Attack Resilient Cyber-Physical Systems for Industrial Automation & Control

By

Dr. S. Rominus Valsalam
Associate Director & Head
Control & Instrumentation Group
Centre for Development of Advanced Computing (CDAC)
(A Scientific Society of the Ministry of Communications and Information Technology, Govt. of India)
Vellayambalam, Thiruvananthapuram - 695 033, Kerala, India.
### Changing Horizons of Automation & Control Technology

<table>
<thead>
<tr>
<th>Physical World</th>
<th>Virtual Environment Before Real-World Realization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Climate Protection</td>
<td>Digital Factory</td>
</tr>
<tr>
<td>Artificial Intelligence Rule Based / Neural</td>
<td>Biological Systems “Life Forms”</td>
</tr>
<tr>
<td>Software-Based (Execute via Command)</td>
<td>Holonic Control System</td>
</tr>
<tr>
<td>Hardware Based (Dumb)</td>
<td>Learning System</td>
</tr>
<tr>
<td>Relay I/O Modules</td>
<td>Programmable Controls</td>
</tr>
</tbody>
</table>

#### Notations
- **Relay I/O Modules**: Hardware Based (Dumb)
- **Programmable Controls**: Software-Based (Execute via Command)
- **Learning System**: Artificial Intelligence Rule Based / Neural
- **Holonic Control System**: Artificial Intelligence Rule Based / Neural
- **Biological Systems “Life Forms”**: Artificial Intelligence Rule Based / Neural
- **Digital Factory**: Virtual Environment Before Real-World Realization
- **Climate Models**: Global Climate Protection
IMPORTANCE OF PLANT MODELS

CONVENTIONAL CONTROL SYSTEM

- Set point
- Controller
- Process
- Black Box
- Controlled Variable
- Steady State Error
- Time

ADVANCED CONTROL SYSTEM

- Set point
- Controller
- Process
- Sensor
- Estimate Measurement
- Estimate
- Process
- Environment
- Sensor
- Understand and Adapt
- PROCESS MODEL
- ESTIMATOR
- Manipulated Variable
- Steady State Error
- Time
OVERVIEW OF SCADA SYSTEM FOR A CHAIN OF HYDEL POWER STATIONS

PHANSIDEWA
(Administrative Building)

RADIO LINK
2.4 TO 2.5 GHz
2.4 TO 2.5 GHz
2.4 TO 2.5 GHz

PS-I SCADA SYSTEM
PS-II SCADA SYSTEM
PS-III SCADA SYSTEM
Cement Plant Rotary Kiln Control Optimization System

**CDAC System**
- Kiln Optimization Workstation
- Reinforces Setpoints $R_s, C_s, \& P_s$
- FUZZY LOGIC INTELLIGENT DECISION SYSTEM

**SIEMENS System**
- OPC Console
- Siemens 417 – 4H Controllers
- Siemens Panel
- Field I/Os (~3000 nos.)

**Kiln Control Room**
- OPC
- Raw Meal Feed Rate
- Preheater fan speed
- Coal Feed Rate
- Kiln Speed
- Back-end Temp
- CO Content
- Burning Zone Temp
- Kiln Ampere

**DAS Room**
- PID Controller
- Coal Feeder
- Raw Meal Feeder
- Preheater Fan
- IPA Controllers
- $C_s$ & $P_s$

**Kiln Process**
- Schenk Controller
- M
- Field I/Os (~3000 nos.)
- Durag Camera
- Preheater fan
- Cyclones
- Coal feed
- Raw Meal

**Reinforcement Setpoints**
- $R_s$, $C_s$, $P_s$
Complex Measurement of Crystal Size in Sugar Industry - Through Image Processing

Raw Water supply

Solenoid valve

Pneumatic cylinder

Solenoid valve

Air supply

Solenoid valve

Vacuum Pan

Spray Water Nozzle

Slots for Sample

Spreading brush

Cleaning brush

6mm thick glass

Reject sample

Smart camera

Solenoid valve

Display Unit

Control unit

Control & Instrumentation Group

IIPTeC - Sugar Crystal Size Characterization
Energy Crisis

Solar thermal power industry

- Growing rapidly

- 1.2 GW under construction (April 2009)

- 13.9 GW announced through 2014.

- Spain is the epicenter of solar thermal power development with 22 projects for 1,037 MW under construction.

- United States 5,600 MW of solar thermal power projects have been announced.
Behaviour of Cyber – Physical System in Modern Solar Power Plants and Control Problems

- Collectors movement (sun tracking)
  - Slow
  - Open loop (almost)

- Temperature and pressure control
  - Rich dynamics (PDEs, deadtimes, nonlinear, ...)
  - High disturbances
  - Closed loop (almost)
Why controlling the solar plants is a challenge?

- The energy source is not a manipulated variable but a perturbation!
- Complex dynamics: Non linear, PDE, dead time, never at a steady state
- Constraints (operating closed to constraints)
- Deciding the operating mode is part of the control strategy.
MPC vs. PID

PID: \[ u(t) = u(t-1) + g_0 e(t) + g_1 e(t-1) + g_2 e(t-2) \]
Cloud based SCADA offers Alternatives to Traditional Systems

Service provider purchases and maintains a shared pool of configurable computing devices

- Networks
- Servers
- Storage
- Applications
- Services

Water and waste water industry access these resources via the internet

They pay for the Capacity used

Cloud SCADA limits the need for

- H/W & S/W purchase
- Installation
- Maintenance
- System upgrade
Need for Industrial Control System Security
Secured Automation System with Cloud Architecture

Cloud

- Security Gateway 1
- Security Gateway 2
- Wireless Security Manager
- Wireless Network Manager
- Attack Resilient Process Controller
- Intrusion Detection Analysis System
- Backbone Router/Base station
- Wireless IDS
- WFD

Inputs/control commands

FIELD I/Os

SERVER OPERATOR CONSOLE 1 OPERATOR CONSOLE 2 LEAKAGE DETECTION SYSTEM CHEMICAL ADDITION OPTIMIZATION SYSTEM SIMULATION-DRIVEN OPTIMIZATION SYSTEM

Cloud Security Gateway 1 Security Gateway 2

- Inputs/control commands
- Security Gateway 1
- Security Gateway 2
- Attack Resilient Process Controller
- Intrusion Detection Analysis System
- Backbone Router/Base station
- Wireless IDS
- WFD

Cloud

Secured Automation System with Cloud Architecture
Comparison of security requirement for general Information Systems and Automation and Control Systems

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Security Requirement</th>
<th>General Information Systems</th>
<th>Automation and control systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Primary subject for protection</td>
<td>Information</td>
<td>Physical process/plant</td>
</tr>
<tr>
<td>2.</td>
<td>Primary risk impact</td>
<td>Information disclosure, financial</td>
<td>Safety, health, environment, financial</td>
</tr>
<tr>
<td>3.</td>
<td>Security focus</td>
<td>Central server security</td>
<td>Control device stability</td>
</tr>
<tr>
<td>4.</td>
<td>Availability</td>
<td>95 – 99%</td>
<td>99.9 – 99.999…%</td>
</tr>
<tr>
<td>5.</td>
<td>Determinism</td>
<td>Hours to months</td>
<td>Milliseconds to hours</td>
</tr>
<tr>
<td>6.</td>
<td>Operating environment</td>
<td>Interactive, transactional</td>
<td>Interactive, real-time</td>
</tr>
<tr>
<td>7.</td>
<td>Problem response</td>
<td>Reboot</td>
<td>Fault tolerance, on-line repair and restoration</td>
</tr>
</tbody>
</table>
Power and Energy System Control Applications and Cyber – Physical System Security Needs

**Physical System**

**Control Applications**
- Automatic Voltage Regulator (AVR)
- Governor Control
- Automatic Generation Control
- Generation Process Control
- State Estimator
- VAR Compensation
- Wide-Area Monitoring System
- Load Shedding
- Advanced Metering Infrastructure (AMI)
- Demand Side Management

**Typical SCADA Vulnerabilities**
- Communication links
- Digital Controllers
- Tie-line flow and Frequency Control Algorithms
- PMUs vis-a-vis GPS Technology
- FACTS Devices

**Emerging Security Solutions**
- Risk Assessment
- Intrusion Detection and Risk Mitigation
- Attack resistant Robust Controllers
- Attack resistant PMUs and Wireless Sensor Networks.
- Attack Resilient Control Algorithms

**FACTS - Flexible Alternating Current Transmission System**
Can we hop over existing barriers to forge a different future?

From Eagleson, 2002
Need for Cyber-Physical System Security

Security Issues in ICS

- Adoption of standardized protocols and open technologies with known vulnerabilities
- Connectivity of the control systems to other networks/Internet
- Insecure and rogue connections
- Widespread availability of technical information about control systems
- Use of standard OS like Windows
ICS Security incidents

Incidents of cyber-security nature that directly affected Industrial Control Systems and processes
Percentage of critical infrastructure enterprise executives reporting large-scale DDoS attacks and their frequency (source: McAfee) – IEEE P&E Magazine, Jan/Feb 2012
Security Incidents on SCADA Systems

- Siberian Pipeline Explosion (1982) - Trojan
- Chevron Emergency Alert System (1992) – User Compromise
- Salt River Project (1994) – Trojan
- Worcester, MA Airport (1997) – Root Compromise & Denial of Service
- Gazprom (1999) – User Compromise & Trojan
- Davis-Besse Nuclear Power Plant (2003) – Worm
- CSX Corporation (2003) – Virus
- Tehama Colusa Canal Authority (2007) – Misuse of Resources
- Stuxnet (2010) – Worm, Root Compromise, Trojan
- Night Dragon (2011) - Social Engineering, User Compromise, Root Compromise
- DUQU (2011) - Virus
- Flame (2012) – Worm

Contd…..
- Russian-Based Dragonfly Group Attacks Energy Industry (2014) - Power and Utilities United States
- U-2 spy plane caused widespread shutdown of U.S. flights: report (2014) - Transportation United States
- After ‘Godzilla Attack!’ U.S. warns about traffic-sign hackers (2014) - Transportation United States
- Public utility compromised after brute-force hack attack, says Homeland Security (2014) - Power and Utilities United States
SCADA Security Incidents - Examples

- Worcester Air Traffic Communications (March 1997)
  Disabled part of the PSTN using a dial-up modem - airport control and communication system affected, radio transmitter that activates runway lights were shut down

- Maroochy Shire Sewage Spill (2000)
  Using a radio transmitter, the control system for sewage pumping station was interrupted on 46 occasions causing malfunctions resulting in the release of about 264,000 gallons of raw sewage into nearby rivers and parks

- Northeast Power Blackout (August 2003)
  Failure of the alarm processor in the SCADA system prevented control room operators from having adequate situational awareness of critical operational changes to the electrical grid, leading to an uncontrolled cascading failure of the grid. A total of 61,800 MW load was lost as 508 generating units at 265 power plants tripped.

- Stuxnet Worm (2010, 2012)
  Latest widely published cyber attack on ICS. The objective was to corrupt Siemens PLC function by rewriting parts of the code and turning it into the attacker’s agent. Target was nuclear power plants, power grids.
  On 25 December 2012, an Iranian semi-official news agency announced there was a cyberattack by Stuxnet on the industries in the southern area of Iran.
How STUXNET Worked

1. Infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. Search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. Update
If the system isn’t a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. Compromise
The worm then compromises the target system’s logic controllers, exploiting “zero day” vulnerabilities—software weaknesses that haven’t been identified by security experts.

5. Control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. Deceive and Destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won’t know what’s going wrong until it’s too late to do anything about it.
SCADA Vulnerabilities

Architectural vulnerabilities
• Weak separation between process network & field network
• Lack of authentication among the active components

Security Policy vulnerabilities
• Patch management policies
• Anti virus update policies
• Access policies

Software Vulnerabilities
• Buffer overflows
• SQL-injection
• Format string
• Web-application vulnerabilities

Communication Protocols Vulnerabilities in
• DNP 3.0 (IP based)
• IEC 870-part 5 101 profile
• IEC 870 part 5 104 profile (IP based)
• Inter Control Centre Protocol (ICCP, IP based)

Wireless vulnerabilities
Vulnerabilities in field devices with Ethernet interface– PLCs, RTUs, IEDs etc
SCADA aware Security gateway
- Firewall – Modbus TCP, DNP3, ICCP
- IDS – Signature and behaviour anomaly based
- Bump-in-the-wire

Secure SCADA Protocols
- Security Layer for ICCP TASE.2, MMS Protocol Layers
- Security Layer for IEC 61850 Protocol

Hardware/software hardened secure SCADA
- RTU – OS Hardening, Role based access control, data authentication
- DACS (proprietary) protocol – Challenge / Response
- SCADA/HMI - Role based access control, Biometric authentication, control data encryption, SCADA configuration hardening
- Security hardened WSN – IEC 62591 (WirelessHART)
Development of Building Blocks

Attack resilient control algorithms

- Robust networked control
- State controller - Robust Kalman Filter with Bernoulli Loss Model
- $H^\infty$ Control - system with unpredictable structural changes
- Fault-Tolerant control using data fusion and state observer
- Power System Simulation, Collocation and Control
- State Estimation

End point security framework in SCADA

- Whitelist framework for SCADA security with Application control, Network Access Control, USB mass storage device and USB communication device device control for Windows and Linux based end points
- Mobile security solution with application aware firewall, anti malware and Offline mobile application analyser features for Android based mobiles
Security Testing Tools

- Attack simulators
  - SCADA malware DoS (APT) Scenario
  - SCADA unauthorized command execution scenario
  - SCADA System Data Poisoning
- SCADA protocol fuzzers – Modbus TCP, DNP3, ICCP

SCADA Forensics and Incident Response tools

- Forensics acquisition and analysis of
  - Computers on a SCADA network
  - RTU/PLC
  - Intelligent field devices
Security tools for Wireless Field Devices

- Wireless Security Analyser and Detector
  - Wireless Security Analysis system – IEC 62591 (WirelessHART)
  - Intrusion Detection System

Attack modelling framework & tool

- Fault Tree Analysis (FTA)
- Attack Trees
- Petri Nets

Monitoring and Management tools for Risk Assessment

Auditing tool based on SCAP protocol
Secure RTU Architecture

- Policies: RBAC, Data Integrity
- CPU with Hardened LINUX OS
- Security Enhanced SCADA Protocol with Challenge Response Authentication
- RBAC – Role Based Access Control

Server

Console 1

Console 2

NW Switch

DI, AI, DO, AO

SENSORS AND ACTUATORS
Challenge / Response Authentication for RTU Master Communication

If $H! = \text{HASH}(N|S)$
Reset Connection
SELinux (Security Enhanced Linux) provides enhanced security
- A set of kernel modifications and user-space tools that can be added using LSM (Linux Security Modules)
- Configurable policy engine supporting:
  - Type Enforcement (TE), Role Based Access Control (RBAC)
- Type Enforcement (TE) is the mechanism that actually determines if a particular operation is permitted
- The Type Enforcement technology feature of the operating system provides strong separation of:
  - The operating system from applications
  - Applications from each other
Security Hardened SCADA Software

• Enrich the web based SCADA application with strong security features
  ➢ User authentication with role based access
  ➢ Use of strong multi-factor user authentication via biometric interfaces and strong passwords
  ➢ Improved Web Application Security by the use of secure data transfer between server and client using technologies like SSL
  ➢ Encryption of control data
  ➢ Secure configuration database using database encryption
  ➢ Use of electronic signatures
  ➢ Protocol hardening by using a secure SCADA protocol for communication with the RTU
• Develop ICCP Server and Client interfaces for the SCADA software
Security Hardening of Wireless Sensor Network
Objectives

To harden the existing wireless sensor network system for industrial automation developed under the ASTeC programme funded by DeitY.


2. Design and Implementation of IEC 62591 (WirelessHART) standard based security features on Backbone Router (Base Station).


WiSArD- Architecture

Wireless Security Analyzer & Detector (WiSArD)

- Intrusion Detection Tool
- Network Monitoring Device
- Intrusion Detection System

- Threat Simulator & Analysis Tool
- Attack Injector Module
- Security Analysis System

Security Manager
Network Manager

Wireless Sensor Network
Attack Resilient Control Algorithms
RESILIENT INDUSTRIAL CONTROL SYSTEM (RICS)

A Control System designed and operated so that

- Incidence of undesirable incidents can be minimized
- Most of the undesirable incidents can be mitigated
- Adverse impacts of undesirable incidents can be minimized
- It can recover normal operation in a short time
3 – Layer System Model

Production Line or Engineering System - S

- Monitoring
- Operating
- Human

Operators

- Sensors
- Signals
- Measurements

HMI

- Controls
- Executions

ICS

- Automation

Actuators

Physical or Chemical Process
Resilience curve illustrating the Characteristics of Resilient ICS
ESTIMATING RESILIENCE OF AN ICS

ESTIMATION METRICS (Incident $i$)

- No performance degradation
- System reaches performance bottom
- System identifies incident $i$
- System recovers normal operation

Compute

- Protection time: $T_i^p = t_i^d - t_i^0$
- Degrading time: $T_i^d = t_i^m - t_i^0$
- Identification time: $T_i^i = t_i^l - t_i^0$
- Recovery time: $T_i^r = t_i^l - t_i^0$
- Performance degradation
- Performance loss
- Total Financial loss
- Potential Critical loss
Fault tolerant Control System using Sensor Fusion
The Two-Level Linear State Estimator
Cybervulnerability and Mitigation studies using a SCADA Test Bed
SCADA Test Bed Architecture
ON – LINE CONTROLLER DESIGN / RECONFIGURATION FOR NEW SITUATION
Operating Regime Learning and Switching of Controllers to cover wide spectrum of Plant Operation
CO-OPERATION

TYPE-1 : MULTIPLE MODEL SWITCHING CONTROLLERS

CONTROLLER BANK → PROCESS → MODEL BANK

SWITCHING STRATEGY

CALCULATE PERFORMANCE INDEX
TYPE - 2: MULTIPLE MODEL LEARNING ADAPTIVE CONTROLLERS

Identification and Decision Supervisor

Online Controller Design

Bank of Controllers

New Model

New Controller

PLANT

U1

U2

Un

New Model

Y
Diagram of the Resilient Controller
Application 1: Layout of Plant No. 4, Tuticorin Thermal Power Station
Architecture of overall Automation System in Unit 4, TTPS

Field I/O Signals

Field I/O Signals

Field I/O Signals

Control Signals

ABB PROCONTROL P 13/42

HITACHI HIDIC V 90/20

SECURED CDAC AUTOMATION SYSTEM

OPC

Signals

* Steam Temp Control
* Furnace Safety System
* Soot Blower
* Turbine Control

* Drum
* ID,FD Fans
* PA Fans
* BFPs
* Mill Control

* SH Control
* RH Control
* Modelling & Simulation
* Prediction Control
* Soft Sensor for Coal Flow
* Expert System
* Cooling Water Pump Monitoring
SYSTEM ARCHITECTURE - TTPS

- Superheater Prediction Control System Implementation
- Reheater Control System Expert System
- Six Coal flow Soft Sensors Implementation
- Motor Bearing, Winding Temp & Discharge Pressure
- Cooling water
- Pump House II (4 pumps)
Secured Automation System for TTPS Boiler

- Server
- Operator Console 1
- Operator Console 2
- PULV. COAL FLOW SOFT SENSOR
- Real Time Modelling, Simulation and Prediction System
- Expert System for Operator Guidance
- Superheater (Left)
- Superheater (Right)
- Superheater Prediction Control System Implementation
- iCon#1
- FIELD I/Os
- Reheater (Left)
- Reheater (Right)
- Reheater Control System
- iCon#2
- iCon#3
- Coal Mill A - F
- Six Coal flow Soft Sensors Implementation
- Motor Bearing, Winding Temp & Discharge Pressure
- Cooling Water Pump House II (4 pumps)
- Wireless IDS
- Backbone Router/Base station
- Security Gateway 1
- Wireless Network Manager
- Security Gateway 2
- Intrusion Detection Analysis System
KALMAN FILTER STATE ESTIMATION
AND
SECURITY SYSTEM IMPLEMENTATION
IN
THERMAL POWER STATIONS
SCHEMATIC DIAGRAM OF STEAM, WATER AND FLUE GAS FLOW LINES OF A DRUM TYPE BOILER

TEMPERATURE CONTROL

PRESSURE CONTROL

COMMON
CONVENTIONAL SUPERHEATER STEAM TEMPERATURE CONTROL SYSTEM
CONTROL PROBLEMS OF SECONDARY SUPERHEATER

The secondary superheater exhibits a large process lag ($\tau_p$) of the order of 8 to 10 minutes.

Process lag changes heavily according to factors such as Main steam flow, CV of coal etc.,
CONCEPT OF STEAM TEMPERATURE PREDICTIVE CONTROL SYSTEM
BY M/s HITACHI

\[ \theta(t + \tau_p) = \text{PREDICTED ESTIMATE FOR } \tau_p \text{ SECS INTO FUTURE, KNOWING THE ESTIMATE AT TIME } 't' \]
PROPOSED METHOD OF STEAM TEMPERATURE CONTROL

MAIN STEAM TEMPERATURE SET POINT

PI

PREDICTED STEAM TEMP.

PI

PREDICTION FOR $\tau_p$ SECS (8 to 10 minutes)

ATTEMPERATOR DYNAMICS

SEC. SUPERHEATER DYNAMICS

STEAM TEMP.

FUEL / SPRAY FLOW

SET VALUE

TIME

1

2

$\tau_p$

TIME

1'

2'

PRESENT

PREDICTED VALUE

MAIN STEAM TEMP.

PREDICTION TIME $\tau_p$
ARCHITECTURE OF ADAPTIVE PREDICTIVE STEAM TEMPERATURE CONTROL SYSTEM
(Incorporates Control System Security)

Main steam temperature

Set Point
541°C

Conventional PID Control System

Fuel flow/spray flow

Boiler Plant

N - Step State prediction by Kalman Filter

\( \hat{X}_s(k + N/k) \)

Computation of controller parameters

State estimation by Kalman Filter

\( \hat{X}_s(k/k) \)

Adaptive Process Identification by Kalman filter

\( \hat{\phi}_s \), \( \hat{\Gamma}_s \)

Boiler Plant model

\( X_s(k+1) = \phi_s X_s(k) + \Gamma_s U(k) \)
INTEGRATED MODEL FOR BOILER

Furnace Inputs

FURNACE MODEL

\[ \dot{X} = f(X,U) \]

\[ X = \begin{bmatrix} h_{eg} \\ \rho_{eg} \end{bmatrix} \]

DRUM MODEL

\[ \dot{X}_d = f(X_d,U_d) \]

\[ X_d = \begin{bmatrix} \rho_d \\ V_{dw} \end{bmatrix} \]

Furnace Exhaust Gas

PRIMARY SUPERHEATER MODEL

\[ X_p = A_p X_p + B_p U_p \]

\[ X_p = \begin{bmatrix} T_s \\ T_{mp} \end{bmatrix} \]

SECONDARY SUPERHEATER MODEL

\[ \dot{X}_s = A_s X_s + B_s U_s \]

\[ X_s = \begin{bmatrix} T_s \\ T_m \end{bmatrix} \]

ATTEMPERATOR MODEL

\[ \rho_d \]

\[ V_{dw} \]

\[ T_{sp} \]

\[ T_{gp} \]

\[ T_{si} \]

\[ T_{s} \]

\[ F_{spa} \]

\[ h_{spa} \]

\[ p_s \]

\[ F_d \]

Main Steam

Saturated Drum Steam

Furnace

Exhaust

Gas

Saturated

Drum

Steam

Exhaust Gas

Furnace Gas model

\[ X = f(X,U) \]

\[ X = \begin{bmatrix} F_d \\ T_{mp} \end{bmatrix} \]
The SSH is considered as a Stochastic Process

**STOCHASTIC PROCESS MODEL**

\[ X_s(k) = \phi_s X_s(k-1) + \Gamma_s U_s(k-1) + \Omega W(k-1) \quad \text{with} \quad X(0) = X_0 \]

\[ \Omega \] is a 2x2 coefficient matrix

**OBSERVATION MODEL**

\[ Y_s(k) = CX_s(k) + V(k) \]

**W(k) - Process Noise**

2x1

**V(k) - Measurement Noise**

2x1

White noise sequences
Stationary, Zero mean, Gaussian
It is assumed that very little is known about the process initially
\[ \hat{X}_s(0/-1) = 0 \quad \text{and} \quad P(0 /-1) = \infty \]

**KALMAN FILTER ALGORITHM**

(i) **Error variance algorithm**
\[ P(k/k) = \left[ P^{-1}(k/k –1) + C^T R^{-1} C \right]^{-1} \]

(ii) **Gain algorithm**
\[ K(k) = P(k/k) C^T R^{-1} \]

(iii) **Estimation algorithm**
\[ \hat{X}_s(k/k) = \hat{X}_s(k/k–1) + K(k) [Y_s(k) – CX_s(k/k –1)] \]

(iv) **Prediction (Extrapolation) algorithm**
\[ \hat{X}_s(k/k–1) = \phi_s \hat{X}_s(k–1/ k–1) + \Gamma_s U_s(k–1) \]
\[ P(k/k–1) = \phi_s P(k – 1/ k –1)\phi_s^T + \Omega Q \Omega^T \]
COMPUTATIONAL SEQUENCE OF N - STEP PREDICTION BY KALMAN FILTER

Enter loop with $\hat{X}_s(k/k-1)$ and $P(k/k-1)$

1. Compute error variance $P(k/k)$
2. Compute Kalman gain $K(k)$
3. Project one step ahead $\hat{X}_s(k+1/k)$ and $P(k+1/k)$
4. Compute filtered estimate $\hat{X}_s(k/k)$

For $i = k, k+1, k+2, \ldots, k+N-1$

- $\hat{X}_s(i+1/k) = \phi_s \hat{X}_s(i/k) + \Gamma_s U_s(k)$
- $P(i+1/k) = \phi_s P(i/k) \phi_s^T + \Omega Q \Omega^T$

$\hat{X}_s(k+N/k)$ and $P(k+N/k)$
ADAPTIVE PROCESS IDENTIFICATION

Using Extended Kalman Filter

System Model
\[
\begin{align*}
X_{K+1} &= A_K(\theta)X_K + \Gamma_K(\theta)\xi_K \\
V_K &= C_K(\theta)X_K + \eta_K
\end{align*}
\]

Parameter Model
\[
\theta_{K+1} = \theta_K + \xi_K
\]

Augmented System Model
\[
\begin{align*}
\begin{bmatrix}
X_{K+1} \\
\theta_{K+1}
\end{bmatrix} &= 
\begin{bmatrix}
A_K(\theta_K)X_K \\
\theta_K
\end{bmatrix} + 
\begin{bmatrix}
\Gamma_K(\theta_K)\xi_K \\
\xi_K
\end{bmatrix} \\
V_K &= 
\begin{bmatrix}
C_K(\theta_K) & 0
\end{bmatrix}
\begin{bmatrix}
X_K \\
\theta_K
\end{bmatrix} + \eta_K
\end{align*}
\]

\(\theta\) - Parameter Vector
Architecture of a SCADA-specific Security Solution (Xware)

Xware AB - Sweden
Trust Counter- Data Fusion assurance for the Kalman Filter in Uncertain Networks
An Example of Centralized Data Fusion for Networked Control Systems
The Architecture for Fusion Assurance
Tracking without Trust Rating
Tracking with Trust Rating
Block Diagram of Robust Outlier Detection and Resilient Estimation

Contaminated Measurements

Robustified Kalman Filter

Robust Outlier detection

\[ \hat{y} \]

\[ \tilde{y} \]

\[ e \]
Detection of Multiple Outliers

Detection of 3 Outliers
Detection of Multiple Outliers
Optimization of Drinking Water Production, Distribution and Consumption – Grand Challenges and Technology Driven Solutions for the Modern World
Conventional Chemical Addition Control (pH and Turbidity)
Clarifier lag Compensation and Optimal Process Control

Heuristic knowledge

Alum Tank 1
Alum Tank 2

Variable Speed Drive

Lime Tank 1
Lime Tank 2

Model Driven Estimator/Predictor

Heuristic knowledge

Setpoint

PID

Alum Delivery Pipe

Turbidity Sensor

Flow Transmitter

Raw water channel

Clarified water to filter bed
GRAND CHALLENGES IN OPTIMIZATION

- Quality
- Quantity
- Cost
- Safety

- Automation
- Leakage detection
- Pressure gradient monitoring
- Theft detection
- Smart metering
- Supply – demand balancing
- Evaluating problems in coming minutes
- Scenario evaluation

Overcome Threats

- Quality degradation vis-a-vis low pressure
- Cyberattack
- Climate change
Cyberattack on Drinking Water Supply System

Maroochy Shire Sewage Spill (2000)

Using a radio transmitter, the control system for sewage pumping station (Queensland, Australia) was interrupted on 46 occasions causing malfunctions resulting in the release of about 2,64,000 gallons of raw sewage into nearby rivers and parks.

Consequently, the drinking water supply system got affected badly.

It was polluted by sewage water.

Cost impact
Estimated $1 million loss.
The Maroochy Sewage Spill

- On April 23, 2000 Vitek was arrested with stolen radio equipment, controller programming software on a laptop and a fully operational controller.
- Vitek is now in jail...
Combine Hydraulic Modeling and SCADA into one Software Application

- **Optimization Methodology**
  - on-line
  - off-line

- **Collocation**
- **Multiple-Shooting**

**SCADA Security**
Simultaneous System Simulation & Optimization

- Analyse events as they happen
- Perform First Simulation with operational decision
- Monitor accuracy
- Change decision and quickly perform Second Simulation
- Compare level of improvement
- Select Ready-to-go campaign
- Implement control decisions

- Problems that remain
- Costs of the change
Secured Automation System

- SERVER
- OPERATOR CONSOLE 1
- OPERATOR CONSOLE 2
- LEAKAGE DETECTION SYSTEM
- CHEMICAL ADDITION OPTIMIZATION SYSTEM
- SIMULATION-DRIVEN OPTIMIZATION SYSTEM
- Security Gateway 1
- Security Gateway 2
- Wireless Security Manager
- Wireless Network Manager
- Intrusion Detection Analysis System
- Backbone Router/Base station
- Wireless IDS

Inputs/control commands
FIELD I/Os

- iCon#1
- iCon#2
- iCon#3
Thank You
Availabilty of solar energy: storage and hybridization

Time of Day

MW

Fossil Backup
Solor Direct
From Storage
To Storage
Firm Capacity Line

0 2 4 6 8 10 12 14 16 18 20 22 24
Solar Thermal Power Stations Announced in the USA

<table>
<thead>
<tr>
<th>MW</th>
<th>Name</th>
<th>State</th>
<th>Location</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>850</td>
<td>SES Solar One</td>
<td>California</td>
<td>San Bernardino County</td>
<td>stirling engine</td>
</tr>
<tr>
<td>750</td>
<td>SES Solar Two</td>
<td>California</td>
<td>San Bernardino County</td>
<td>stirling engine</td>
</tr>
<tr>
<td>553</td>
<td>Mojave Solar Park</td>
<td>California</td>
<td>San Bernardino County</td>
<td>parabolic trough</td>
</tr>
<tr>
<td>500</td>
<td>Fort Irwin</td>
<td>California</td>
<td>San Bernardino County</td>
<td>unnamed solar thermal technology, military</td>
</tr>
<tr>
<td>340</td>
<td>Hualapai Valley Solar Project</td>
<td>Arizona</td>
<td>Mohave County</td>
<td>parabolic trough</td>
</tr>
<tr>
<td>300</td>
<td>Unnamed</td>
<td>Florida</td>
<td></td>
<td>fresnel reflector</td>
</tr>
<tr>
<td>290</td>
<td>Starwood Solar I</td>
<td>Arizona</td>
<td>Harquahala Valley, Maricopa County</td>
<td>parabolic trough</td>
</tr>
<tr>
<td>280</td>
<td>Solana Generating Station</td>
<td>Arizona</td>
<td>West of Gila Bend, AZ</td>
<td>parabolic trough</td>
</tr>
<tr>
<td>250</td>
<td>Beacon Solar Energy Project</td>
<td>California</td>
<td>Kern County</td>
<td>parabolic trough</td>
</tr>
<tr>
<td>250</td>
<td>Harper Lake Solar</td>
<td>California</td>
<td>San Bernardino County</td>
<td>solar trough</td>
</tr>
<tr>
<td>250</td>
<td>Amargosa Solar Power Project</td>
<td>Nevada</td>
<td>Amargosa Desert, Nye County</td>
<td>parabolic trough</td>
</tr>
</tbody>
</table>
Errors minimized over a finite horizon

Constraints taken into account

Only the first control move is applied

Model of process used for predicting

MPC
Only the first control move is applied again
Representative efforts in the area of best practices for control systems security

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Title and URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>DHS</td>
<td>Industrial Control Systems Joint Working Group (ICS JWG); Cross Sector Cyber Security Working Group (CSCSWG); IT Sector Coordinating Council (IT SCC); Communications Sector Coordinating Council (CommSCC)</td>
</tr>
<tr>
<td>Organization with enforced standards</td>
<td>NERC</td>
<td>Cyber Attack Task Force (CATF) and several related task forces; Security guidelines: NERC 1300, CIP-002-1 through CIP-009-1; <a href="http://www.nerc.com/docs/standards/sar/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf">http://www.nerc.com/docs/standards/sar/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf</a></td>
</tr>
<tr>
<td>Publication</td>
<td>National Institute of Standards and Technology (NIST) SP800-53R3</td>
<td>NIST Special Publication 800-53, Revision 3; <a href="http://csrc.nist.gov/publications/PubsSPs.html">http://csrc.nist.gov/publications/PubsSPs.html</a></td>
</tr>
<tr>
<td>Working Group</td>
<td>NIST Smart Grid Interoperability Panel (SGIP)</td>
<td>NIST Smart Grid Interoperability Panel, the Cyber Security Working Group (CSWG); <a href="http://www.nist.gov/smartgrid/">http://www.nist.gov/smartgrid/</a></td>
</tr>
</tbody>
</table>
Representative efforts in the area of best practices for control systems security (Contd.)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards/Working Group</td>
<td>International Electrotechnical Commission (IEC) Technical Committee 57 Working Group 15</td>
<td>Data and Communications Security; focused on security for protocols 60870-5, 60870-6, 61850, 61970, and 61968</td>
</tr>
<tr>
<td>Standards</td>
<td>API 1164</td>
<td>Pipeline SCADA Security <a href="http://engineers.ihs.com/document/abstract/6BZBCBAAAAAAAAC">http://engineers.ihs.com/document/abstract/6BZBCBAAAAAAAAC</a></td>
</tr>
<tr>
<td>Standards</td>
<td>FIPS 140-2</td>
<td>Security Requirements for Cryptographic Modules</td>
</tr>
<tr>
<td>Standards</td>
<td>IEC 62210</td>
<td>Power System Control and Associated Communications—Data and Communication Security <a href="http://webstore.iec.ch/preview/info_iec62210%7Bed1.0%7Den.pdf">http://webstore.iec.ch/preview/info_iec62210%7Bed1.0%7Den.pdf</a></td>
</tr>
<tr>
<td>Standards</td>
<td>IEC 62351</td>
<td>Power Systems Management and Associated Information Exchange—Data and Communications Security, Part 1 (there are seven parts, all of which can be found on the IEC Web site): <a href="http://webstore.iec.ch/preview/info_iec62351-1%7Bed1.0%7Den.pdf">http://webstore.iec.ch/preview/info_iec62351-1%7Bed1.0%7Den.pdf</a></td>
</tr>
<tr>
<td>Academic Research</td>
<td>Trustworthy Cyber Infrastructure for the Power Grid</td>
<td>Trustworthy Cyber Infrastructure for the Power Grid <a href="http://tcipg.org/">http://tcipg.org/</a></td>
</tr>
</tbody>
</table>
International Scenario

- Idaho National Laboratories, National SCADA Test Bed Programme
- The Centre for SCADA Security, Sandia National laboratories
- US Department of Energy, National SCADA Test bed programme
- NERC (North American Electric Reliability Corporation) reliability standards for CIP
- VIKING (Vital Infrastructure, Networks, Information and Control Systems Management) – a research project funded by EU to create tools for risk analysis, develop a requirement baseline and test mitigations against threats
Security Aware Gateway

Proposed developments

SCADA Aware Firewall
  - Rule-based filtering
  - Stateful Packet Inspection (SPI)
  - Threshold – based filtering
  - Secure firewall configuration interface

Network Intrusion Detection/Prevention System (NIDS/NIPS)
  - Signature based
  - Anomaly based

Protocols Supported
  - Modbus TCP
  - DNP 3.0
  - ICCP
  - IEC 60870-5-104
  - DACS
Features of SCADA Aware Firewall

- **Rules based filtering**: Series of rules are defined based on: allowable source and destination IP addresses, listening port numbers of respective protocols and the protocol header.

- **Stateful packet Inspection**: Tracks the interrelationship between the packets allowed, by keeping a history of accepted packets and the state of current connection, only anticipated traffic is accepted.

- **Threshold based filtering**: Threshold-based filtering works by keeping statistics on the packets received and monitoring for threshold crossings based on configured time intervals and threshold levels. A database to maintain packet counts and a monitoring module to detect and enforce threshold crossings.
Features of NIDS

- **Signature based**: Attack scenarios exploiting the vulnerabilities in Modbus, DNP 3.0, ICCP, IEC 60870-5-104 and DACS is transformed into corresponding signature rules in the onboard NIDS.

- **Anomaly based**: Detects zero-day attacks based on statistical samples of network or host operating information (like CPU utilization rate, number of failed login attempts etc) and its deviation from the norm.

- Provision to manually import persistent alerts from Anomaly based IDS mode as a signature rule in the Signature based IDS mode, after an expert verifies it and validates it as a possible attack scenario.
To address SCADA vulnerabilities it is proposed to enrich the RTU developed by C-DAC with the following security enhancements:

- Role Based Access Control
- Security enhanced SCADA protocol
- Kernel OS hardening
- Data Authentication
Role Based Access Control

- Role-based Access Control (RBAC) is a method of regulating access to RTU resources based on the roles of individual users within an organization.
- Access control provides improved security by allowing users access to only certain permissions.
SCADA Forensics- System Architecture & Tools

- SCADA Computer Systems
  - Control Layer Nodes
    - Field devices
    - Intelligent electronic devices
  - RTU
  - PLC

- Forensics Data Acquisition Tool Suite
  - Computer Disk/Memory/Log Acquisition Tool
  - RTU/PLC Non-volatile Memory Acquisition Tool
  - Intelligent Field device Non-volatile memory Acquisition Tool
  - SCADA Forensics Analysis Tool
  - Forensics Image