, with the ultimate risk of crippling entire systems.

It has also become possible to set and modify protective relays at substations and control breakers through remote operations. Such remote control is desirable from the standpoint of convenience, but also carries the risk of intrusion by malcontents and crackers.
Hence discussions are considering the need to protect and isolate control systems from inappropriate Internet access, as well as the need to add information security functions to control systems centered on SCADA systems (Supervisory Control and Data Acquisition systems, control systems used by electric power, oil refining and other public utilities).

In addition, the President's Commission on Critical Infrastructure Protection, reporting directly to the President, was established on July 15, 1996 in order to study countermeasures to cyber-terrorism. This commission submitted a report to the president on October 20, 1997. The essence of this report is appended as Reference Material 3: "Report of the U.S. President's Commission on Critical Infrastructure Protection."
Chapter 3: Urgently Needed Measures to Prevent Cyber-Terrorism and Cracking

In the previous chapters, the current state of security measures at companies both within and outside Japan was considered, and it was shown that there is an awareness of the inadequacy of such measures to prevent malicious intrusion by cyber-terrorists as systems become more open in nature. This committee has therefore summarized the minimum measures that must be devised by companies to such ends, using only technologies now available. It is recommended that individual companies refer to the detailed measures described below and compare them with the status of measures implemented at each plant and facility. At present, however, there is a trade-off between security and convenience; moreover, there are limits to the costs, human resources and operating capacity that can be devoted to such efforts. Consequently it will likely be difficult or impossible to implement all the measures described below at once. Companies should however implement measures in succession beginning with the most easily executed items.

3.1 Establishment of Security Policies

The first step that should be taken in devising information security measures is to establish a security policy. In addition to clarifying to what extent computers within the organization can be shown, and to whom, as well as what information can be shown to outsiders, it is also necessary to elucidate and prioritize resources requiring protection against attacks by malicious intruders. If the resources to be protected and their ranking or priority are not clearly stated, then investments in security measures will balloon, and effective measures will become impractical.
As one example of a security policy, the User Company Subcommittee has designated three priority levels for items for protection in plants.

[1] Examples of items with greatest importance
• Valves must not be operated
• Tuning parameters must not be falsified
• Control settings and upper/lower limits must not be modified
• Control System LANs must not be disrupted
• Data files and control programs must not be modified, corrupted, or stolen

[2] Examples of items with intermediate importance
• Control System Information LANs must not be disrupted
• Process computer screens must not freeze
• Data files (quality, recipes etc.) must not be stolen
• Process data must not be stolen

[3] Examples of items with low importance
• Process computers must not be intrude
• Process computer operation data must not be stolen

The above are the items most frequently cited by companies; all items are listed in the table below.

Table 6. Example of security policy for a plant network

(Symbols in the Category column have the following meanings.
X: Networks and systems must not be intrude, there must be no unauthorized logins or access, no freezes or disruption of the system
Y: There must be no theft or reading of data or programs
Z: There must be no falsification, corruption or modification of data or programs, and no intervention into screens or operation.

In addition, priorities are, in decreasing order, 1, 2, 3.)

<table>
<thead>
<tr>
<th>No</th>
<th>Item/area for protection</th>
<th>Category</th>
<th>PRI</th>
<th>Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No disruption of Control System LAN</td>
<td>X</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>No accessing of Control System LAN</td>
<td>X</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>No virus intrusion</td>
<td>X</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>No remote logins to consoles</td>
<td>X</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>No freezing of console screens</td>
<td>X</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>No theft of control equipment data</td>
<td>Y</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>No theft of control programs</td>
<td>Y</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>No theft of EWS data</td>
<td>Y</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>No theft of process computer software</td>
<td>Y</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>No operation of valves</td>
<td>Z</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>11</td>
<td>No changes to tuning parameters</td>
<td>Z</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>12</td>
<td>No changes to control settings</td>
<td>Z</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>13</td>
<td>No changes to control hi/lo limits</td>
<td>Z</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>14</td>
<td>No falsification/corruption of control programs</td>
<td>Z</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>15</td>
<td>No changes to measurement values</td>
<td>Z</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>16</td>
<td>No falsification/corruption of data files</td>
<td>Z</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>No falsification of EWS data</td>
<td>Z</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>No falsification of backup data</td>
<td>Z</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>No intervention in warning operation</td>
<td>Z</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>No intervention in trip operation</td>
<td>Z</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>21</td>
<td>No intervention in console screens</td>
<td>Z</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>22</td>
<td>No disruption of Control System Information LAN</td>
<td>X</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>No freezing of process computer screen</td>
<td>X</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>No theft of data displayed on console screen</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>24</td>
<td>No theft of data files (quality, recipes etc)</td>
<td>Y</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>25</td>
<td>No theft of console data via ftp etc</td>
<td>Y</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>26</td>
<td>No theft of process data</td>
<td>Y</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>27</td>
<td></td>
<td>Y</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>28</td>
<td>No falsification of history data</td>
<td>Z</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>29</td>
<td>No corruption of process computer database</td>
<td>Z</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>30</td>
<td>No corruption of process computer configuration</td>
<td>Z</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>31</td>
<td>No falsification of process computer history data</td>
<td>Z</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>32</td>
<td>No intrusion into process computer</td>
<td>X</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>33</td>
<td>No theft of process computer operation data</td>
<td>Y</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>34</td>
<td>No modification of process computer hi/lo limits</td>
<td>Z</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

### 3.2 Threat Analysis Using HAZOP and FTA

Engineering firms, which play a vital role in plant design and construction, include risk analysis (analysis of safety and reliability) as part of their plant design activities. In designing plant network security systems also, it should be possible to apply procedures similar to those used in plant risk analysis.

(1) **Proposals for Process Security Engineering**

In designing plant network security systems, it is necessary that risk analysis be performed assuming that there are points of contact between the control system and external systems and networks. Depending on the plant type, there may be much equipment which comprises infrastructure of vital importance to society, making risk analysis mandatory. And even in ordinary plants, unplanned stoppages can result in serious economic losses, so that risk analysis
is again essential. If there is a need to connect the control system of a plant with a different network in some form or other, in addition to safety considerations, it will be necessary to reconsider the control system design from the standpoints of economy and social impact as well.

Current security measures for isolated control systems are comparable to or exceed those for general information systems. However, if the scope of the system configuration is expanded as described above, more comprehensive studies become necessary.

In the life-cycle of plant facilities, from planning and design through manufacture, construction, operation and maintenance, and disposal, though the user company bears responsibility for execution in all these stages, the proportion represented by operation and maintenance is high. Engineering companies must provide client companies with multifaceted services, which therefore affect all aspects of the system; but a greater proportion of such services is concentrated in design and construction, and in many cases engineering firms will be entrusted with complete responsibility for design and construction projects. Vendor companies generally take charge of parts of design, manufacturing and construction. As recent transactions for new plant construction indicate, when the customer demands of the engineering firm comprehensive business performance including information systems, it will consign to the engineering firm responsibility for overall network security including control systems, and as part of plant design activities will adopt network specifications and will undertake plant design based on the latter.

In particular, in the process of studying individual security measures, often there will be requests for measures based on plant behavior and design concepts.
Hence there is a growing need for engineering processes to include evaluations of current network security measures in the plant design stage, studies of reinforced measures based on these results, and cost assessments of same. Procedures for systematization of such processes have not yet been established; for the present, engineering companies will play the central role in creating and supporting security policies, performing basic analyses of process security risks and conducting detailed risk analyses of network security in order to establish new methodologies, with the cooperation of user companies, vendors and network specialists. Figure 2 illustrates the framework for process security engineering by engineering firms in connection with planning, design and construction, as well as areas for study and related matters.
Support for General Security Policy Creation
Various studies are conducted for the purpose of creating a general security policy to address such issues as the main security risks at the plant, the current status of security technology, declines in convenience owing to security measures, and cost estimates.

Basic Analysis of Process Security Risks
Process HAZOP analyses are performed of
- Control systems for reactors, furnaces, material supply systems
- Control systems for plant utilities
for modified control parameters, and risks are analyzed. Particularly serious risks are subjected to FTA analysis.

Detailed Network Security Risk Analysis
- Security HAZOP is performed based on Security Guide Words for each node of the network to analyze risks.
- FTA risk analysis is performed in important areas.

Figure 2 Process security engineering
(2) Checklist for HAZOP and FTA Security Evaluations

The HAZOP, FTA and other procedures used to assess plant safety were applied to security risk analysis in the network design stage (cf. Attached Figure 1: Analysis of Communication System Difficulties Using the HAZOP Procedure, Attached Figure 2: Basic Structure of General Security Risks, Attached Figure 3: FTA for Cyber-Terrorism Risks in Control Networks). However, because execution of HAZOP and FTA for network security is attended with difficulties even for engineering firms and security specialists, there is a need to develop a new, simpler procedure based on these. This committee undertook the preparation of a simple checklist which can be utilized by ordinary users and vendors in assessing the security of control systems. Figure 3 summarizes the checklist for security evaluation. In actual use, this checklist should be references in expanding the several branches of the "tree structure" for analysis to analyze specific individual items.
Figure 3 Checklist for security evaluation

Process Side Risk Levels
- Level AA: Operation stoppages for six months or more (internal explosions, configurations etc.)
- Level A: Operation stoppages for one month or more (damage to process equipment etc.)
- Level B: Operation stoppages for several weeks (abnormal stoppage of material systems, security systems)
- Level C: Operation stoppages for one week or less (other temporary operation stoppages)

Control anomalies due to oversight of falsified control system files

Operation stoppage due to accidents or expansion of process anomalies

Failure to prevent or suppress process anomalies

Nonfunctioning of measures to prevent illicit data falsification

Failure to reject anomalous control output due to illicit falsification

Inoperation of functions for monitoring/warning of process anomalies

Inadequate monitoring of access

Failure to control illicit access

Inadequate limitation of access settings

Failure to confirm accessing users

Inadequate inspection for illicit input

Inadequate management to deal with illicit changes

Inadequate safety for information communication, storage

Independent, closed access

Access control

Access route settings

Access right settings

Limitation of access permission

Access encryption

Check of input item types

Check of change patterns

Check of input times

Check of change limits

Integrity checks

Encryption

Measures for floppy disk security

Security policy

Establishment of management system

Continual acquisition of safety information

Periodic checks of monitor records

Password changes

Removal of access for former employees

Measures to deal with system changes

Security education

Isolation of important data

File encryption

Communication encryption

Use of private lines

Management of communication access points

Use of non-rewritable devices

Virus countermeasures

OS with high security level

Monitoring of control output upper/lower limits

Monitoring of rate-of-change upper/lower limits

Monitoring of parameter changes

Monitoring of process state variables

Early detection of control anomalies

Warning of process anomalies

Measures to prevent expansion of anomalous states

Security training

Computer passwords

Call-back method

Notification of caller number

One-time passwords

Voice, fingerprints, handprints, etc.

Electronic signatures, certificates

Monitoring of access attempts

Monitoring of access time

Monitoring of access content

Monitoring of past usage patterns

Access list comparisons

Multilevel access control
(3) Relation of Security Violations Event to Methods of Intrusion

Starting from the security policies of user companies, threat analysis using FTA and approaches to measures of both an engineering and a management nature were studied. Because these were case studies, process computers and other components were not considered, and the "analysis tree structure" was used for simplification. In analyzing a system implementation, study on a more detailed level will be needed.

In order to select actual measures, the probability of occurrence of phenomena, the costs associated with different countermeasures, and other factors must be considered. Here, however, we limit ourselves to an explication of items necessary for studying individual causal relations and methods for prevention in each case, and do not assess probabilities or costs.

Using FTA, measures to be adopted can be clarified. That is, in the case of an AND gate or sequential AND gate, it is sufficient to prevent one of the factors below the gate. In the case of an OR gate, on the other hand, all factors must be prevented (see Attached Figure 4).

The specific order of analysis using FTA is as follows (cf. Table 7).

[1] The abovementioned security policy (items requiring protection) are divided as follows into three categories as violations of security events.

•Violations of Security events

I. Falsification/corruption

Falsification: Willful modification or falsification of data, resulting in incorrect data.

Corruption: Destruction or falsification of programs or databases, resulting in runaway operation, erroneous operation, inability to read data and other phenomena.
II. Unauthorized acquisition of confidential information (security leaks):

Unauthorized acquisition of internal information via outside networks. From an internal perspective, this involves leaks of data, programs or other resources.

III. Intrusion:

Unauthorized intrude into a network, or the inducing of confusion in the network.

• What areas of the system configuration model are affected or related? (related equipment)
• What is the extent of the effects? (classified into three categories—great, moderate, small)

• Characterization of violations in terms of the following:
  a. Network (LAN) intrusion
  b. Following intrusion of the network, login to process computers or DCS
  c. Following intrusion of the network, accessing of process data via gateways
  d. Following intrusion of the network, use of X terminals and other functions for screen theft
  e. Following intrusion of the network, use of special unpublicized communications for access

[2] Violations are selected for analysis. (Violations which can be regarded as equivalent to other selected violations are not selected.)

[3] FT diagrams are prepared for selected violations.

[4] The relations between causes at FT diagram terminuses and violation phenomena are summarized.
### Table 7. Security violations and degree of impact

<table>
<thead>
<tr>
<th><strong>Security Violations</strong></th>
<th><strong>Related Equipment</strong></th>
<th><strong>Impact</strong></th>
<th><strong>FT diagram no.</strong></th>
<th><strong>Violation type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>I. Falsification/Corruption</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I-1 Falsified operation output</td>
<td>Consoles, controllers</td>
<td>Large</td>
<td>Attached Fig. 4-1</td>
<td>c</td>
</tr>
<tr>
<td>I-2 Falsification of variable parameters</td>
<td>Consoles, controllers, engineering consoles, EWS</td>
<td>Large</td>
<td>Attached Fig. 4-2</td>
<td>c</td>
</tr>
<tr>
<td>I-3 Corruption of data files, control programs</td>
<td>Engineering consoles, EWS, process computers, controllers</td>
<td>Large</td>
<td>Attached Fig. 4-3</td>
<td>b e</td>
</tr>
<tr>
<td>I-4 Falsification of measurements</td>
<td>Controllers and higher-level components</td>
<td>Large</td>
<td>Attached Fig. 4-4</td>
<td>c</td>
</tr>
<tr>
<td>I-5 EWS data falsification</td>
<td>EWS</td>
<td>Large</td>
<td>Attached Fig. 4-3</td>
<td>b</td>
</tr>
<tr>
<td>I-6 Falsification of historical data</td>
<td>Consoles EWS and above</td>
<td>Moderate</td>
<td>Attached Fig. 4-3</td>
<td>b</td>
</tr>
<tr>
<td>I-7 Corruption of process computer database</td>
<td>Process computer</td>
<td>Moderate</td>
<td>Attached Fig. 4-3</td>
<td>b</td>
</tr>
<tr>
<td>I-8 Falsification of process computer configuration</td>
<td>Process computer</td>
<td>Moderate</td>
<td>Attached Fig. 4-2</td>
<td>b</td>
</tr>
<tr>
<td>I-9 Falsification of process computer control upper limits</td>
<td>Process computer</td>
<td>Small</td>
<td>Attached Fig. 4-2</td>
<td>b</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>II. Unauthorized Acquisition of Confidential Information (security leaks)</strong></th>
<th><strong>Related Equipment</strong></th>
<th><strong>Impact</strong></th>
<th><strong>FT diagram no.</strong></th>
<th><strong>Violation type</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>II-1 Unauthorized acquisition of data files</td>
<td>Engineering consoles, EWS, process computers, consoles</td>
<td>Large</td>
<td>Attached Fig. 4-5</td>
<td>b</td>
</tr>
<tr>
<td>II-2 Unauthorized acquisition of control programs</td>
<td>Engineering consoles, controllers</td>
<td>Large</td>
<td>Attached Fig. 4-5</td>
<td>b</td>
</tr>
<tr>
<td>II-3 Unauthorized acquisition of control station data</td>
<td>Controllers</td>
<td>Large</td>
<td>Attached Fig. 4-5</td>
<td>c</td>
</tr>
<tr>
<td>II-4 Unauthorized acquisition of EWS data</td>
<td>EWS</td>
<td>Large</td>
<td>Attached Fig. 4-5</td>
<td>b</td>
</tr>
<tr>
<td>II-5 Unauthorized acquisition of process computer software</td>
<td>Process computer</td>
<td>Large</td>
<td>Attached Fig. 4-5</td>
<td>b</td>
</tr>
<tr>
<td>II-6 Unauthorized acquisition of process data</td>
<td>Operation console, process computers</td>
<td>Moderate</td>
<td>Attached Fig. 4-5</td>
<td>c</td>
</tr>
<tr>
<td>II-7 Unauthorized acquisition of console screen information</td>
<td>Consoles</td>
<td>Moderate</td>
<td>Attached Fig. 4-5</td>
<td>d</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>III. Unauthorized Intrusion</th>
<th>Related Equipment</th>
<th>Impact</th>
<th>FT diagram no.</th>
<th>Violation type</th>
</tr>
</thead>
<tbody>
<tr>
<td>III-1 Freezing of console screens</td>
<td>Consoles</td>
<td>Large</td>
<td>Attached Fig. 4-6</td>
<td>b</td>
</tr>
<tr>
<td>III-2 Confusion of Control System LANs</td>
<td>Control System LANs</td>
<td>Large</td>
<td>Attached Fig. 4-7</td>
<td>a</td>
</tr>
<tr>
<td>III-3 Intrusion of Control System LANs</td>
<td>Control System LANs</td>
<td>Large</td>
<td>Attached Fig. 4-3</td>
<td>e</td>
</tr>
<tr>
<td>III-4 Login to consoles</td>
<td>Consoles</td>
<td>Large</td>
<td>*</td>
<td>b</td>
</tr>
<tr>
<td>III-5 Intervention in warnings/trip actions</td>
<td>Operation console, controllers</td>
<td>Large</td>
<td>Attached Fig. 4-2</td>
<td>c</td>
</tr>
</tbody>
</table>
### III-6 Freezing of process computer screens

| Process computers | Moderate | Attached Fig. 4-6 | b |

### III-7 Confusion of Control System Information LANs

| Control System Information LANs | Moderate | Attached Fig. 4-7 | a |

### III-8 Login to process computers

| Process computers | Small | * | a |

Note: An asterisk (*) in the FT diagram no. column indicates equivalence to logins at various points in the different diagrams.

The FT diagrams prepared in this study (Attached Figures 4-1 through 4-7) and a table giving the relation between terminal causes and violations (Attached Figure 4-8) are appended to this document.

### 3.3 Threat Analysis by Route of Intrusion

Intrusion routes were added to the plant model diagram (Figure 1) to produce Figure 4. Threats to security may be classified by route of intrusion as follows.

(1) Intrusion via networks
   
   (a) Information system LANs
   
   (b) Dialup connections
   
   (c) Wireless application networks

Intrusion types that are related to the plant life-cycle include:

(2) Unauthorized intrusion at time of plant planning, design or construction

(3) Unauthorized intrusion during maintenance, including remote maintenance

Other types of intrusion include:

(4) Intrusion by computer viruses
(5) Intrusion via social engineering (see the Glossary). The possibility of penetration by these routes, and possible threats following intrusion, were analyzed and listed.
Figure 4. Plant networks and intrusion routes

(1) Intrusion via Networks

Connections with the Information system LAN and other information systems in the plant are essential for transfer of production schedules, production results, quality information, and other data exchanges with plant information management systems (PIMS). However, connection with information systems means connection with enterprise-wide systems and, in turn, with the Internet and public communication circuits. From the standpoint of network security, such connections are attended by considerable risks.

[1] Explanation of intrusion routes

(a) Intrusion routes over Information system LANs, and means of data theft

The following are means of intrusion of an Information system LAN from peripheral systems and equipment.

| • Intrusion through unauthorized connection of PCs via open hub circuits and conference room or reception area network jacks |
| • Intrusion from office workstations connected normally to LANs |
| • Intrusion via wireless application networks |
| • Intrusion via the Internet |
| • Intrusion through dialup lines (general telephone lines, portable telephones, PHS sets) |

The following are examples of specific means used for penetration.

<p>| • Accessing files via FTP, RCP, etc. |
| • Remote login (telnet, rlogin) |
| • Accessing of shared network files via NFS etc. |
| • Manipulation of screens using the X protocol |
| • Accessing of control data through TCP/IP |</p>
<table>
<thead>
<tr>
<th>Accessing of control data via general-purpose communications (DDE/OPC/ODBC/remote SQL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insertion of an unauthorized program or command into communication data to falsify or access firewall file systems or network objects</td>
</tr>
<tr>
<td>Sending large volumes of data packets from outside to dramatically degrade firewall performance and impede operations</td>
</tr>
</tbody>
</table>

In addition, the following means of data theft may be used.

<table>
<thead>
<tr>
<th>Installing listening devices (bugging devices) in telephones and modems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing protocol analyzers and other equipment in LANs</td>
</tr>
<tr>
<td>Reception of leaked radiation from physical circuits (IDF, MDF, circuit clipping etc.)</td>
</tr>
<tr>
<td>Interception of wireless communication signals (portable phones, PHS, microwave communications, satellite communications, wireless LANs)</td>
</tr>
</tbody>
</table>

(b) Intrusion routes via dialup connections

Methods for connection to control systems through dialup connections are as follows.

Ordinarily, computers at plants are connected to remote terminals (PCs etc.) via communication circuits (modems). In the case of a phone circuit connection, for example, connection at the level of the physical circuit is possible from anywhere in the world if one knows the phone number at the plant. (Among current phone circuits are some with functions to check the phone number of the calling side (such as ISDN lines), and some which have no such functions; connections are possible in the latter case.)

When the circuit connection is completed, as with ordinary LAN connections, the modem can perform remote login, file transfer and other processing with the directly connected computer. And depending on settings, the modem can use the directly connected computer as a TCP/IP router in direct communications (remote login etc.) with any arbitrary computer on the LAN.

(c) Intrusion via wireless application networks
Connections to control systems through wireless application networks are as follows.

In the past, intercoms and transceivers were used as a means of contact between onsite workers and central control rooms; there were no connections with the control system. But with the spread of mobile computing, new equipment was used to make connections to control systems also.

One such example is the "Maintenance Patrol Support System". This system uses wireless application networks to send information obtained in patrols to control rooms for use in maintenance and equipment operation; conversely, it enables onsite checks of documents and other information received from the central control room. It is thus a highly useful system for patrol activities.

Such systems are today used widely due to emphasis on enhanced convenience; but in view of the advantages for simplification of cable installation and the increasing diversification of application systems, it is entirely possible that Control System LANs, Control System Information LANs, and Information system LANs will go wireless in future.

The threat of intrusion from wireless application networks is higher than for other networks, due to the great danger of interception. It is best to bear in mind that anyone can intercept wireless signals if specialized equipment is used.

[2] Threats following intrusion

As threats common to intrusion by all the above three routes, there is the possibility of unauthorized acquisition of the following kinds of control system data.

| • Control data                  |
| • Data communicated between control systems and information systems |
| • Address information for gateway routers of the control system |
| Basic information for use in intrusion (account names, passwords, address information, host names, filenames, etc.) |
| Recipe, history, quality, etc. databases on the process computer |
| Configuration data for the control system |
| Various kinds of software (OS, application programs, package software, etc.) |

Not only is there the possibility that such data and programs may be stolen; there is also the threat that they may be falsified or otherwise modified.

In addition, wiretapping/eavesdropping also carries the threat of Unauthorized acquisition of the abovementioned basic information for intrusion, as a precursor to actual intrusion.

In addition, the following threats exist as a result of e-mail file attachments and viruses intrusion via the web, as examples of intrusion via the internet.

| Release of a "Trojan horse" in the control system |
| Delays or stoppages of communication, or other disruption to communication between control systems and information systems |
| Exhaustion of resources (disk space, memory, etc.) |

Threats Related to the Plant Life-Cycle

(2) Threats in the Plant Planning, Design and Construction Stages

[1] Threats in the plant planning and design stages

In the plant planning and design stages, various design specifications and drawings for plant equipment are studied, and these are disclosed to customer and vendor companies in the form of design documents. In the stages of plant equipment planning and design, if interlock diagrams, DCS configuration diagrams, network diagrams and other documents are leaked to outside parties, they may at a later date serve as the basic information for cyber-terrorists. This potential threat should be born in mind in these stages. In the
past, such information was mainly recorded on paper; but today nearly all such information is handled in electronic form, and of course information is exchanged over networks. Even previously, unauthorized removal of papers from an office, or theft of documents in transit, were possible; but when such information is in electronic form, it is more vulnerable to willful intrusion and theft by cyber-terrorists.

[2] Threats relating to adjustments at time of plant construction

At the time of plant construction, adjustments to DCS and the overall control system are performed. Current DCS systems are shipped after certificate tests, and in essence no major corrections are made onsite after shipment. However, various smaller corrections are performed at the site as a result of DCS startup testing, electrical and functional connection tests of controllers and detection terminals for production equipment, process computer and DCS connection tests, remote maintenance checks and other testing.

As an additional possible engineering trend, in future software may be loaded from remote sites at this stage.

Also, plant construction, control room construction, and adjustments and modifications to these are generally being performed under pressure to meet a deadline.

The following are anticipated current and future threats at the time of plant construction.

- During operation, DCS parameters not changed by the operator (PID tuning parameters, parameters to change algorithms, etc.) are changed. For this reason, adjustments are made in engineering mode. If parameters are left in an accessible state, they constitute a security hole.
During operation, unused debugging tools are installed. These tools can be used to manipulate functions extending to the system core.

Often passwords are left at their default settings.

These settings made during adjustments must be changed to the settings to be used in continual operation when the equipment is delivered to the user, or else a gaping security hole will be left.

In addition, software to be added urgently is often installed from floppy disks. This carries the risk of virus infection.

In addition, the employees of various contractors are constantly coming and going on the site, and it is possible that some of them may devise some means of enabling intrusion at a later date. For example, possible threats include equipment installation to enable wiretapping, and the introduction of a Trojan horse used to steal passwords.

(3) Threats Related to Maintenance, Including Remote Maintenance

Remote maintenance involves preventive maintenance and the identification and restoration of malfunctioning areas in computers (process computers, consoles, engineering consoles, EWS etc.) and the networks connecting computers (modems, routers, LANs, hubs, etc.). Recently services ("help desks") offering answers to questions and guidance in the use of OSes and application software, as well as network monitoring services, are subsumed in the category of remote maintenance. Demands for reduced user TCO (total costs of ownership) have given rise to a trend toward expanded services in the following areas of remote maintenance.
[1] Objects of remote maintenance

Objects of remote maintenance include computers and peripheral equipment, software, network equipment, and operation management.

[2] Summary of remote maintenance services

It should be noted that recent services such as help desks and network management are also included within the scope of remote maintenance.

(a) Preventive maintenance (PM)

PM includes collection of data used to forecast hardware malfunctions, analysis of malfunctions, and periodic inspections of parts. Also included are collection of historical data on software operation; collection of various error log data and analysis of said data; improvement of software performance and the provision and employment of correction data for malfunction locations; and provision of documents and news related to maintenance.

(b) Restoration of malfunctioning equipment

In the event of anomalous behavior, tasks are executed to identify the locations of hardware and software malfunctions. Specifically, the causes of an anomaly identified as originating in hardware are separated, parts are identified, converted items are delivered, and switching to substitute equipment is performed. Also, the causes of an anomaly identified as originating in software are separated, software correction data is acquired and utilized, operation of the corrected software is confirmed, various error logs are collected and analyzed, survey data (memory dumps, file dumps etc.) is collected, and new versions of software are made available or exchanged.

(c) Operation monitoring

Data on the state of operation of system equipment and software is collected, the state of operation is monitored, notifications of aberrant behavior
are made, measures are taken to prevent anomalous states, and procedures for recovery are provided.

(d) Malfunction management

Information on malfunction rectification is accumulated, historical data on the application of malfunction correction data is recorded and managed, information on corrections performed at time of malfunction based on the malfunction phenomena is retrieved, and correction information is extracted.

(e) Resource distribution

Unified management of various software resources operating at servers and clients on the network is performed, and new software versions and software patches are distributed to servers and clients.

(f) Configuration information management

The hardware and software configurations of servers and clients on the network are determined, and information on hardware and software versions is managed.

(g) Performance information management

Network traffic is monitored, the occurrence of convergence is monitored, and performance information is collected and analyzed in order to maintain stable system operation.

(h) Backups and data restoration

Periodic backups are scheduled and backups are performed according to schedules; backup media are stored at several locations, and requests for data restoration are accommodated.

(i) Help desks

Queries on hardware, software, application programs and other topics are received and answered via telephone and e-mail, survey answers are provided.
and operation is supported.

[3] Threats to security in remote maintenance

Remote maintenance has a dramatic effect in stabilizing system operation and shortening the time required for recovery from malfunctions. But on the other hand, because it is a service which uses networks, like networks in general it is vulnerable to security threats. In addition, by their nature remote maintenance services involve direct manipulation of the core components of the system. Consequently the tradeoff between convenience and safety must be carefully considered when assessing the security problems posed by remote maintenance.

(a) Threats related to maintenance personnel

• The personnel performing remote maintenance services must be trustworthy.

When connecting a remote maintenance service to the system to be maintained, it must be possible to certify that the individuals in question are legitimate maintenance personnel.

• In the event that the names and account names of legitimate maintenance personnel are used falsely in order to gain access to the system being maintained, it is possible that important data may be deleted and plant control data may be deleted or falsified, resulting in anomalous behavior or inability to control the plant in question.

• In addition, leaks by maintenance personnel of documents used in maintenance tasks, and loss of account names or passwords of maintenance personnel, can have serious consequences for system security.

• Deletion of data due to simple mistakes by maintenance personnel during remote maintenance, errors in maintenance tasks resulting from
misunderstandings, and similar incidents can also have grave consequences.

• There is also the danger of leaks of account names or passwords as the result of threats or bribes of maintenance personnel by malicious persons or organizations.

(b) Threat of intrusion via circuits for remote maintenance

• Remote maintenance services may use leased lines or other circuits that are perpetually connected, or it may use circuits based on dialup connections, established whenever the need for service arises. When using leased or private circuits, there is the danger of wiretapping at points between the service provider and the service user. Further, there is great danger of malicious access using remote maintenance service terminals and communication equipment at the service provider site.

• There is the danger of information leaks through this equipment. Also, if management of maintenance-related documents has not been established, unauthorized copying or theft of such documents is also a possibility.

• In remote maintenance using dialup connections, leaks of telephone numbers or the account names and passwords of personnel may result in unauthorized intrusion.

• Even when dialup connection telephone numbers are unpublished, there is the danger of telephone number leaks and of discovery of telephone numbers through random dialing.

• Even when using callback modems, connections may be made by invalidating callback modems.

• If information is transferred to a fraudulent host through abuse of modem transfer functions, account names, passwords and other important confidential information may be leaked to outside parties.
(c) Threat of theft of remote maintenance circuits

• Care is needed to ensure there are no leaks of the account names or passwords of maintenance personnel through wiretapping devices installed in modems or communication circuits. If commands or filenames which can be used in remote maintenance are obtained through wiretapping, abuse of the access privileges of maintenance personnel could occur, possibly resulting in leaks or corruption of important data or recipes.

• There is also the possibility that account names and passwords may be registered to enable subsequent intrusion, based on information gained through wiretapping. This has the effect of giving malicious parties additional time for system intrusion and other hostile acts. The creation of account names and passwords for use in future intrusions can be likened to a door with no lock; the potential harm of such an open door is unfathomable.

(d) Threat of computer virus infection

• Conceivable routes for computer virus infection include via networks used to provide remote maintenance services, via magnetic media carried onsite by maintenance personnel, and through e-mail and e-mail file attachments in exchanges with the help desk. In particular, when magnetic media infected with a virus is used by maintenance personnel in maintenance operations, the system being serviced will inevitably be infected.

• In addition, if files sent and received as e-mail attachments are infected, the scope of the infection can be expanded with considerable rapidity. Infection occurs before any awareness of the presence of a virus, so that it is often difficult to identify the route of the infection.

• Damage resulting from virus infection can vary greatly, from consumption of memory, disk and other resources on the infected system, to deletion of files,
corruption of screen displays, or displays indicating that the system has been infected. A system infected with a virus may no longer be capable of ordinary functions or performance. And in addition, there may be collection of account names, passwords and other information intrude into the system, to be passed on to malicious parties. A system infected with such a virus no longer has any security defenses, and is exposed to addition intrusion threats.

Other threats

(4) Threats Due to Computer Virus Intrusions

Anti-virus measures are needed to anticipate threats from many other directions besides remote maintenance services.

[1] Computer virus varieties

Computer viruses (hereafter simply "viruses") are a menace throughout the world. As Table 8 indicates, nearly all virus-induced damage is to PCs. There are more viruses on PCs than any other type, at some 14,000 varieties or more. In contrast, viruses targeting workstations and general-purpose computers exist only locally and have not spread worldwide. However, a cyber-terrorist aiming to foment confusion in computer systems will be ready to attack the weak points of any system, and so anti-virus measures must be implemented which include workstations and general-purpose computers as well as the rest of the system.

Table 8. Number of different computer virus varieties worldwide (as of December 1997)

<table>
<thead>
<tr>
<th>Computer Type</th>
<th>Number of Varieties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal computers (Windows, DOS)</td>
<td>14,000 varieties</td>
</tr>
<tr>
<td>Personal computers (Macintosh)</td>
<td>50 to 60 varieties</td>
</tr>
<tr>
<td>Workstations (UNIX)</td>
<td>Several varieties</td>
</tr>
</tbody>
</table>
[2] Routes of virus intrusion

• Intrusion from recording media

In order to prevent virus intrusion, it is first of all necessary to thoroughly inspect the recording media used on each computer. Recording media includes floppy disks, CD-ROMs, MO disks and other media; any of these may be infected by viruses. As a rule CD-ROMs are not infected after initial creation, but if a virus is present in programs or data which are burned onto CD-ROMs, the CDs should be regarded as infected. Anti-virus measures should be taken bearing in mind that all recording media, whether used in enterprise-wide systems, information systems or control systems, are potential entry points for viruses.

• Intrusion via networks

In order to prevent intrusion via networks, thorough inspections must be performed of all programs and data acquired over networks connected with outside entities via enterprise-wide systems, information systems and control systems. Macro viruses may be present in the information published on a web site; a program found on a bulletin board may be a Trojan horse; many other scenarios occur frequently.

However, while the network is connected with outside systems, it is not the case that virus intrusion occurs solely through acquired programs and data. Prime examples of exceptions are worms and Java viruses. A worm will automatically find and intrude security holes in computers connected to the network. And a Java virus, placed on a web site by a malicious individual, can intrude without warning during a web browsing session.
In this way, all networks connected to outside entities can be channels for virus intrusion, and so appropriate preventive measures are required.

[3] Threats posed by viruses

When a virus intrude a system, possible consequences include leaks of information on disk or in memory, falsification or corruption of data, disruption of screens displaying the system state or operating state, and inability to control system components or equipment. These effects may in turn give rise to system malfunctions, anomalous shutdowns and other serious results.


Below are listed the names and a brief description of viruses currently in existence or which may be expected to appear in future, together with the timing of system intrusion.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boot sector viruses</strong></td>
<td>This type of virus attacks the boot sector and master boot sector of floppy disks and hard disks. When a computer is started from a floppy disk or hard disk infected with this kind of virus, the virus invades the computer. This kind of virus can also infect data floppy disks. Hence anti-virus measures are necessary even for floppy disks not containing system files.</td>
</tr>
<tr>
<td><strong>File-infecting viruses</strong></td>
<td>These viruses enter program files. In general they attack regardless of the type of program file, and so may have infected all program files. When a program infected with this kind of virus is run on a computer, the computer becomes infected.</td>
</tr>
<tr>
<td><strong>File-boot sector viruses (hybrid viruses)</strong></td>
<td>These viruses invade computers both in the form of boot sector viruses, and as file-infecting viruses, described above.</td>
</tr>
</tbody>
</table>
• **Macro viruses**

This kind of virus invades data. Viruses which infect the data generated by word processing and spreadsheet programs are rampant in many countries. When a file infected with this kind of virus is displayed by an application program, the virus enters the computer. A virus which has infected data created with one software package can in principle reproduce when the file is opened with different software, so long as that software has macro functions. Hereafter it will be necessary to take precautions with respect to data files prepared using software with macro capabilities.

• **Worms**

This program causes problems while multiplying in a multitasking, multiuser OS environment. Many of these were intended to operate within workstations and general-purpose computers. Worms penetrate the security holes in other computers connected by a network. Worms invade from outside automatically, and so especially stringent countermeasures are required.

• **Trojan horses**

A Trojan horse has the external appearance of a utility program or other software, but in reality it sets about stealing or corrupting data when the program is run. This kind of virus deceives the user to gain access to the computer.

• **Java viruses**

A Java virus is written in the Java language; it lurks on WWW sites on the Internet, and invades when a web page on which it resides is viewed. At present there are no clear reports of damage sustained by this type of virus (though there are many cases in which the cause of damage is unknown), but likely instances are gradually becoming more common. This type of virus is likely to demand the greatest amount of caution in future.

(5) Social Engineering

(Acquisition of the information necessary for intrusion from a human being (a legitimate user))

[1] Social engineering
The objects of social engineering are wide-ranging, from system managers to operators, normal system users, persons in charge of public relations, system maintenance personnel (both software and hardware), system developers, and persons previously employed in all these areas. In some cases, the wives, husbands, paramours, or confidants of these people may also be targets of social engineering.

A variety of techniques are used on these targets, in attempts to gain information related to the system, such as access information.

Passwords and other information needed for system access, or personal information from which passwords might be surmised--names, nicknames, phone numbers, dates of birth, employee numbers, and so on--are acquired from the target, by methods which are not quite illegal. Many different stratagems are used; the perpetrator might pose as a new user and telephone a system administrator, asking for information related to the system.

Criminal actions might include the use of bribery or intimidation to acquire information on the system, or intentional leaks of confidential information on the system by ex-employees.

[2] Other related matters

There are many other techniques besides asking people directly for information. One involves searching through the trash generated by a company for related information. For example, if routine memos are thrown away unwittingly, they may fall into the hands of "crackers" and become valuable sources of information. And, screen burn-in, the electromagnetic radiation from monitors, and other evidence of password entry may become valuable sources of information.
• Magnetic media (floppy disks, hard disks etc): Though a user may have thought that delete functions were sufficient to erase a floppy disk, their contents can be easily read. In order to ensure they are rendered unreadable, they should be cut into pieces.

• Printouts: Various printouts are routinely discarded; they may contain valuable system-related information. They should be shredded or incinerated.

• Memos and similar: Memos with hard-to-remember passwords and other scribbled information may prove invaluable to others.

• Manuals: Manuals for older versions of software, system training manuals and the like may contain important information on accessing the system.

• Displays: The electromagnetic radiation generated by displays may be intercepted, or burn-in on older displays may allow others to acquire important information.

• Information may be acquired through surreptitious observation of the entry of password or other information.

3.4 Security Measures by Route of Intrusion

As a result of analysis of threats by route of intrusion based on the model system, it was found that in control systems there is considerable possibility of intrusion via large-scale plant networks as systems become more open in future, partly due to the substantial use of general information system technologies.

Hence in this section are listed the absolute minimum security measures (both engineering measures and methods for their use) which must be executed using technologies currently available to user companies, engineering companies, and vendor companies. The following items cannot be said to give
complete protection from cyber-terrorism and system cracking; but measures in each area should be implemented by all companies, starting from those items for which execution is most viable, in order to enhance security.

(1) Measures Related to Connections with Information Systems

In connections with information systems, thoroughgoing security measures are first of all essential in general computer networks. The following are examples of measures which user companies should take in addition to engineering and vendor firms.

[1] Establishment of a security policy (clarification by the user company of resources to be protected and assignment of priorities), and creation of an environment of strict compliance

[2] Establishment of firewalls between control systems and Information system LANs

- Installation of firewalls as general measures for network security
- Examination of services required with higher-level networks (ftp, telnet etc.), and permission of only the bare minimum of services
- Measures to prevent leaks of address information

[3] Fortification of Control System Information LAN management. For example, the following measures may be considered.

- Periodic changes of passwords
- When using public communication circuits in particular, the use of one-time passwords
- Limitation of computers and equipment connected to Control System Information LANs
- Recording of all communications for which connections are permitted and prohibited by firewalls, and periodic inspections for abnormalities
- Elimination of unnecessary network services
The measures described below should be executed immediately upon resolving problems with implementation. Representative examples of tools for detection of intrusion include the TCP wrapper and Intrusion Detection System, and the Tripwire tool for detection of file data falsification. These are each explained in the appended Glossary.

[4] Encryption of important files and communication data
[5] Introduction of an identification system (bionics identification, IDs) and authentication system
[6] Prevention of unauthorized writing and falsification through routers and other communication equipment comprising control systems
[7] Installation of Intrusion Detection Tools
[8] Establishment of functions for detecting data falsification in communication channels and notifying system managers
[9] Monitoring of firewall file systems and detection of abnormalities, in order to monitor anomalies in firewalls themselves
[10] Introduction of measures to impede routing to routers, as a means of thwarting attacks of large data packets

(2) Measures for Dialup Connections (principally for user companies)

[1] Fortification of access control at the time of connection of dialup equipment (modems etc.)

•Limitation of connections to originating telephone numbers outside the plant already approved in advance
  --Use of callbacks when originating phone number notification functions cannot be used
  --Use of originating phone number notification functions when available

•Use of the password authentication functions of dialup equipment (modems etc.)
In order to more rigidly control access, installation of remote access servers and authentication servers

[2] Fortification of PPP (point-to-point protocol) access control
- Execution of CHAP/PAP etc. password authentication
- Use of account names and passwords other than those used on LANs

[3] Fortification of access control at login
- Preparation of accounts specifically for dialup connections, and use of passwords other than those used for accounts on LANs
- Use of prompts other than ordinary prompts (or prompts for login requests on the LAN side) in order to prevent automatic login
- Use of prompts which do not include the machine name or other text which might unwittingly provide information
- Establishment of an appropriate delay time following authentication failure, in order to render difficult "replay" attacks

[4] Collection of logs containing records of connection requests which were permitted or forbidden, and periodic analysis

The above measures can be implemented using current functions and operations.

(3) Measures for Wireless Application Networks (principally user companies)

[1] Measures to prevent wiretapping
* Wireless application networks and Control System LANs should always be configured as different segments, in order to prevent the flow of unnecessary data on the wireless network. If there are OS functions or hardware for encryption packets, they should be used.

[2] Measures to prevent "replay" attacks
•To the above measure [1] is added a function for dynamically changing the address information of portable terminals at fixed intervals.

Measures to prevent intrusion

•Only communications limited to portable terminal applications are permitted, using firewall functions for routers or dedicated computers.

•When not using wireless networks, as for example while in motion on patrol, power to wireless devices should be turned off scrupulously, and management of devices should be thorough.

(4) Measures in Plant Network Planning, Design and Construction (primarily for engineering companies)

[1] Measures in the planning and design stages of plant networks

•Thorough management of entrance/egress to design facilities
•Thorough management of design blueprints and other documents
•Preparation and implementation of standards relating to management of information resources (identification of information resources, standards for disclosure within and outside the company, management of storage etc.)
•Preparation and implementation of standards relating to management of electronic information resources (identification of electronic information resources, measures to prevent unauthorized access, anti-virus measures, system monitoring etc.)
•Reliable authentication and thorough encryption in the event of transfers of vital electronic information


Engineering and vendor companies have the responsibility of checking the following items to ensure nothing is left unconfirmed. Task procedures are prepared and are followed thoroughly. At the time of delivery to the user company, there should be final confirmation of matters among the user, vendor and engineering companies.

•Default settings for parameters should be changed according to user needs.
• Checks should be made to ensure that unnecessary or unauthorized programs (debugging tools, special drivers etc.) are not installed.

• The installed DCS software should be checked to ensure it is correct (version no. etc.).

• Passwords and other parameters are changed so that they are different during construction and after operation begins.

• Equipment used in dialup connections should be checked to ensure callback security has been provided.

(5) Measures Related to Maintenance, Including Remote Maintenance

[1] Measures to be taken by the service supplier (vendor)

(a) Service supplier organization

• Service supplier organizations and individuals must be trustworthy.
• Entry/egress of engineers to service supplier facilities should be managed.
• Storage of maintenance-related documents should be managed.
• Access to equipment used in supply of services should be managed adequately.
• Security measures for networks connected to equipment used in services should be executed reliably.
• A system should be established for management of account names and passwords on systems used for services, adopting methods which offer a high degree of safety.

(b) Management of maintenance personnel

Maintenance personnel should be educated in the threats and routes of intrusion in large-scale plant networks, and should be thoroughly managed.

• Maintenance personnel engaged in supply of services must be trustworthy.
• Personnel must have received education in security matters.
• An organization should be established for the management and monitoring of security matters related to maintenance personnel.

(c) Operation management
The scope of operation management includes physical management, storage and management, development management, and personnel management.

• In physical management, entry/egress to buildings and rooms in which are installed service provider equipment must be strictly managed.

• In storage and management, storage of maintenance documents related to customer systems and access to them must be managed thoroughly.

• Storage, supervising of disposal, and management of performance data, traffic data, login data and other information collected in order to supply services must be performed thoroughly.

• In development management, in addition to management of development tasks arising as a result of remote maintenance services, the use, storage, disposal of development documents and study materials used in development must be managed.

• In personnel management, the account names and passwords issued to development engineers and maintenance personnel must be managed, and appropriate measures to ensure the mental health of engineers and maintenance personnel should be taken.

(d) Security education

Education of personnel and managers engaged in development, supply and execution of remote maintenance services should be performed. Appropriate education is necessary in each of the following areas.

• What kinds of passwords are safe passwords?

• How are passwords registered and changed?

• How should documents be stored and managed?

• How should the storage and disposal of collected data be managed?

• What should be done if a person with malicious intent makes contact with you or calls you?

(e) Computer virus countermeasures
Measures to prevent virus infections, and to prevent their spread to outside systems, should be thoroughly executed by the service suppliers themselves.

• Thoroughgoing measures to prevent virus infection must be taken to prevent infection of the suppliers themselves.

• Virus inspections should be performed for recording media on which software is supplied to the customer, and a system for execution of such inspections should be established.

• In particular, the magnetic media to be used by maintenance personnel in maintenance tasks, collection of data, and the provision of information should undergo rigorous virus inspections, and only media passing these inspections should be used.

• Virus inspection tools should always be maintained such that they are capable of discovering and eradicating the most recent viruses.

(f) Monitoring and inspections

• Measures to be taken by service providers should be executed reliably, and should be monitored to ensure effective functioning. Inspections should be performed periodically or for random samples.

• The persons directly involved with remote maintenance services must not be put in charge of monitoring and inspections.

[2] Measures by receiver of services (user company)

(a) Security policy

• When using remote maintenance services, the user company should be aware of tradeoffs between convenience and vulnerability. Either the existing security policy should be revised to adjust for this, or a new and consistent security policy should be devised.

(b) Selection of services and method of provision

• The user company should be aware of the convenience and vulnerability in security terms of remote maintenance services, and should carefully select services, the objects of services, and the method of circuit connection.
• In making selections, thorough analyses should be conducted on risks perceived as security threats, and countermeasures devised.

• In order to effectively and safely utilize the selected services, there should be adequate discussions between the service provider and the user of security measures, and the two must cooperate fully for added safety.

• Services may be provided either by accumulating various types of information gathered by the service provider, or by accumulating data on the side of the company receiving services. Whether data warning of malfunctions, operating history data, error logs and other maintenance-related information is to accumulated externally, or is to be accumulated on a maintenance server installed within the company, is a matter which must be decided in accordance with security policy.

(c) Monitoring and inspections

Independent monitoring and inspections of the following items must be performed by the service provider where remote maintenance services are being used.

• Are entrances for remote maintenance services being used for any other than legitimate purposes?

• Are identification and authentication being performed properly?

• Are there any signs of unauthorized use?

• Are rules adopted for service provision being followed?

[3] Security functions to be provided in rendering remote maintenance services (responsibility of vendor companies)

(a) Measures to prevent intrusion

• Positive identification and authentication must be performed to ensure that persons other than legitimate maintenance personnel are not using remote maintenance entrances for intrusion.

• Identification and authentication must be performed reliably on the service provider side, on the service user side, and in making connections to the system to be serviced.
• Arrangements must be made to prevent the use of commands and access of files outside the permitted range.

• It must be possible to construct an environment closed off from the outside and independent, such that only authorized persons can access vital core areas of the system.

• Address information for equipment and systems receiving remote maintenance must be concealed.

(b) Monitoring and sensing

• In remote maintenance, monitoring and sensing must be performed so as to prevent unauthorized acts and erroneous operation.

(6) Anti-Virus Measures

Basic anti-virus measures should adhere strictly to MITI’s standards for anti-virus measures. In the control system in particular, user companies must thoroughly implement the following measures.

[1] Organizational actions

• Specific anti-virus measures should be instituted, and users made to conform to them completely, with periodic inspections. More rigorous approaches include inspections by a third party.

• In order to clarify responsibility for anti-virus measures, an anti-virus section should be established within the management division, or persons responsible for such measures should be named and made known to all.

• Management units and managers should acquire and distribute to users the most recent virus vaccines. The latest information from domestic IPA security centers and from overseas virus-related public and private entities should be collected, and new measures instituted as necessary.

• In the event of damage, the process of intrusion should be elucidated, and a response formulated on an organizational level as opposed to the level of individuals.

[2] Basic measures at the individual level
Despite organizational measures taken within user companies, their effect is greatly diminished if individual employees are not sufficiently aware of their importance. Employees should be made to adhere to the following measures completely.

- The most recently distributed virus vaccines should be used.
- Data backups should be performed periodically.
- Floppy disks and e-mail attachments should be inspected before use.

(7) Social Engineering Measures

[1] Management of password information

It is thought that password theft, unauthorized password use, and other password-related actions account for the majority of intrusion. The following are examples of password-related measures.

- Passwords should never be disclosed even to other users.
- Passwords which can easily be guessed, such as those using birthdates or employee numbers, should not be allowed.
- Changes in access privileges and removal of passwords as employees leave the company or are transferred should be executed without delay.
- ID cards, fingerprints and other techniques for authentication should be adopted for system managers and other responsible persons in positions which are vital for system security. In addition, there should be regulations placing physical limits on terminals used.

[2] Management of other information to be kept concealed

These are problems pertaining to account names, passwords, address information, manuals and the like; measures are required with respect to system operation, personnel management, and education.

- Employees should be thoroughly educated.
- Punishments for leaks of confidential information should be clearly stated as part of security management regulations.
<table>
<thead>
<tr>
<th>• Janitors and other outside service staff should be prohibited from physical proximity to control systems.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• During inspections, the approaches of each user to social engineering issues should also be checked.</td>
</tr>
</tbody>
</table>
Chapter 4: Proposals to Reinforce Security

Current engineering and operation security levels are inadequate to cope with the threats of cyber-terrorism and system cracking which are anticipated to grow in magnitude in the near future. Therefore in what follows, this committee proposes measures necessary to further boost security levels. We would request that all personnel at user, engineering and vendor companies, from top management down to general employees, arrive at a common understanding on the security measures proposed in this chapter and the last, and seriously study their implementation.

4.1 Institution of Plant Security Guidelines

Concepts of safety will differ depending on the environment and circumstances of the nation, company or individual; hence objective standards for the safety to be sought for control systems are needed. First of all guidelines for security in operations which should be obeyed by user, vendor and engineering firms, as well as reinforcement of organizations within the company for adherence to these guidelines, are needed. Moreover, control systems are configured from the systems and equipment provided by multiple vendors, and so unified standards for security assessment are needed not only for individual products, but for the system as a whole as well.

The bare-minimum engineering and operation measures described in Chapter 3 of this report may be described as an alpha-version of plant security guidelines. Hereafter it will be necessary to prepare a final version of these guidelines, while in the meantime executing the proposals described below--creation of standards for plant security assessment; development of procedures for threat analysis; and development and verification of preventive technologies.
(1) Standards for Plant Security Assessment (revision of standards for prevention of unauthorized access)

"Standard Countermeasures to Unauthorized Computer Access" be revised and augmented to enable application to large-scale plant networks. For example, in control systems, operation management must be stricter than in ordinary information systems. This committee studied items to be added to "Standard Countermeasures to Unauthorized Computer Access" and "Standard Countermeasures to Computer-virus". Examples of the main items considered are listed below. For the details of items to be added to or deleted from standards, please see Reference Material 4: "Items for Addition/Deletion (Unnecessary) in Countermeasure Standards".

a. Measures to be taken by system designers to prevent unauthorized access

| (a) Institution of firewalls, to prevent unauthorized communications from entering the control network |
| (b) Withholding permission for changes to routers and other components of the control network by persons not authorized to make changes |
| (c) Appropriate measures to prevent unauthorized leaks of configuration management information, such as address information for components of a control network and router packet filtering information |
| (d) Provision of functions to notify system managers in the event that data falsification is detected in a communication channel. Also, provision of functions to close networks not necessary for plant operation |

b. Measures to be taken by system managers

<p>| (a) Provision of functions for management of access of the system from outside |
| (b) Provision of functions which can be used only by specified (limited) persons to change system information |
| (c) The ability to quickly detach connections in the event that intrusion (access) from outside is discovered |</p>
<table>
<thead>
<tr>
<th>(d) Appropriate measures to prevent unauthorized access and information leaks within networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>c. Anti-virus measures to be taken by system managers</td>
</tr>
<tr>
<td>(a) In order to prevent damage by viruses, no services should be provided which can be used anonymously</td>
</tr>
<tr>
<td>d. Measures to be taken by software suppliers</td>
</tr>
<tr>
<td>(a) In order to prevent penetration of viruses, software should be manufactured and shipped with appropriate quality controls in place</td>
</tr>
<tr>
<td>e. Other measures</td>
</tr>
<tr>
<td>(a) System architecture design policies should be clarified to enable backup operation and other actions in the event that (operator) consoles freeze</td>
</tr>
</tbody>
</table>

The above measures will be formally announced in a MITI notification in the near future.

**2) Establishment of Plant Security Assessment Guidelines**

At present there are no methods available for objectively assessing and demonstrating the safety of systems composed of the products of multiple vendors. Moreover, system users are unable to objectively explain the degree of safety required. There is a need to develop some common objective measure which can be used by the designers, providers and users of products, systems and services, as standards for assessing security (for plant systems). A protection profile (PP) for control systems must be created, based on the common criteria (CC) now being studied as worldwide standards to serve as objective yardsticks for evaluating the security levels of information systems.
In addition, vendor and engineering companies must design common standards for measures at the time of plant construction (changes in network configuration and network detachment when shifting from the construction to operation stage, changes in passwords and other management information, etc.), standards for prevention of leaks of design materials and other confidential information, and measures related to remote maintenance.

With respect to remote maintenance in particular, there are threats posed by such events as identity theft as maintenance personnel, intrusion via remote maintenance circuits, wiretapping circuits, discovering dial-up telephone numbers through random dialing, and virus infection. Thus vendors also require adequate evaluation standards, beginning with identification and authentication, monitoring and inspections.

4.2 Development of Methodologies for Analysis of Threats to Network Security

In each engineering process of plant design, there is a need to perform network security risk analysis. New systematic procedures based on HAZOP, FTA, JRAM and other existing methodologies must be established for use in these analyses. And, the results of risk analysis employing these new techniques must be reflected in newly established standards for control system security evaluation.

4.3 Research and Development of Preventive Technologies

This committee represents the first instance of a forum for user, vendor, and engineering companies to meet for the purpose of discussing plant network security, and in future R&D on technology to prevent unauthorized actions will
constitute an area for deliberation by all three types of participant. For example, there is a need to study the following R&D themes, including economic viability.

(1) Application of Authentication Technologies to Control Systems

Numerous security technologies are being developed in succession predicated on use with the Internet, including user authentication, encryption, and certification authorities (CAs) within corporations. In order that these technologies may be applied in large-scale plant networks, a number of problems must first be resolved, among them issues of processing speed and ease of maintenance, operation and use. Technologies must be developed which are suitable for use in control systems.

For example, the following might be considered.

* Development of plant-specific firewall systems
* Reexamination, with a view to introduction in plant systems, of technologies which normally are too costly to consider for information systems, such as fingerprint-based authentication

(2) Development and Demonstration of High-Speed Encryption Technology

Encryption of control data is a useful means of preventing wiretapping and leaks of control data. However, in order to ensure realtime communication in control systems, processing speed and functions are given top priority; and so there is a need to develop high-speed encryption technology which detracts from processing speeds and functions as little as possible. On the other hand, communication between process computers and information systems is often allowed to deviate from realtime response more than in the case of Control System LANs, and security, rather than processing speed, must be emphasized.
Plant networks should be designed which adopt encrypted communications based on the above distinctions, and demonstration tests conducted.

(3) Study of the Development of DCS with Security Measures

DCS, and in particular controllers, are essential devices which provide signal outputs, and techniques need to be developed to prevent unauthorized access of them.

The functions of DCS and process computers are sophisticated and wide-ranging, but from a security standpoint they cannot be said to always be designed with functions divided appropriately or using products of an appropriate construction. Hereafter care must be taken to ensure that control function security is not compromised as systems become more open. There is a need to aim at function separation with a view to security as systems grow in functionality and openness, and users should be able to select necessary functions and security levels corresponding to the degree of system openness.

It will also probably be necessary to develop schemes to simplify sampling of change histories for DCS control parameters (at present, often it is not possible to sample logs for changes from sequences or higher-level systems).

(4) Mock Attack Experiments

Second-generation (UNIX) and third-generation (NT) control systems should be selected for use in attack experiments, to check for security holes.

4.4 Publicity and Education on Network Security

In Japan there is generally less awareness of security matters than in other countries, and so there is a need to publicize the importance of security in
large-scale system networks, in order to raise the general level of awareness of user, vendor, and engineering companies. In doing so, large-scale plant networks may be taken as examples in order to generate an awareness of the need for security measures at each stage of plant design, administration, operation and maintenance. At the same time, we would also like to propose that security issues for networks of vital social importance be studied by each industry, or by individual government organs. There is an especially urgent need for publicity about social engineering measures and measures to be taken in the event of remote maintenance and use of wireless communications.

In addition, international conferences should be held in order to promote the exchange of opinions and information.

4.5 Summary

The problem of security in large-scale plant networks may be regarded as one instance of the application of network security to systems of vital importance to society. Recent computer systems are vulnerable to malicious attacks from both inside and outside system networks as a result of tendencies to make connections via the Internet or other networks with other computers, with only a dim awareness of network security issues. In this day and age it is essential that, when constructing and operating large-scale facilities which have a major impact on the lives of citizens, and in particular the control systems for such facilities, we take into full consideration the need for network security.

More concretely, this committee recommends that, while bearing in mind the detailed issues raised in this and the previous chapter, companies perform checks of individual plants with a view to ensuring that the following three requirements are met.
[1] Networks and systems must be constructed with user, vendor, and engineering companies bearing joint responsibility for security. It should be recognized that corresponding investments will be necessary.

[2] The trend of the times is toward more open networks. It is essential that security be maintained even as systems become more open, without opting for solutions which impede the trend toward greater openness.

[3] Even specialized closed networks are and have typically been connected in one form or another with other systems within the company or in other business units. It is important that all persons engaged in the operation of such systems be made more aware of security issues.

It is said that Japan lags behind countries in the West in taking legal action to combat computer crime. It has been noted that indictments cannot be brought if there are no actual damages, and that punishments tend to be relatively minor. In light of the fact that unauthorized acts perpetrated against plants through computer networks may result in both vast damage and tremendous impacts on society, it is clear that, in addition to promoting autonomous preparation by companies, the government must prepare a legal framework to prevent wrongdoing in advance.
In Conclusion

The results of studies by the Large-Scale Plant Network Security Committee were finalized with the cooperation of all persons concerned. As the somewhat inexperienced committee chairman, I may have inconvenienced members in various ways, but I wish again to thank them all for their efforts.

It was in mid-summer that the initial meeting was held at MITI, members for the committee were selected, and discussions were held with assistant manager Mukai and others as to the direction the committee deliberations should take. In early autumn committee activities were begun in full attendance, each member having willingly agreed to devote time and effort. That we have been able to produce tangible results in such a short time is due to the energy with which studies were approached by the committee members, who shared an awareness of the importance of the theme at hand.

Each of the subcommittees freely made requests of the others, and as the culmination of unstinting efforts by all parties, a common understanding was reached on the various problems faced. The various activities of the subcommittees were highly fruitful.

The subcommittee leaders placed great weight on the opinions of each member, and as a result, efforts to achieve consensus were successful in each case.

The fact that, on this occasion, the various system user companies expressed their discontent with current conditions by raising problems, and the vendor and engineering firms for their parts viewed these as business opportunities in making corresponding proposals, serves I think to demonstrate the sincerity of all parties. The contents of these discussions summarized above should prove useful, even for companies not represented on the committee, in
spurring awareness of security matters, in educating employees on security issues, in devising improvements on both engineering and management levels, and in coping with future security-related developments.

It appears that there are various plans among committee members for ongoing problem resolution, and so I hope to be able to meet with all members again in future.

It is my fervent hope that this report will be highly regarded as containing valuable information of use in attaining the original objectives of the committee. I once again would like to thank all the persons associated with this committee for their generous efforts.

Tomio Umeda
Chairman, Large-Scale Plant Network Security Committee
Professor, Department of Project Management, Chiba Institute of Technology
Chairman, Management Information Committee, The Japan Petroleum Institute
Attached Materials

• Glossary

(1) Information System

Refers to an information or data processing system used for corporate accounting, personnel, sales and other processing.

(2) (Plant) Control System

A system deployed in order to control the operation of valves, pumps, compressors, and other equipment within a plant; used primarily to process control data for facilities and equipment.

(3) Large-Scale Plant Network

A large-scale hierarchical network formed by interconnection of control systems in multiple plants, and further connection with information systems within and/or outside the company.

(4) DCS (Distributed Control System)

The core of a control system, consisting of controllers, consoles, engineering computers, gateways and Control System LANs, and Control System Information LANs (but not including process computers).

(5) Information system LAN

An information system network at a business unit, connecting host computers, terminals and personal computers for staff use. Also used to connect the head office with other systems.

(6) Control System Information LAN

A network configured for each plant at a business site, connecting process computers, engineering workstations (EWS) and consoles in order to expedite engineering functions. Sometimes connected to staff personal computers as well.

(7) Control System LAN
A network, divided into plant control units, connecting controllers and consoles. Multiple Control System LANs are deployed within a plant or factory.

(8) Field Bus

A network connecting controllers with the equipment being controlled.

(9) OA (Office Automation) LAN

A network connecting personal computers and other systems used by employees at a business site to make use of the data of information systems and control systems. Sometimes installed independently of the Information system LAN.

(10) Equipment Management LAN

A network connecting specialized personal computers in order to execute equipment management functions within the business site in an integrated manner; sometimes installed independently of Information system LANs and Control System Information LANs.

(11) Controllers (and PLCs)

Controllers are hardware devices which govern plant operations; at this time, their configurations are unique for different companies.

Within controllers are housed units for analog control of quantities such as temperature and flow rates, and process control (control logic) for process stepping and other tasks. Between controllers and the site (field equipment) are electrical connections (4 to 20mA analog and digital signals, etc.); these details are not considered in this report.

In recent years there has been progress in standardizing field buses and various other kinds of field network; such networks rank as local networks installed within plants. (These also were excluded from studies.)
Where PLCs (programmable logic controllers) are concerned also, there has been a shift from the traditional independent devices toward networked devices. In this report, PLCs are considered as one kind of controller in the broad sense of the term.

(12) Consoles (POCs, Process Operator Consoles)

These are devices used to monitor the plant operating state; they enable observation of plant conditions on a CRT. (Typically several POCs are installed in each plant.)

In early DCS systems, OSes proprietary to the manufacturer were typically used, but in recent years there has been a shift to equipment using general-purpose OSes such as Unix and Windows.

Plant operators may use POCs to start and stop the control logic of controllers or change settings as the need arises.

In the past, it was rare for equipment connected to various Control System LANs such as consoles or the engineering workstations or engineering consoles described below to be connected directly to an Ethernet or other Information system LAN. More recently, however, there has been a mounting need to exchange data with closely related information systems, and so there is a growing tendencies to connect such equipment directly to Ethernet systems.

(13) Maintenance Consoles

Maintenance consoles are dedicated devices used to modify and monitor the start/stop/control logic of individual controllers.

These devices are not normally connected to controllers. (In systems where they are always connected, it is assumed that they will be operated on dedicated circuits isolated from general-purpose networks.)

(14) Engineering Consoles (ENGS)
These are program development devices for the DCS, used to modify the control logic within controllers and correct monitoring information within consoles (data displayed on the CRT, warning formats). As with consoles used to monitor operation, there is a growing tendency for these devices to run general-purpose OSes. When development of DCS programs is carried out by several engineers in parallel, engineering workstations (EWS) are connected by a general-purpose LAN, using personal computers or other equipment as input terminals.

(15) Engineering Workstations (EWS)

Whereas consoles are used principally to monitor operation, these devices provide functions supporting equipment operation, including analysis of process states and simulations to determine optimum operating parameters. Often the hardware used is the same as that providing the functions of process computers, described below.

(16) Remote Maintenance (R/M)

Remote maintenance does not refer to hardware or devices, but is rather a general term for various diagnostic tasks performed on control systems. In the past, connections tended to be by modem, using specialized procedures. Of late, however, various general-purpose procedures and protocols (Ethernet, telnet, FTP, etc.) are often used. Initially, diagnostic tasks consisted mainly of collection of information by the manufacturer to determine the robustness or pinpoint problems with system functions. More recently, however, it has also become possible to perform partial recovery from malfunctions (modification of those programs within the DCS provided by the manufacturer).

The following are representative examples of diagnostic functions that are possible through remote maintenance.
Collection of temperature, humidity, other environment data

(17) Gateway (G/W)

A gateway is hardware that relays signals between a Control System LAN (manufacturer LAN) of the DCS itself and a general-purpose LAN (Ethernet). Process computers, engineering workstations and other computers can reference and modify various plant parameters via gateways. Gateways normally exchange data with outside systems by means of protocols (procedures for referencing/setting plant data) specific to individual companies. However, these protocols are described in manufacturer documents (user manuals), and so have a low level of confidentiality. Because these devices were originally positioned as the hardware interfacing with external systems, they are the DCS component most in need of consideration from the standpoint of network security.

(18) Process Computer

Whereas the DCS handles plant control functions, the process computer governs functions for data management, principally manufacturing management and data collection functions. Depending on the system, they may be used to execute setup control or dynamic control using process models. In terms of network security, these systems are computers which adopt general-purpose technology (Unix, Windows).
(19) Wireless Application Networks and Portable Terminals (Terminals for Onsite Patrols)

With the emergence and widespread adoption of wireless application networks, wireless connections are seeing increasing use to link the portable terminals of plant operators with process control systems.

The main functions of portable terminals include

• Remote reading of onsite indicators: Instead of a controller directly measuring a process state variable, information is sent to the controller via an onsite terminal.

• Commands for operators: Auxiliary information is supplied to operators carrying portable terminals (executing onsite patrols) from consoles or workstations, such as instructions for inspection routes or information on process states collected by controllers.

At present, this equipment is used in limited applications, but in future it may emerge as a standard component of plant control equipment, used to change settings from portable terminals for instance.

(20) ERP (Enterprise Resource Planning)

An information system created primarily for the purpose of ensuring consistency among the enterprise-wide tasks and activities of a company. The salient feature of ERP systems is the fact that data used in various tasks is shared throughout the company and is used in common. Recently such systems have been commercialized as ERP packages.

(21) Plant Information Management Systems (PIMS)

Information systems used to manage in an integrated manner the information relating to plant construction, operation and maintenance.

(22) HAZOP (Hazard and Operability Studies)
A procedure for assessing the safety of plants (chemical processes). Deviations from design intentions are hypothesized, and the causes and effects of these are studied in order to examine the viability of safety measures. A team of specialists is assembled to conduct assessments.

(23) FTA (Fault Tree Analysis)

Faults or accidents and their causes are supposed, and the causal relation between phenomena and causes are described in a tree structure, in order to extract the set of causes which must be eliminated in order to avoid the phenomena.

(24) JRAM (Jipdec Risk Analysis Method)

In JRAM, system risks are analyzed using the FTA method, and at the same time a JRAM questionnaire is used to obtain and assess the subjective perceptions of risks by responsible persons in divisions using the system. The two are combined in a comprehensive report.

This method was developed in 1984 by JIPDEC (Japan Information Processing Development Center). (cf. references: "Analysis of Computer Security Risks--the JRAM Approach")

(25) Watchdog Timer

A timer used to confirm the soundness of the system. For example, a watchdog timer set to two seconds assumes that some action which can confirm system soundness is performed periodically within two seconds. By confirming that the action was completed within two seconds, or by determining that it was not, normal or abnormal operation is determined.

(26) Social Engineering

This term is used among "crackers" and "samurai" to refer to a "cracking" technique which relies on the vulnerability of "wetware"--that is, human beings--rather than software. The aim is to trick an individual into revealing a
password or other information which threatens the security of the targeted system. The classic scam involves phoning a "mark" who has the required information and posing as a field service technician or a fellow employee with an urgent access problem. (from The Hacker's Dictionary, ASCII Shuppankyoku)

(27) TCP Wrapper

TCP Wrapper is a tool on Unix hosts which provides filtering and logging functions. That is, it has functions to limit access, and to accumulate data on said access (logging), when there is a request to use a program providing ftp, telnet and other TCP-based Internet services. When there is access from an unexpected IP address or domain, this can be detected by TCP Wrapper. Because firewalls can be constructed with relative ease, it is widely used in Japan.

(28) Intrusion Detection System

An intrusion detection system is a tool for detecting and notifying managers of unauthorized intrusions via networks; however, it is also capable of detecting attempts to obstruct services. There are two techniques used to detect such events.

• Misuse detection methods

• Anomaly detection methods

In misuse detection, the techniques and features of different types of intrusion into or disruption of the system are maintained, and if phenomena with such features occur on the network being protected, a notice is issued. Each time a new method of attack is discovered, the database retained by the tool must be updated. In this respect, it is similar to computer antivirus software, the database of which must likewise be updated in order to be able to cope with new virus types. At present, most of the intrusion detection
systems sold are of this type. They are commercialized versions of systems originally used by military and government organization in the U.S.

Anomaly detection methods maintain the normal state of operation of the system, and detect the degree of any deviations from this state; if certain conditions are met, notification is issued. Statistical techniques are used to process the state of system utilization by users and other variables, in order to determine the normal state of the system; artificial intelligence is sometimes used. There are descriptions of this method in the papers presented at conferences and in journals.

At present, intrusion detection systems are developed as application systems, but logically it should also be possible to install such tools as management information blocks in standard network management protocols.

(29) Tripwire (tool for detection of data falsification)

Tripwire is a checksum tool available on Unix hosts for detection of file falsification. A checksum tool calculates and stores a number which is characteristic of the normal state of a file, and periodically recalculates the characteristic number to confirm that the value coincides with the stored value. In Tripwire, when calculating this characteristic value, one-way functions and other techniques are used to ensure that the same value is not obtained at different times. Reasons for failure to match include normal file addition, updates, deletion, and unintentional but unauthorized modifications.

Tripwire was developed by the COAST project at Purdue Univ. in the U.S. It is not much used in Japan, unfortunately, perhaps because the documentation has not been translated into Japanese.

If lack of a Japanese translation of documents is a factor impeding the introduction of Tripwire, translation should be undertaken immediately. In
addition, the functions of this tool should be installed where specialized operating systems and networks are in use.
### 用語リスト

<table>
<thead>
<tr>
<th>情報系 ＬＡＮ</th>
<th>Information System LAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>制御（系 ＬＡＮ</td>
<td>Control System LAN</td>
</tr>
<tr>
<td>不正アクセス</td>
<td>Unauthorized access</td>
</tr>
<tr>
<td>侵入</td>
<td>Intrusion</td>
</tr>
<tr>
<td>なりすまし</td>
<td>Injection</td>
</tr>
<tr>
<td>破壊</td>
<td>Destruction</td>
</tr>
<tr>
<td>サービス妨害（業務妨害）</td>
<td>Denial of service (DoS)</td>
</tr>
<tr>
<td>脆弱性</td>
<td>Vulnerability</td>
</tr>
<tr>
<td>セキュリティホール</td>
<td>Security hole</td>
</tr>
<tr>
<td>識別</td>
<td>Identification</td>
</tr>
<tr>
<td>認証</td>
<td>Authentication</td>
</tr>
<tr>
<td>暗号化</td>
<td>Encryption</td>
</tr>
<tr>
<td>復号化</td>
<td>Decryption</td>
</tr>
<tr>
<td>不正操作</td>
<td>Unauthorized operation</td>
</tr>
<tr>
<td>停止（コンピュータ、システムの）</td>
<td>Shutdown</td>
</tr>
<tr>
<td>改ざん</td>
<td>Falsification</td>
</tr>
<tr>
<td>汎用ＯＳ</td>
<td>Open OS (Operating System)</td>
</tr>
<tr>
<td>暗号</td>
<td>Cryptograph</td>
</tr>
<tr>
<td>（独自、専用）カスタムＯＳ</td>
<td>Custom OS</td>
</tr>
<tr>
<td>オープンネットワーク</td>
<td>Open Network</td>
</tr>
<tr>
<td>プロコン</td>
<td>Process computer</td>
</tr>
<tr>
<td>エンコン</td>
<td>Engineering console</td>
</tr>
<tr>
<td>オペコン</td>
<td>Operator console</td>
</tr>
</tbody>
</table>

(*)シンポジウム(99/10/01)講演資料内で使用