Current Status of ICS in Developing Countries

Case Study of Argentina and LATAM
About Me

Who am I?
Pablo Martin Almada, IoT/IIoT Cybersecurity Director at KPMG.

Education
Systems Engineer - Universidad Tecnológica Nacional, Argentina.
Master, Information Security - Buenos Aires University, Argentina. (Thesis defense)
Postgraduate, Embedded Systems - Buenos Aires University, Argentina.
ISA/IEC 62443 Certified member

Role and Specialization
Director of the Cybersecurity Practice, specialized in Industrial Control Systems, Cyber-Architecture, Secure Software, among other subjects.
Agenda

Context

What are the Companies Doing in Argentina?

Common Issues by Industry

How does this story continue?

Local Cases

Conclusion
Why LATAM?
Its Relevance

Quick facts
Latin America is a group of countries and dependencies in the Western Hemisphere where Roman languages such as Spanish, Portuguese, and French are predominantly spoken, it is broader than the terms Ibero-America or Hispanic America.

Area: 20,111,457 km².
Population: 642,216,682
Gross Domestic Product: $10,586,642 billion

Natural Resources – In a Nutshell

- Lithium: 65%
- Silver: 49%
- Oil: 20%
- Gas: 7%
Quick facts

Argentina is a massive South American nation with terrain encompassing The Andes Mountains, glacial lakes and grasslands of the Pampas which are the traditional grazing ground of its famous beef producing cattle population. The country is famous for the dance and music of the Tango.

Area: 2,780,400 km².
Gross Domestic Product (2015) $971.967 billion
Shale Oil and Shale Gas

_Vaca Muerta_ is a geological formation of 30,000 km² located mainly in the province of Neuquén in the south of Argentina and containing oil and gas found at a depth of more than 2,500 meters, far from the groundwater that in this region is located at a depth of between 300 and 400 meters.

It is estimated that the total recoverable hydrocarbons from this formation will be _16.2 billion barrels of oil_ and _308 trillion cubic feet of natural gas_. 
What are the Companies Doing in Argentina?
Let’s begin by making a distinction between the Private and Public Sector.

Private Companies...

...are on a self-discovery stage. For this reason they are:

- Starting to break down IT and OT “working barriers” to join efforts for addressing a secure network integration.
- Performing Cybersecurity assessments.
- Establishing a roadmap to deploy Cybersecurity best practices.
- Performing OT-based Cybersecurity awareness campaigns.
What are the Companies Doing in Argentina?

Public Companies...

...are not paying attention to Cybersecurity concerns:

• Energy
• Nuclear Plants
• Dams
• Transportation
• Water and Wastewater
• Health
• Others...

Nowadays...

These companies do not have Cybersecurity areas exclusively focused on the OT sector.

These companies do not have OT-related Cybersecurity policies.
Common Issues by Industry LATAM
Based on the development of multiple assessments in LATAM, including countries, such as: Colombia, Mexico, Chile, Argentina, Ecuador and Costa Rica. We’ve gathered substantial information that allowed us to understand the current Industrial Cybersecurity Landscape in the region.

Common Issues by Industry

These countries are the main industrial centers of LATAM.

It is worth mentioning that all the companies involved in this study had never performed a cybersecurity assessment before.

Based on the work of more than 20 companies from the industrial sector.
Industrial Cybersecurity Standards

Companies are adapting their industrial cybersecurity posture based on the following standards:

- **Manufacturing Companies**: Steel Shop, Steel Manufacturing & Brewing Companies.
- **Oil & Gas Companies**:
  - **Upstream**: Early Productions Facilities (EPF), Central Processing Facilities (CPF), Natural-Gas Processing Plants, LNG Facilities, Ports.
  - **Midstream**: Gas pipelines and LNG carriers
  - **Downstream**: Gas Stations.
- Companies included in the Bulk Electric System (BES), covering:
  - **Generation Stations**: Thermal Power Station, Hydro Power Stations, Coal-fired Power Stations, Wind Turbine Farms.
  - **Distribution**: Sub-stations Step-Down.

Based on the work of more than 20 companies from the industrial sector.

**ISA 62443-2-1**
Level of Compliance: overview

Companies’ level of compliance is broken-down by the following graphs:

LATAM currently presents a low level of compliance with ICS Standards.

(*) Including Fully Compliant and Partially Compliant controls.
Level of Compliance: detailed statistics

To get a better understanding of the overview, here are detailed statistics to offer an additional insight:

<table>
<thead>
<tr>
<th>100%</th>
<th>Didn’t have an Industrial Cybersecurity Policy and their ICS Governance was in early stage.</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>Didn’t have a cybersecurity awareness program focused on ICS.</td>
</tr>
<tr>
<td>86,7%</td>
<td>Industrial networks assessed lacked proper segmentation with IT networks.</td>
</tr>
<tr>
<td>89,1%</td>
<td>Don’t have an Incident Response Plan to detect cybersecurity events and act accordingly.</td>
</tr>
<tr>
<td>70,3%</td>
<td>Don’t have a Business Continuity Plan to recover operations if they are impaired by a cybersecurity incident.</td>
</tr>
<tr>
<td>60,4%</td>
<td>Don’t have a Business Continuity Plan to recover their operations.</td>
</tr>
<tr>
<td>85,7%</td>
<td>Critical ICS systems aren’t hardened and have applications not necessary for operations that present vulnerabilities.</td>
</tr>
<tr>
<td>94,0%</td>
<td>Don’t have an Incident Response Plan.</td>
</tr>
<tr>
<td>82,5%</td>
<td>A Patch Management process isn’t in place and the patches are applied based on the operators expertise.</td>
</tr>
<tr>
<td>100%</td>
<td>Of the companies assessed didn’t have an Industrial Cybersecurity Policy.</td>
</tr>
</tbody>
</table>

(*) All the values listed are based on the first assessments of the companies involved. Currently, most of the companies assessed are working on their remediations plans.
Gas Processing & Distribution

Although gas processing and distribution companies have certain levels of development regarding Critical Infrastructure Cybersecurity, they have some incorrect concepts such as security by obscurity or not implementing basic security network concepts.

Common Findings

- Physical access to field equipment is not restricted
- Server hardening is not implemented
- There are no antivirus/antimalware systems
- Non-implementation of Cyber asset inventories
- Change Management and Program Development controls are not in place
The Oil & Gas industry is leading the path of building a strong cybersecurity posture without focusing solely in securing their operations, but working strongly on cyber-awareness programs and ICS trainings to solidify their operative personnel knowledge.

**Common Issues by Industry**

**Oil and Gas**

IT policies and procedures are not defined and documented

- Non-implementation of Cyber asset inventories
- Physical access to field equipment is not restricted
- Antivirus and Patch Management controls are not in place
- Server hardening is not standardized
- Change Management and Program Development controls are not in place
Common Issues by Industry

Power Generation
The Power Generation sector is composed by civilian serving critical infrastructures that could impact people’s everyday life if an outage occurred. Also, It holds a worryingly low Cybersecurity Maturity level.

Common Findings

Physical access to field equipment and computer rooms is not restricted

Obsolete and unsupported operating systems
Detected malware
Antivirus and Patch Management controls are not in place
There are no antivirus/antimalware systems
Interconnection between industrial and corporate networks without minimal Cybersecurity measures
Local users run with administrator permissions
Unsecured remote access tool
Manufacturing

The Manufacturing Sector could be considered the less developed in the region. In addition, their operative team is production-focused and take for granted that production lines interruptions are a common issue rather than considering the possible impact of a Cyber Attack.

Common Findings

- IT policies and procedures are not defined and documented
- Physical access to the Control and Computer rooms is not restricted
- Antivirus and Patch Management controls are not in place
- Server hardening is not standardized
- Logical access controls have not been implemented
- Most systems share the same user ID and password for all users
- Change Management and Program Development controls are executed by the software vendors at their discretion
How does this story continue?
So... What about the remediations?

The remediation projects developed by the companies are compiled in the following table:

<table>
<thead>
<tr>
<th>Status</th>
<th>Remediation Projects</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accomplished</td>
<td>ICS Cybersecurity Policy</td>
<td></td>
</tr>
<tr>
<td>Ongoing-Project</td>
<td>OT System Hardening</td>
<td></td>
</tr>
<tr>
<td>Planned</td>
<td>OT Assets Inventory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICS Cybersecurity Awareness</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Physical Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Segmentation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incident Response</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business Continuity Plan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OT Network Monitoring Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AV/Anti-Malware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Patch Management</td>
<td></td>
</tr>
</tbody>
</table>

Reference:
- Green: Accomplished
- Yellow: Ongoing-Project
- Red: Planned
Local Cases
Traffic Light System - Cyber Incident

**Event**
Different media sources have informed that the traffic lights system of the capital of its principal state has been compromised by anonymous hackers.

**Location**
City of La Plata

**Impact**
Anonymous hackers attacked the city traffic light control center affecting more than 400 devices. The lights were turned off during rush hours for a couple of weeks. Those irregularities could be seen in the city center and the periphery.
Power Outage - Cyber Incident

Event
One of the most important companies of energy distribution of Buenos Aires suffered a remote sabotage on its control system.

Location
Autonomous City of Buenos Aires

Impact
An attacker operated the SCADA network from an unknown location for evil purposes. As a result of the attack, blackouts occurred across the entire city. The attacker could not be identified.
Sabotage Incident

Event
A company of energy distribution of Buenos Aires suffered physical sabotage due to issues with Labor Unions.

Location
Buenos Aires

Impact
Transformers theft were reported. The attackers had high knowledge of remote networks because the attack did not affect the distribution of energy.
Do You Want to Hack the National Power Grid?
Do You Want to Hack the National Power Grid?

What would you think if I were to tell you that all the information necessary to prepare a cyber-attack against the Argentinian power grid is freely available on the Internet?

It's a lie.

It’s absolutely true
Do You Want to Hack the National Power Grid?

Cammesa is a joint venture between the national Government and private sector representatives...

And its website exposes the complete power grid...including his status!
Do You Want to Hack the National Power Grid?

... are exposed
Do You Want to Hack the National Power Grid?

...and there is more!
Do You Want to Hack the National Power Grid?

We know that many cyber assets are exposed to the Internet...

...and we know some of these assets are measuring instruments used to make automatically decisions on the control network...

So, we could manipulate some info in these cyber assets to make that the control system take decisions based on misinformation.

... could we overload the devices?

...could we interrupt the power supply?
Conclusion
Conclusion

**Critical Infrastructure Situation**
Argentinian industries as well as Latin American, present enormous deficiencies regarding Critical Infrastructure Cyber Security and its operations. The question isn’t IF the critical infrastructure is going to be attacked but WHEN.

**Cyber Incidents**
Companies do not have the obligation to report incidents. In addition, companies do not have the ability to detect if they were targets of cyber-attacks. That is why some incidents are public and many others remain hidden. Despite of the circumstances, we suspect that the attacks are increasing every day.
Questions?
Thanks!
palmada@kpmg.com.ar