SMART Security

Strengthening Information Protection in your ICS

Charles Liang

CISSP-ISSMP, CSSLP, CISM, CISA, CGEIT, CRISC, CEH
IT Security Policy Manager
CLP Power Hong Kong Limited
Disclaimer

The context is delivered as sharing from the perspective of information security practitioner.

In case there are individuals, organization names and/or technology brand names mentioned during the talk, this does not represent CLP endorse, nor recommend, nor criticize.
Today’s outline

1. About

2. Alignment

3. Project stage

4. O&M stage

5. Challenge

6. Key take away
1. About CLP – assets at a glance

When CLP turned on its first generator in Hong Kong a century ago, the territory’s total electricity demand was just one tenth of a megawatt.

As of 31 December 2012, we have invested in 13,556 equity MW of electricity generation and 8,999 MW of capacity purchase across the Asia–Pacific region. We have over 70 power generation assets using a wide range of fuels from renewable sources, coal and gas through to nuclear.

Learn more about our assets that are under development or are commissioned by exploring the regional map.

Source: www.clpgroup.com
1. About CLP

- **CLP Holdings Limited** – listed on the Hong Kong Stock Exchange and one of the largest investor-owned power businesses in Asia. Outside Hong Kong, **CLP Holdings Limited** holds investment in the energy sector in Australia, Chinese Mainland, India and Southeast Asia. It has diversified portfolio of generating assets with wide range of fuels including coal, gas, nuclear and renewable sources.

- **CLP Power Hong Kong Limited**, wholly owned by **CLP Holdings Limited**, operates a vertically integrated electricity supply business in Hong Kong, and provides a highly reliable supply of electricity and excellent customer services to 5.8 million people in its supply area.

  - Generation capacity of 6,908 MW (as at 31 Dec 2012)
  - Network includes around 14,200 km of overhead, underground and submarine cables
  - More than 13,750 substations
  - Achieve supply reliability of 99.999%

Source: www.clpgroup.com
1. About me

- 10+ years IT background
- Another 10+ years Infosec practitioner
- Look after Infosec for CLP (at Group level) in both IT and OT
  - Establish and recommend management directives (written policies)
  - Facilitate enforcement of directives
  - Provide cyber risk advisories for IT/OT project and business process
  - Collaborate security assessment, incident respond
  - Collect intelligence
  - Bring up situation awareness
- Pace of cyber world changes rapidly
  - Have to keep on learning everyday to enhance domain knowledge
  - Attended various ICS events: Red Tiger Security training, DHS/ICS-CERT: 201 & 301 (Red Team/Blue Team) courses, ICSJWG, ICS Cyber Security Conference
Today’s outline

1. About

2. Alignment

3. Project stage

4. O&M stage

5. Challenge

6. Key take away
2. Alignment – definition

- ICS definition (http://ics.sans.org)

*Industrial Control Systems (ICS), which include Process Control, Distributed Control, PLC-based, and SCADA systems, are instrumental in the production of goods and provision of essential services. ICS is the label for the digital technology that collects, monitors, analyzes, decides, controls, and acts to safely produce and move physical things.*
2. Alignment – examples

... and many more involving ICS, they are all around us.
2. Alignment – modernization
2. Alignment

- Competitive market
- Fully integrated automation for
  - Business intelligence
  - Process optimization
  - Cost reduction
- Remote access to get information or status, decision support
- Behind the scene, lots of information are flowing thru different components across the network
- Commodity hardware / software are used for system, application & network to build the ICS
- Therefore, ICS is exposed to same cyber threats in ICT
2. Alignment

- If the system and network are insecure, the information regarding A-I-C will be affected.
- The ICS will then operate incorrectly.
- Depending the target purpose of the ICS, the outcome could affect the community in different degrees:
  - Blackout
  - Uncontrolled waste or toxic materials spill
  - Unsafe machinery operation ... etc.

- So, protecting the info is vital to secure the ICS operation:
  - How much cyber security is enough?
  - How to decide the optimal protection?
  - The vendor has claimed the ICS components are secure, but what about how these components are deployed?
  - Where do we start with?
2. Alignment

High level ICS life cycle

- Project definition
  - Engineering design, system build, commissioning
- Asset management
- De-commissioning

Project stage

O&M stage

Reference in this talk

Setting expectation – this talk isn’t technical deep-dive, focus is more on people and process aspects, and energy utility based.
Today’s outline

1. About
2. Alignment
3. Project stage
4. O&M stage
5. Challenge
6. Key take away
3. Project stage – understand interconnectivity

Understand how your ICS connects with other neighbours
3. Project stage – understand risk

An insecure component in the infrastructure could harm not just itself but also other connected components.
3. Project stage – cyber inter-dependency

Factors/Forces contributing to Energy Crisis in California
- Deregulation Policies
- New Energy Marketplace Dynamics
- Tight, High-Cost Gas Supplies
- Utility Financial Crisis
- Substantial Load Growth
- Lack of New Generating and Transmission Capacity
- Aging Fleet of Power Plants
- Low Hydro Conditions
- Transmission/Environmental Constraints

Electric Power
Supply/Demand Imbalance

First-Order Effects
- Gas Supply
- Curtained Natural Gas Production

Second-Order Effects
- Cogeneration
- Reduced Steam Injection for Heavy Oil Production

Third-Order Effects
- Oil Production
- Reduced Heavy Oil Production

Oil Pipelines
Disruption of Product Pipelines

- Refineries
- Inventory Buildup; Curtained Operations

- Road Transportation
- Shortages of Specially Formulated Gasoline

- Air Transportation
- Disruption of Flight Schedules

- Storage Terminals
- Inventory Drawdown; Shortages of Gasoline and Jet Fuel

- Agriculture
- Crop Losses

- Banking and Finance
- Financial Losses

Water
Disruption of Irrigation Pumps

Fig-5: http://www.inl.gov/technicalpublications/Documents/3489532.pdf

American Blackout Documentary 2013, NatGeo
3. Project stage – assess risks holistically

- Assess risks beyond own ICS
- Think also about impacts then mitigation regarding:
  - Human safety
  - Own infrastructure
  - Inter-connected systems (grid, partners)
  - Community (blackout)
  - Environment (waste spill) … etc.
3. Project stage – design ICS & infrastructure

- Edge perimeter
- Incoming, outgoing and transit
- Zone separation & control
- “Packet” inspection
- Supporting facilities
3. Project stage – conceptual model

PNNL: Cyber Security Plans: Potential Impacts for Meteorology Programs
3. Project stage – typical model

Fig-10 Complete defence-in-depth strategy
[Link to detailed strategy document](https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf)
3. Project stage – identify info & flow across nodes

Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security
Figure 2-3 Logical Reference Model
3. Project stage – secure different info states

At-rest

In-motion (flow)

In-use
3. Project stage – don’t be blind, need status
3. Project stage – decide IR / BCP

Detect the expected, handle the unexpected
3. Project stage

- Other than technology, we must not forget to incorporate these in the design for subsequent O&M
  - Alarm & event management
  - Incident response (IR)
  - Business continuity planning (BCP)
  - ICT sustainability arrangement
  - Be part of the commissioning process to validate cyber security controls

**Apply engineering, business risk management, ICT practices and IT security principles into the ICS design**
Today’s outline

1. About

2. Alignment

3. Project stage

4. O&M stage

5. Challenge

6. Key take away
4. O&M stage

The ICS is secured per design and validated during commissioning, is this full stop and relaxed?
4. O&M stage – address new vulnerabilities

ICS sustainability is required
4. O&M stage – upkeep protection

Again, ICS sustainability is required
4. O&M stage – execute secure disposal

Digital Bond, Inc
http://www.digitalbond.com/blog/2012/03/12/proper-equipment-disposal/
4. O&M stage – maintain situation awareness

- Keep aware of new threats and assess impact to own organization, e.g. DNP3 vulnerabilities, speculated attacks to specific industry

- Avoid similar incident from lesson learned\(^1\)
  - Failure of EMS while performing DB update
    - While performing DB restore, the standby communications server in the Primary Control Center was manually restarted, causing reversal of the DB edits to fail and created faulty data files that synchronized across the integrated system servers.
  - SCADA failure resulting in reduced monitoring functionality
    - A utility’s primary control center SCADA servers became unresponsive, resulted in a partial loss of monitoring and control functions for more than 30 minutes.
  - Loss of EMS – IT communications disabled
    - Transmission system operators lost the ability to authenticate to the EMS system, resulting in a loss of monitoring and control functionality for more than 30 minutes because a specific firewall policy allowing authentication failover from the local authentication server to the remote authentication server was inadvertently deleted.

4. O&M stage

- **Situation awareness**
  - Lesson learned from own or public incidents to avoid similar
  - Keep aware of new vulnerabilities and address them

- **Validate control (periodic)**
  - BCP or IR readiness
  - Revisit if control remains effective

- **Manage change**
  - ICT sustainability
  - New standards, new regulations, new business function, new interface, new system integration, ... etc.

- **Secure de-commissioning**
  - Disposal of replaced components
  - Removal of control
Today’s outline

1. About
2. Alignment
3. Project stage
4. O&M stage
5. Challenge
6. Key take away
5. Challenge – remote monitoring or even access

- **Legitimate business needs are always there**
  - Fulfill ICS performance per contract
  - Remote status monitoring by vendor
  - Remote support, diagnosis, tuning for fast throughput and cost-effectiveness (without fly-to-site)

- **Enable rather than prohibit**
  - Understand how it works and what are involved
  - Assess risk
  - Define allowable use cases with vendor
  - Deploy technology (one-way traffic flow, strong authentication etc.)
  - Establish process & awareness to complement technology
  - Consult with SME if required
  - Register external connection for periodic review
5. Challenge – sustainability

- ICT lifecycle is shorter than machinery
- Business decision among resource, asset book value, risk, compliance for retrofit or refresh
- Change management is the key in this process
5. Challenge – in the Cloud

- Complex model: hosting, facilities, multi-tenancy
- Understand security protection and resolve gap
- Which party’s responsibility if things go wrong
- Business decision and commercial arrangement
If control is deployed incorrectly, then protection won’t be effective; have 3rd party assessment.
5. Challenge – improper understanding / usage

This plug-and-play innovation bypasses all network zoning segregation, gateway level content inspection & perimeter control with just least privilege.

Technical control and awareness are essential.
5. Challenge – improper understanding / usage

Fictional Cyber Attack, SANS Institute
http://www.securingthehuman.org/cyberattackdemo
5. Challenge – improper understanding / usage

HOW AM I EVER GOING TO PROTECT SCADA?!

IT REQUIRES YOU TO BE PATIENT AND WATCHFUL AT ALL TIMES.

IT REQUIRES A DEDICATION TO EDUCATION—AND DISCUSSIONS WITH OTHER SMART PEOPLE.

THERE IS NO EASY OR FAST ANSWER.

SCADA and Me, Robert M. Lee
ISBN-10: 149127512X
5. Challenge – so many domains to cater for

- **Customer service**
  - Incorporate appropriate usage terms for proper use of the services

- **Procurement**
  - Understand the work scope to establish the relevant contractual terms before contract award for the project or O&M services

- **Legal**
  - Understand the situation and advise effectiveness of contractual terms with vendor and usage terms with customers

- **Public Affairs**
  - Get prepared of Lines-To-Take to fast track the media in case there is significant cyber incident

- **ICS Project team**
  - Understand what to protect
  - Specify cyber security
  - Incorporate into contractual requirements
  - Validate before commissioning

- **ICS (asset) owner**
  - Make decision in IR/BCP

- **ICS operation team**
  - Use ICS properly per design

- **ICS support team**
  - Assess impact to manage change
  - Manage vendors, service providers
  - Upkeep effective cyber security protections
  - Get preparedness for IR/BCP

Engage stakeholders to support ICS cyber security
5. Challenge – so many domains to cater for

Transform stakeholders to secure ICS

ASK NOT WHAT YOUR COUNTRY CAN DO FOR YOU. ASK WHAT YOU CAN DO FOR YOUR COUNTRY.

J. F. KENNEDY
5. Challenge – insider threats (complex)

<table>
<thead>
<tr>
<th>Data</th>
<th>Observation</th>
<th>Indicator</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directly available information</td>
<td>Inference from data that reflects a specific state</td>
<td>Action/event as evidence of precursor to inferred behavior</td>
<td>Sequence of actions associated with a purpose</td>
</tr>
</tbody>
</table>

Incoming data processed to infer observations
Observations processed to infer indicators
Indicators assessed to gauge threat

Data
- Email traffic
- Inter/intranet traffic
- Remote access traffic
- Building access
- Social/org
- Calendar
- Time reporting

Observations
- Web sites
- File size
- Install scripts
- HR/personal information
- Location
- Authentication attempts

Indicators
- Disregard for policies
- Access attempts against privilege
- Harvesting proprietary data
- Suspicious communications
- Disgruntled employee

Behaviors
- Discover and associate actions that fit a malicious exploit profile

http://www.pnnl.gov/cogInformatics/media/PNNL-MBCbig.jpg

© 2013 CLP Power Hong Kong Limited. All rights reserved
5. Challenge – insider threats (simpler)

Set directive (admin control) with deterrent to enforce desired state
Today’s outline

1. About
2. Alignment
3. Project stage
4. O&M stage
5. Challenge
6. Key take away
6. Key take away

On top of engineering aspects to build the ICS ...

- Also need these practices
  - Business risk management – mitigate risks cost effectively
  - ICT discipline – change management
  - IT security principle – threat modelling

- Think cyber infrastructure from physical world, e.g.
  - Airport – zone separation
  - Road system – proper usage

- Enforcement
  - Training & awareness
  - Technical controls to avoid mistakes and protect at certain degrees
  - Administrative controls to enforce beyond technology
  - Backed by law and regulation as last resort
6. Key take away – SMART security

Secure ICS by design
Manage cyber security controls throughout ICS lifecycle
Assess ICS business risks in a holistic view
Resolve identified ICS cyber security issues promptly
Transform stakeholders to support ICS cyber security
<table>
<thead>
<tr>
<th>Slide</th>
<th>Source (last accessed Nov 2013)</th>
</tr>
</thead>
</table>
| 9     | http://commons.wikimedia.org/wiki/File:London_Underground_Escalator.jpg  
       | http://commons.wikimedia.org/wiki/File:Singapore_cable_car_exterior.jpg  
       | http://commons.wikimedia.org/wiki/File:Nodding_Donkey_-_geograph.org.uk_-_1398099.jpg  
       | http://commons.wikimedia.org/wiki/File:Dartford_station_platform_4_look_west2.JPG  
       | http://commons.wikimedia.org/wiki/File:Mass_Rapid_Transit_tracks_Singapore_-_20080501.jpg  
       | http://commons.wikimedia.org/wiki/File:Scene_at_car_wash_in_Summit_NJ.JPG  
       | http://commons.wikimedia.org/wiki/File:Container-terminal-ost-fmm004.jpg |
       | http://commons.wikimedia.org/wiki/File:Dashboard_(1).jpg  
       | http://commons.wikimedia.org/wiki/File:Rianarchive_341194_Kursk_Nuclear_Power_Plant.jpg  
       | http://commons.wikimedia.org/wiki/File:Estrack_control_centre.jpg |
| 11    | http://commons.wikimedia.org/wiki/File:TVRemote.jpg  
       | http://commons.wikimedia.org/wiki/File:Estrack_control_centre.jpg |
| 17    | Fig-5: INL/EXT-06-11464, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research  
       | P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann Aug 2006  
| 18    | http://en.wikipedia.org/wiki/File:PrestigeVolunteersInGaliciaCoast.jpg  
       | http://commons.wikimedia.org/wiki/File:Train Accident near Klina.jpg  
       | http://commons.wikimedia.org/wiki/File:ESD_Button.jpg |
| 20    | Cyber Security Plans: Potential Impacts for Meteorology Programs  

Illustrations without reference are either from Office Clip Art library or by the author’s collection.
<table>
<thead>
<tr>
<th>Slide</th>
<th>Source (last accessed Nov 2013)</th>
</tr>
</thead>
</table>
| 21    | Fig-10 Complete defense-in-depth strategy  
| 22    | Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security  
Figure 2-3 Logical Reference Model  
| 24    | http://commons.wikimedia.org/wiki/File:Zugansage_Bielefeld_Hbf.jpg |
| 28    | http://commons.wikimedia.org/wiki/File:Mt._Lavinia_Governor%27s_High_Tea.jpg |
| 31    | Digital Bond, Inc. – Proper Equipment Disposal  
http://www.digitalbond.com/blog/2012/03/12/proper-equipment-disposal/ |
| 32    | Joe Weiss – Unfettered Blog » Three blind mice  
| 35    | http://commons.wikimedia.org/wiki/File:TVRemote.jpg |
| 40    | SANS Institute – Fictional Cyber Attack  
http://www.securingthehuman.org/cyberattackdemo |
| 41    | SCADA and Me, Robert M. Lee  
ISBN-10: 149127512X  
| 43    | http://commons.wikimedia.org/wiki/File:Ask_not_what_your_country_can_do_for_you.jpg |
| 44    | http://www.pnnl.gov/cogInformatics/media/PNNL-MBCbig.jpg |

Illustrations without reference are either from Office Clip Art library or by the author’s collection.
Thanks

cliang@clp.com.hk

http://hk.linkedin.com/in/charlesliang/