

Critical Alert for Cyber Terror

WHITE PAPER

Security for Nation's Infrastructure (SCADA & DCS)

: 2002 10 31 (4335)

(winsnort@securityindepth.net)
winsnort@hotmail.com

© Copyright 2002 sanghun , Jeon . All rights reserved.

Table of Contents

.....	3
.....	4
CONTENTS	6
.....	6
.....	13
Infra Structure Control System	15
.....	18
.....	20
SIMULATION	23
Cyber Attack simulation	23
SECURITY PLAN	25
Security Policy.....	25
Security Technic	25
Security for Future	26
REFERENCE	27
BIBLIOGRAPHY	28
ABOUT MY LIFE	29



가

?

2002 9
SPACE”

Cyber
가

“The national strategy To SECURE CYBER

SCADA system DCS

가

가 가

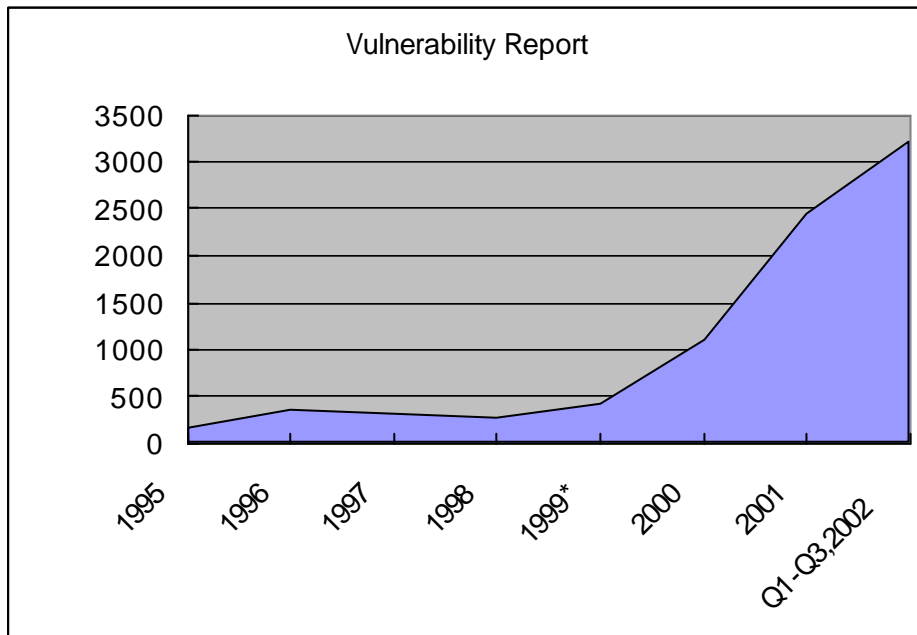
가

Contents

www.cert.org

1995	1996	1997	1998	1999*	2000	2001	Q1-Q3,2002
171	345	311	262	417	1,090	2,437	3,222

가 2000 . 2002 9



가 가 가가 가 가

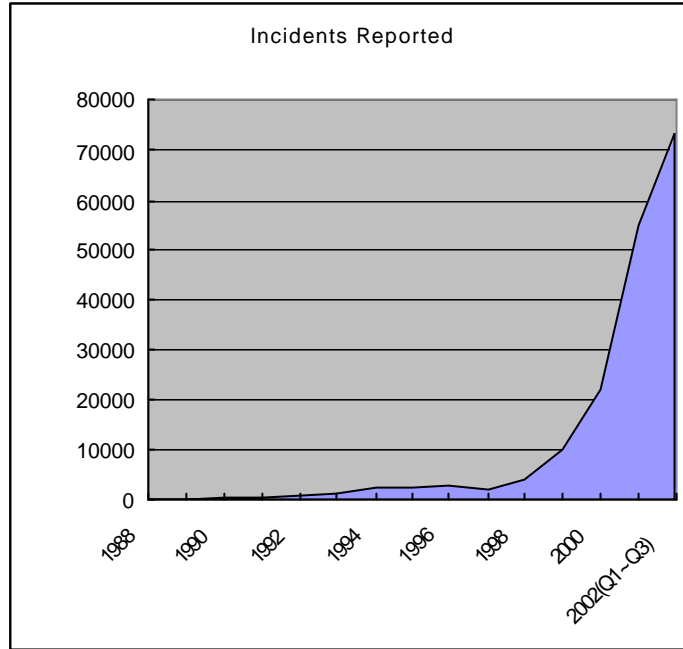
www.cert.org

가

2000

가

Year	Incidents reported
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1334
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999	9869
2000	21576
2001	54658
2002(Q1~Q3)	73359



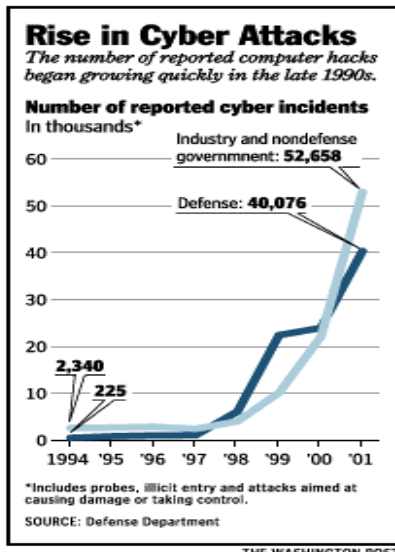
2000

가

IT

가

가

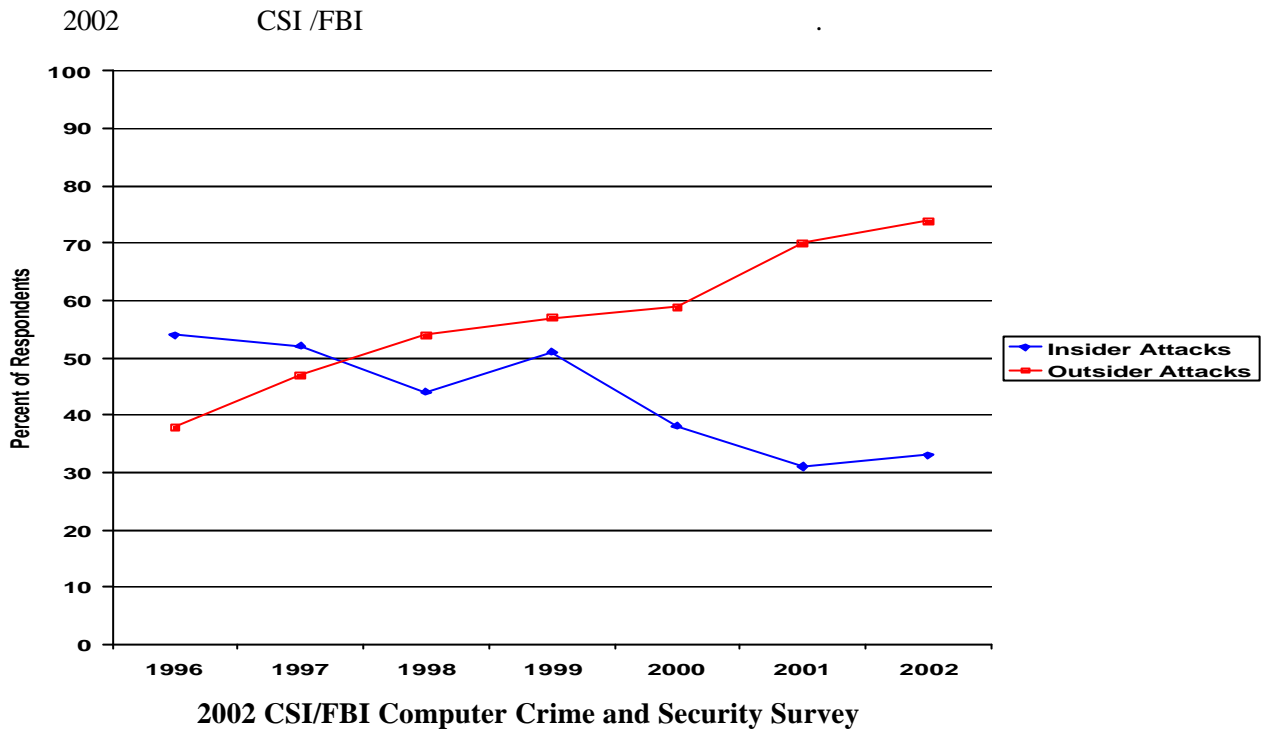


Defense Department
Cyber Attacks statistic

90

가

가



1999
가

IT

가

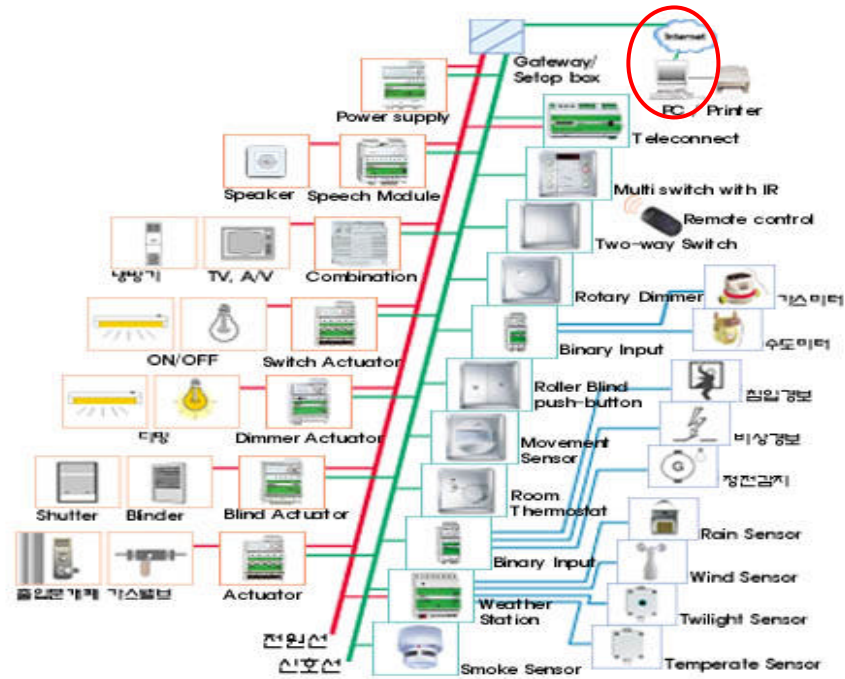
가

Home Network Home

Automation
가

Home Network

* 가 Image



2 - Sample Home Automation Network

2 Home Network
offline

. Home Network
가

PC

가

PC

Home Automation Home Network



* image

Home Server : TCP /IP
LCD

RF

*

Home Gateway:

*

TCP/IP
LCD

RF

PLC

, ARS

Web Pad:

*

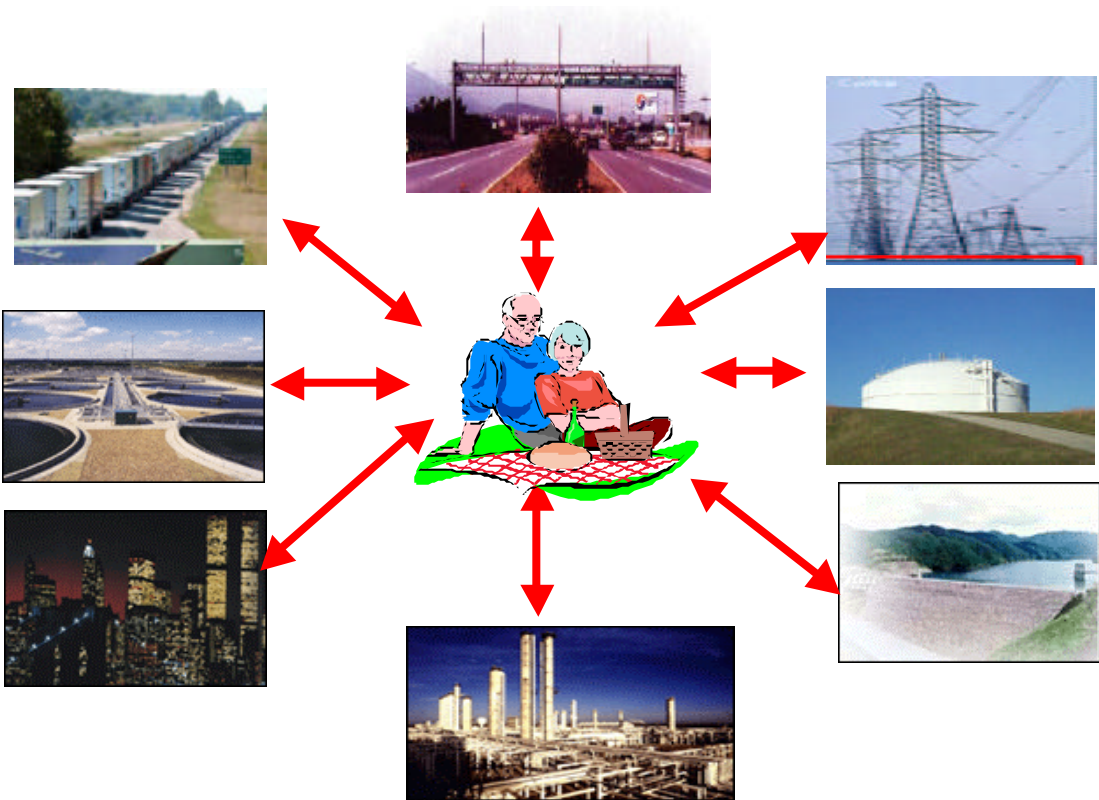
가

/IP
가

TCP
가

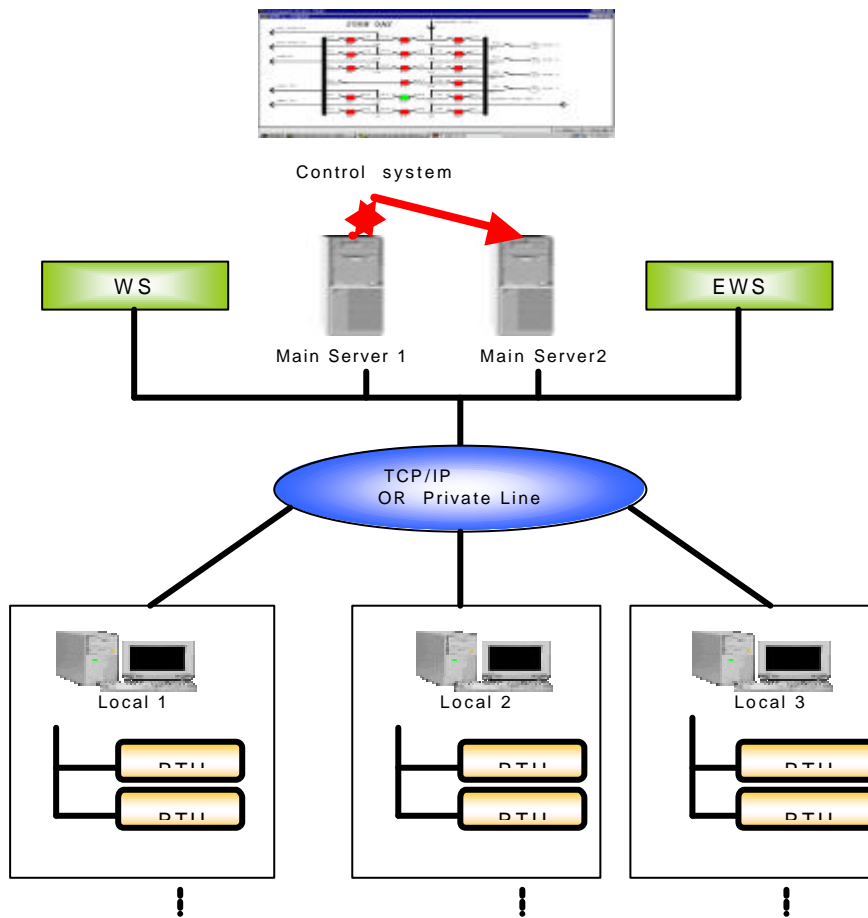
IT

가



WS: Work Station – Factory Automation , Computer Intergrated Manufacturing

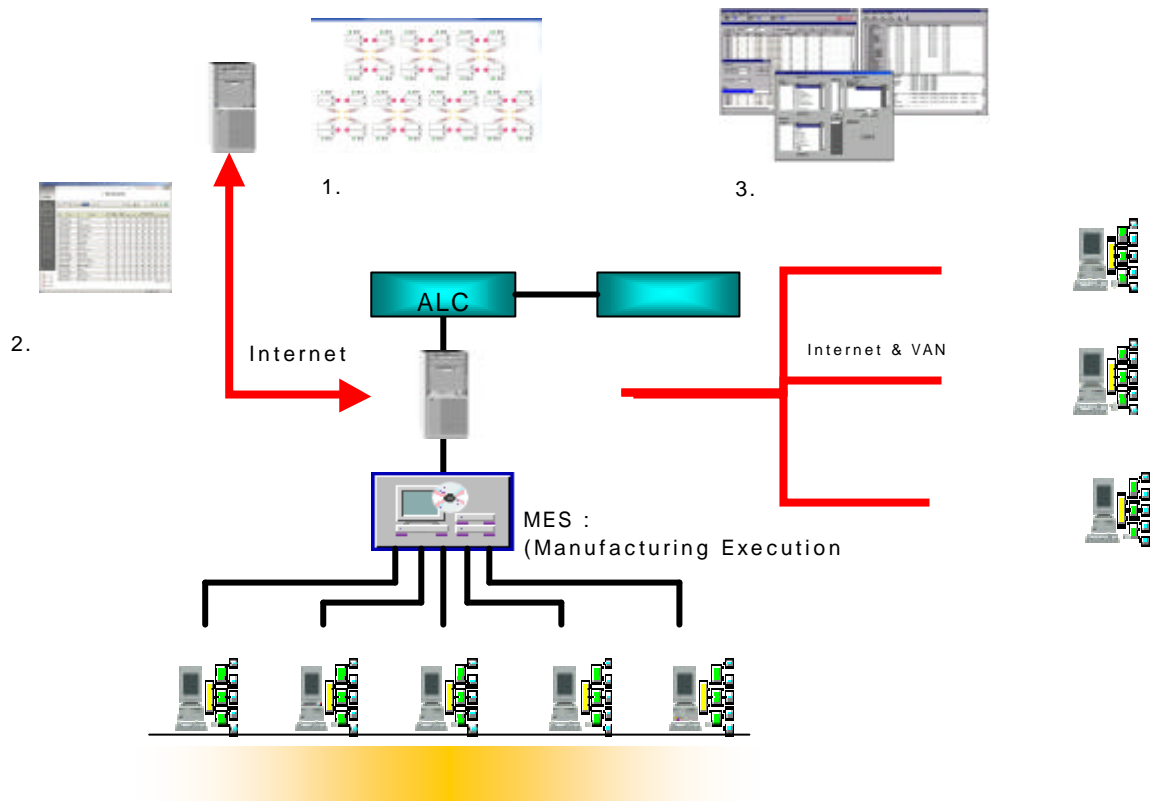
EWS: Engineering Work Station , WS FA



1,2,3

IT

가



IT

IT

가

Cyber Terror Cyber war

DCS (Distributed Control System)

SCADA (Supervisory Control and Data Acquisition)

1. Counterterrorism analysts have known for years that terrorists often prepare for attacks with elaborate "targeting packages" of photographs and notes. But, in January, U.S. forces in Kabul, Afghanistan, found something new. A computer seized at an al Qaeda office contained models of a dam, made with structural architecture and engineering software, that enabled the planners to simulate its catastrophic failure. Bush administration officials, who discussed the find, declined to say whether they had identified a specific dam as a target. The FBI reported that the computer had been running Microstran, an advanced tool for analyzing steel and concrete structures; Autocad 2000, which manipulates technical drawings in two or three dimensions; and software "used to identify and classify soils," which would assist in predicting the course of a wall of water surging downstream. To destroy a dam physically would require

"tons of explosives," Assistant Attorney General Michael Chertoff said a year ago. To breach it from cyberspace is not out of the question.

<http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A50765-2002Jun26¬Found=true>

가
cyber terror
Microstran 2D, 3D 가
autocad 2000
Cyber 가 9

2. In 1998, a 12-year-old hacker, exploring on a lark, broke into the computer system that runs Arizona's Roosevelt Dam. He did not know or care, but federal authorities said he had complete command of the SCADA system controlling the dam's massive floodgates. Roosevelt Dam holds back as much as 1.5 million acre-feet of water, or 489 trillion gallons. That volume could theoretically cover the city of Phoenix, down river, to a height of five feet.

<http://www.itsa.org/ITSNEWS.NSF/4e0650bef6193b3e852562350056a3a7/3f141fc26dcebd5a85256be600617016?OpenDocument>

1998 12
12 SCADA system
489
400 5

3. In Queensland, Australia, on April 23, 2000, police stopped a car and found a stolen computer and radio transmitter inside. Using commercially available technology, Vitek Boden, 48, had turned his vehicle into a pirate command center for sewage treatment. Boden's arrest solved a mystery that had troubled the area's wastewater system for two months. Somehow the system was leaking hundreds of thousands of gallons of putrid sludge into parks, rivers and commercial properties. Until Boden's capture -- during his 46th successful intrusion -- the utility's managers did not know why. Specialists in cyber-terrorism have studied Boden's case because it is the only one known in which someone used a digital control system deliberately to cause harm.

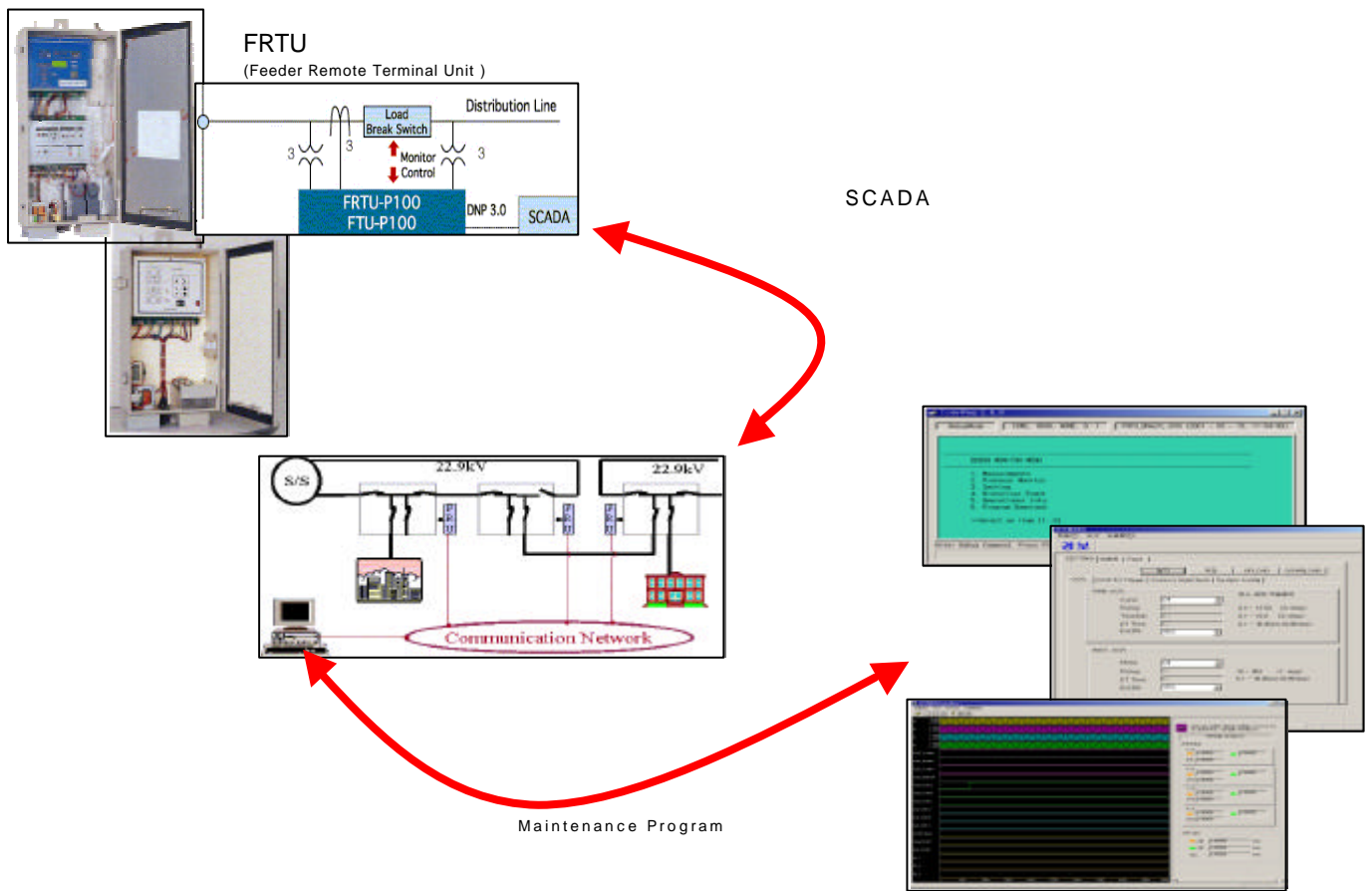
<http://www.theregister.co.uk/content/4/22579.html>

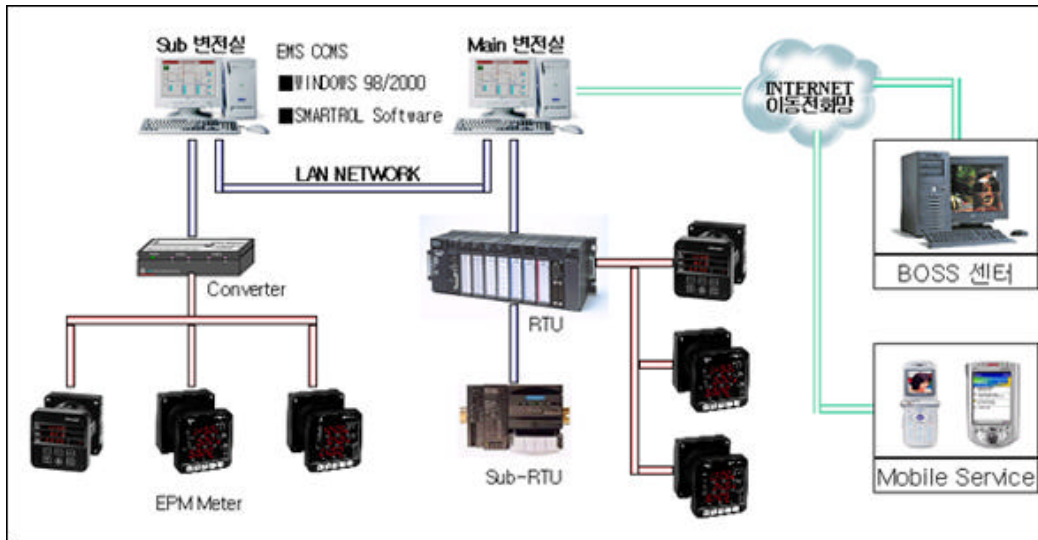
1,2 SCADA 2000 4
Vitek Boden 가 2
40

가

Infra Structure Control system

SCADA (Supervisory Control and Data Acquisition)





가
Mobile Service

MODICON (Modular Digital Controller)
ABB

RS-485,

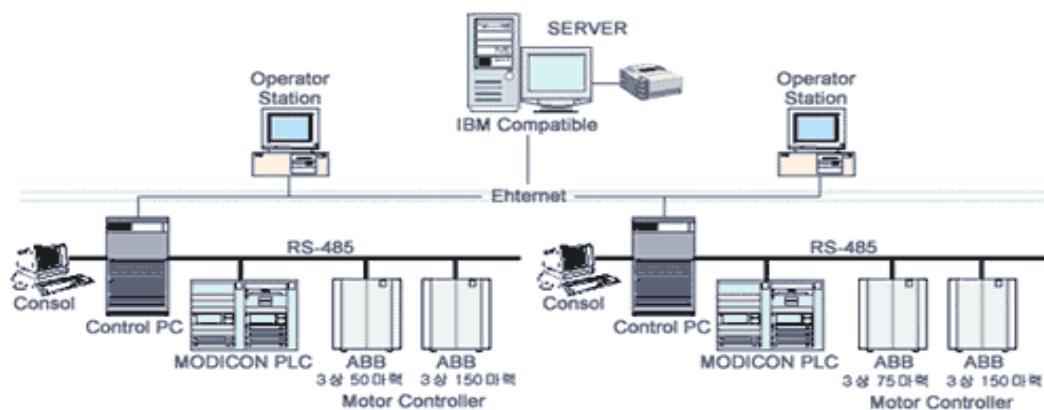
PC
(Programmable Logic Controller)

PLC

Control PC

PLC

Control PC 가

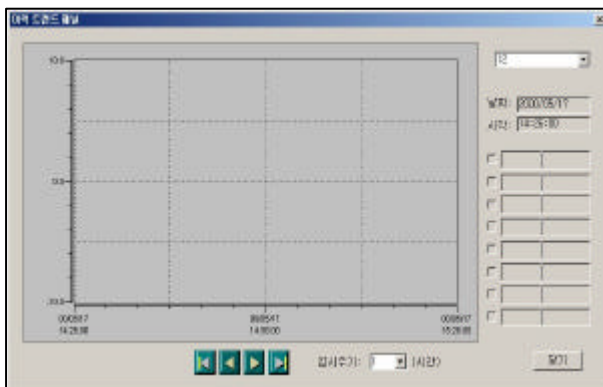
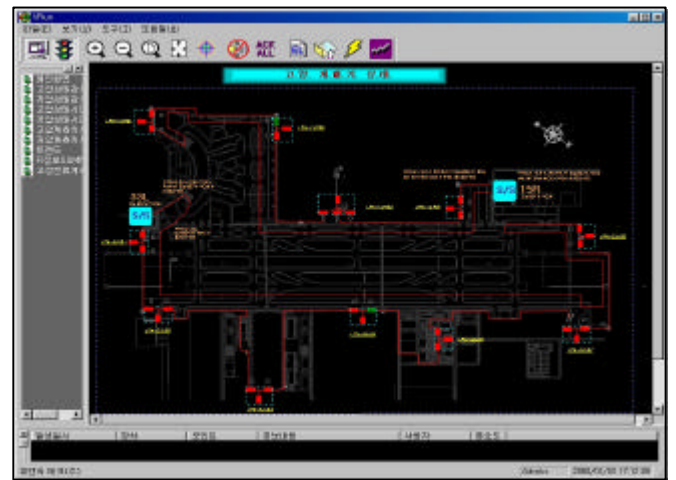
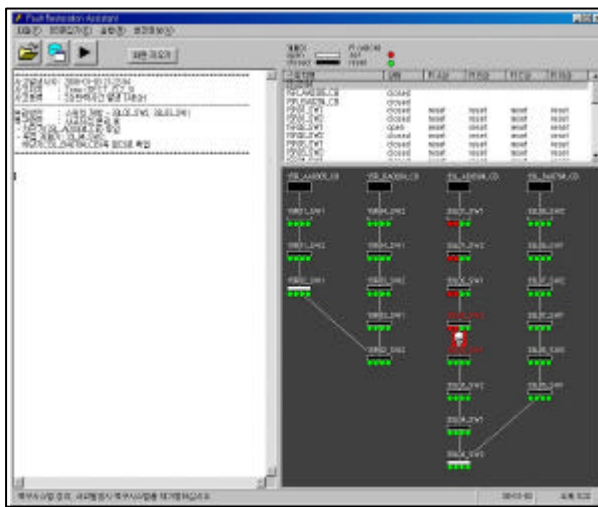


SCADA , DCS

IT

가
가

Visual



The screenshot shows a SCADA/DCS interface with an Event Summary table. The table has columns for ID, NAME, UNIT, TYPE, STATUS, VALUE, and ACTION. The data in the table is as follows:

ID	NAME	UNIT	TYPE	STATUS	VALUE	ACTION	
SYSTEM	1999-09-21 ...	dev1	A1	Data.Chang...	15.0	HIGH	pdv
ALARM	1999-09-21 ...	dev2	D1	Open	0.0	DEFAULT	cey pnd
USER	1999-09-21 ...	dev3	A2	Data.Chang...	20.2	LOW	std pne
SYSTEM	1999-09-21 ...	dev1	A1	Data.Chang...	15.0	HIGH	pdv
ALARM	1999-09-21 ...	dev2	D1	Open	0.0	DEFAULT	cey pnd
USER	1999-09-21 ...	dev3	A2	Data.Chang...	20.2	LOW	std pne
SYSTEM	1999-09-21 ...	dev1	A1	Data.Chang...	15.0	HIGH	pdv
ALARM	1999-09-21 ...	dev2	D1	Open	0.0	DEFAULT	cey pnd
USER	1999-09-21 ...	dev3	A2	Data.Chang...	20.2	LOW	std pne
SYSTEM	1999-09-21 ...	dev1	A1	Data.Chang...	15.0	HIGH	pdv
ALARM	1999-09-21 ...	dev2	D1	Open	0.0	DEFAULT	cey pnd
USER	1999-09-21 ...	dev3	A2	Data.Chang...	20.2	LOW	std pne
SYSTEM	1999-09-21 ...	dev1	A1	Data.Chang...	15.0	HIGH	pdv
ALARM	1999-09-21 ...	dev2	D1	Open	0.0	DEFAULT	cey pnd
USER	1999-09-21 ...	dev3	A2	Data.Chang...	20.2	LOW	std pne

*

SCADA DCS

1. 가

, 가 IP 가
CRM(Customer Relation Management) , CIM(Computer Intergrated Manufacturing)

, 가

가 PC
IDS Firewall ,
가 가

2. Utility Tool 가

SCADA DCS Utility
Tool

Utility 가 가
IDS Firewall

가 가 가가 가
Utility Tool 가

3. Vendor 가)

가 가 가 가 가 가 가 가

: <http://www.hani.co.kr/section-005000000/2002/10/005000000200210142158142.html>

4. 가 Remote management tool
가

IDC (Internet Data Center)
가

Server , VNC IDC 가
PC Anyware , Terminal
SCADA & DCS

2~3 ACL

Orifice , Net bus , Netcat , Key Logger 가
Back

가

가

가

3가

1.

가

2. SCADA

SCADA

가
가

Hot Line

3. SCADA

가

가

SCADA

70
가

가

SCADA

Update

가

~~SCADA~~

~~SCADA~~

~~SCADA~~

~~SCADA~~

~~SCADA~~

~~SCADA~~

25

:

1. Web site

2. DNS Server Zone-Transfer Transfer 가가 가 IP

:

1. FTP, WEB , Mail Server

가

2.

, IDS , VPN 가

3.

4.

가

가

:

1.

가

2. IDS 가

SCADA

:

1. User Interface

VB, ODBC

RAD

가

A.

2.

가

TCP/IP

A.

가

SCADA

1. 가 .
2. RTU IED IP 가 가 .
3. Device Protocol (ex . UCA /MMS & DNP)
가
- OSI 가 .
UCA: Utility communication Architecture
MMS: Manufacturing Message Specifications
DNP: Distributed Network Protocol
4. Legacy Legacy .
5. .
6. 가 Utility Protocol TCP/IP PLC 가 .

SIMULATION

Cyber Attack simulation

1.

가

DMZ Webservice Mail Server

 IP

 Internal Firewall

 DMZ

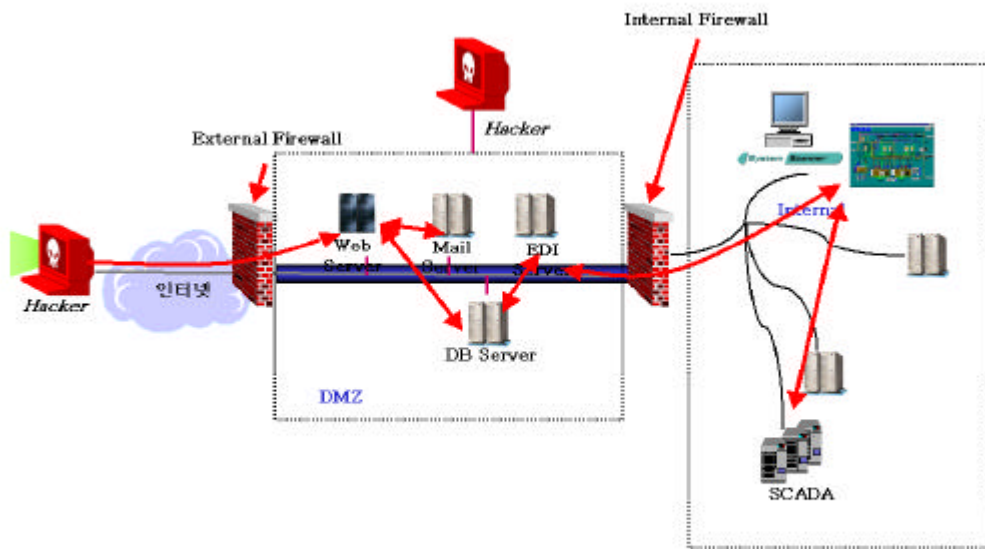
Internal Firewall Sniffer

 DB

 가 가

 Internal Network

 SCADA

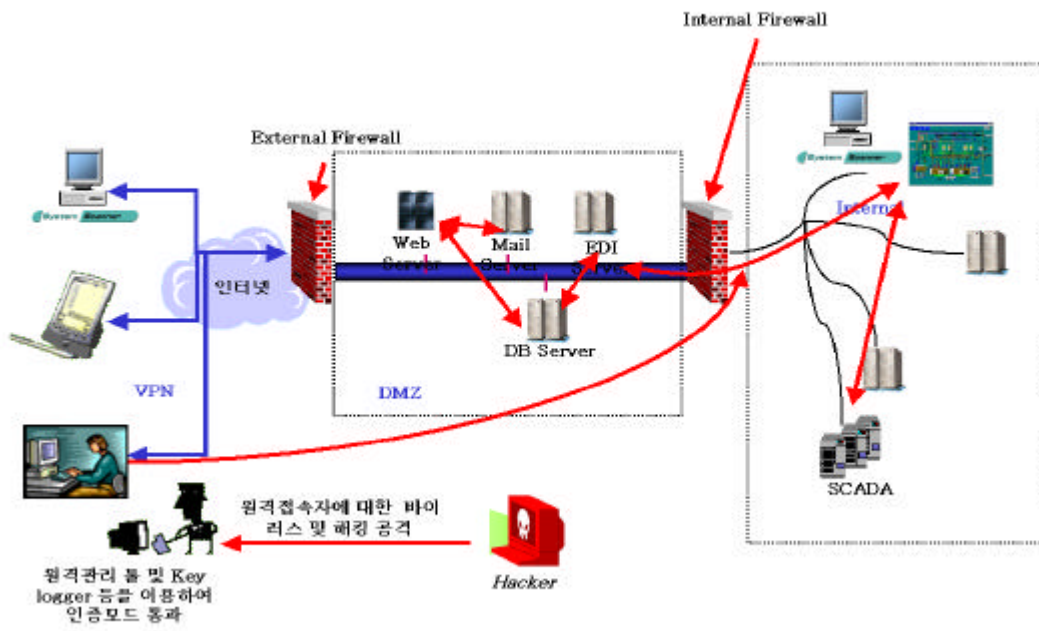


2.

가

PC

ID



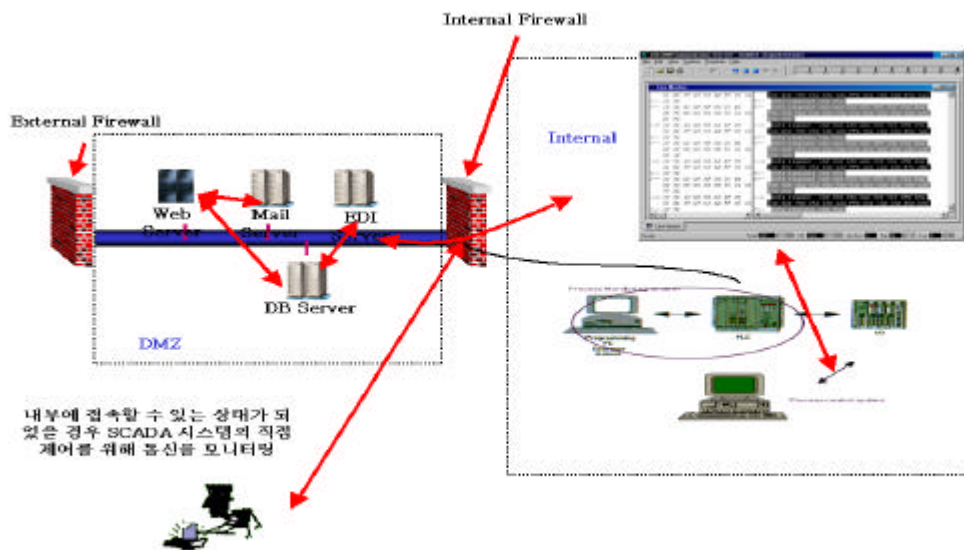
3. DMZ

SCADA system

SCADA & DCS

PLC (Programmable Logic Controller)

. PLC



i. IDS , Firewall , Router

ii.

ESM

iii.

iv.

가

v.

가

Managed Security

vi.

가

Security for Future

가

가

가

가

가

가

가

가

1,2

가

1.

2. 가

Security

3.

가

4.

5.

6.

References

1. <http://www.washingtonpost.com/wp-dyn/articles/A50765-2002Jun26.html>
가
2. <http://www.nwfusion.com/news/2002/0918experts.html>
“Security experts weigh in on cybersecurity plan” By Paul Roberts ,IDG News Service, 09/18/02
3. <http://www.usatoday.com/life/cyber/tech/2001-06-19-cyberwar-full.htm>
“Cyberspace: The next battlefield “ By Andrea Stone, USA TODAY
4. <http://www.computerworld.com/industrytopics/energy/story/0,10801,61313,00.html>
“California hack points to possible IT surveillance threat” DAN VERTON June.12 2001
5. <http://online.securityfocus.com/news/474>
“Feds, Industry, Battle the Biggest Bug” Kevin Poulsen, Jun 12 2002 12:00AM
6. <http://online.securityfocus.com/news/502>
“U.S. Fears Al Qaeda Cyber Attacks” *Barton Gellman*, Washington Post Jun 26 2002 3:59PM
7. <http://www.itsa.org/ITSNEWS.NSF/4e0650bef6193b3e852562350056a3a7/3f141fc26dcebd5a85256be600617016?OpenDocument>
“Internet-Based And Remotely-Controlled Public Infrastructure And Utility Networks More Vulnerable Than Previously Thought “ June 28, 2002
8. <http://www.theregister.co.uk/content/4/22579.html>

Bibliography

“The National strategy to SECURE CYBER SPACE” September, 2002 The President’s Critical Infrastructure Protection board

<http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf>

“Real time Information Protection” Riptech technology.

<http://www.energyitexpo.com/presentations/belcher.pdf>

“Securing supervisory control & data acquisition” Abdo Y.saad ,M.S

http://www.undergroundinfo.com/PGI/pgj_archive/July02articles/securing-supervisory.pdf

“Common Vulnerabilities in Operational Networks” Riptech technology

<http://www.energyitexpo.com/presentations/stempfle.pdf>

“SCADA Security Strategie” , Jonathan Pollet, PlantData Technologies August 8, 2002

<http://www.plantdata.com/SCADA%20Security%20Strategy.pdf>

“Can Hackers Turn your light off?” Jonathan Stidham , September 26 . 2001

<http://www.digital-minds.org/General/lights.pdf>

About My Life

가 가 가 .. 가

가 가 1 가 가 .

) (

가 Cyber 가 .

:
- 2 .
- ...
-

* 가 .

“ 가 ..”