USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

Cybersecurity Incident Response Plan Development

Incidence Response through Supply Chain Preparedness: The GRIDCo Case Study

Table of Contents

Introduction: The Power System

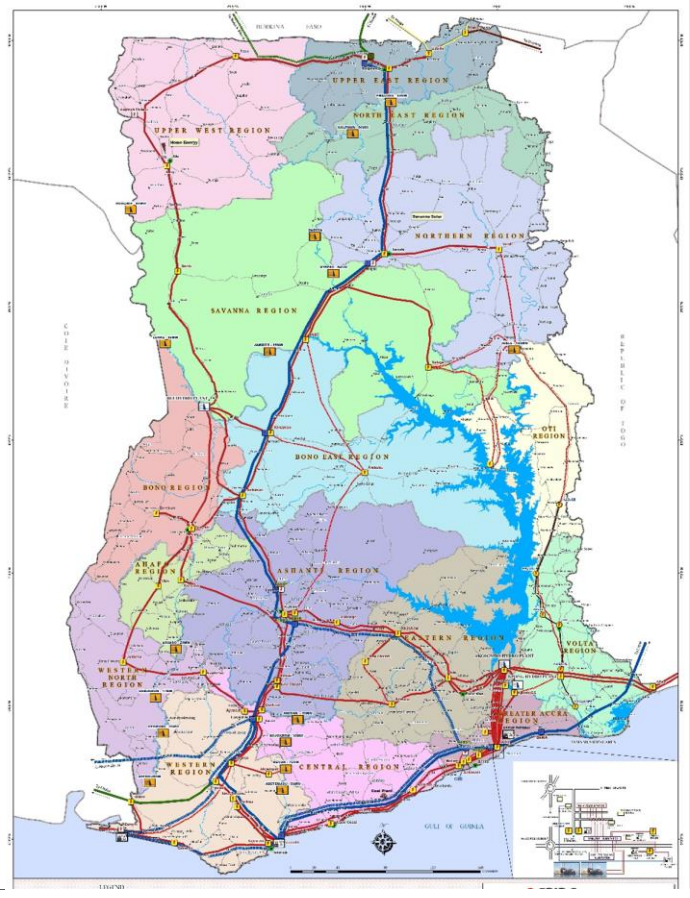
32 Bulk Customers

10 Generating Companies (incl. **IPPs**)

5,231 MW installed generation capacity (3 Hydro, 13 Thermal & 2 Solar Plants)

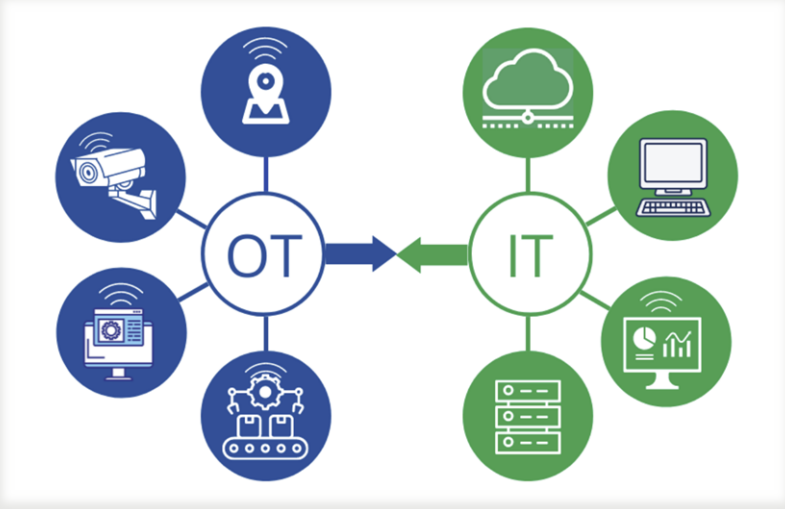
6,472.23 Circuit-km of transmission lines (69 kV, 161kV, 225kV & 330 kV) with about **70%** fiber-optically equipped

Peak Demand – 3,618 MW in December 2023



Introduction: Background Information

- GRIDCo Operates both IT and OT Infrastructure
- GRIDCo is Interconnected with Cote D'Ivoire, Burkina Faso, Togo, Benin
- Potential Impact of Outages
  - Financial Loss of Millions of USD daily
  - Negative impact on GDP as ~80% of National production depends on Electricity
  - Sub-regional security stability



Considerations for OT Security and Incident Management

[to establish basis for IRP]

- Threat actors can introduce compromised components into a system, unintentionally or by design, at any point in the system's lifecycle.
- Attackers set sights on Industrial control systems (ICS) and third parties
- Need to understand Supplier's maturity and security processes and products for connected products and services

Considerations for OT Security and Incident Management

[OT/ICS cannot be handled the same way as IT]

- OT Focus Area
  - Direct Control of Devices and processes
  - Reliability and Continuity of Operations
  - System response times are critical
- OT Devices
  - Customised OS devices running OEM apps, proprietary embedded devices, custom production systems
  - Refresh cycle sometimes over 20 years
  - Usually many legacy units

- IT Focus Area
  - Information Management and Security
  - Digital Technologies
  - Internet and Connectivity
- IT Devices
  - Commonly connected Windows servers, PCs, mobile devices running OS and Apps
  - Refresh cycle is 3-5 years

Considerations for OT Security and Incident Management

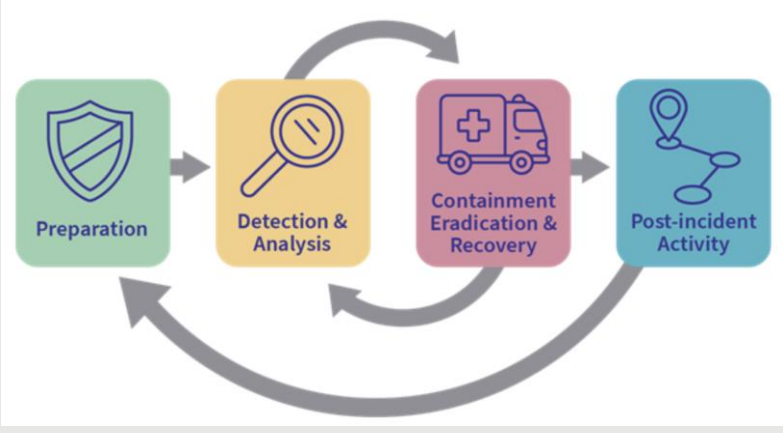
[OT/ICS cannot be handled the same way as IT]

- OT Threat Identification
  - Challenges in identifying domain-specific threats.
  - Higher exposure to zero-day vulnerabilities, especially in embedded devices
- OT Remediation
  - Complex threat remediation
  - High operational risk; incorrect actions can halt production for extended periods

- IT Threat Identification
  - Extensive public database for vulnerability identification
  - Lower zero-day vulnerability exposure
- IT Remediation
  - Simple and more available threat remediation with minimal impact
  - Lower operational risk

GRIDCo's OT Incident Management Plan (IMP) – Based on NIST Guide to OT Security (800-82 Rev. 3)

- GRIDCo has adopted and follows the NIST Guide to OT Security (800-82 Rev. 3) for incident management.
  - NIST 800-82r3 builds on the NIST Framework (Identify, Protect, Detect, Respond, Recover)
- It's IMP includes four main stages:
  - preparation and prevention;
  - detection and analysis;
  - containment, eradication, and recovery;
  - post-incident activity.



GRIDCo's OT Incident Management

Step 1: Preparation and Prevention.

Preparation is key to an effective response.

- Calculate business impacts
- Use existing risk analysis.
- Identify supporting systems/assets
- Triage the Assets [meet 80/48 KPI] – Know and Prioritise Systems that are critical – Control 80% of our operations
- 95% Certainty of the priority of these Assets

GRIDCo's OT Incident Management:

Calculate business impact, using existing risk analysis

Risk Assessment – critical part of our USAID-sponsored BIP Program.

- Engage Relevant Teams (Finance, Procurement, Engineering) to determine estimated value of potential operational losses and restoration costs.
- Assess all probabilities and apply them to calculate Business impact, raw impact, and raw Risk Rating
- Assess Treatment Cost (and status) and Calculate Target Risk and compare with current risk rating for decision making

GRIDCo's OT Incident Management

Step 2: Detection and analysis.

Take steps to put security safeguards in place.

- Ensure to deploy relevant systems
- Vendors must meet GRIDCo's criteria to qualify Vendor [where we are unsure, vendor makes written commitment]
- Implemented Security by Design – Cybersecurity Assessment done with Vendors and Factory Acceptance Testing (FAT) before implementation
- Site Acceptance Testing (SAT) not limited to only system functionality, but also CS compliance
- CS Awareness programs and simulations

GRIDCo's OT Incident Management

Step 3: Containment, eradication, and recovery.

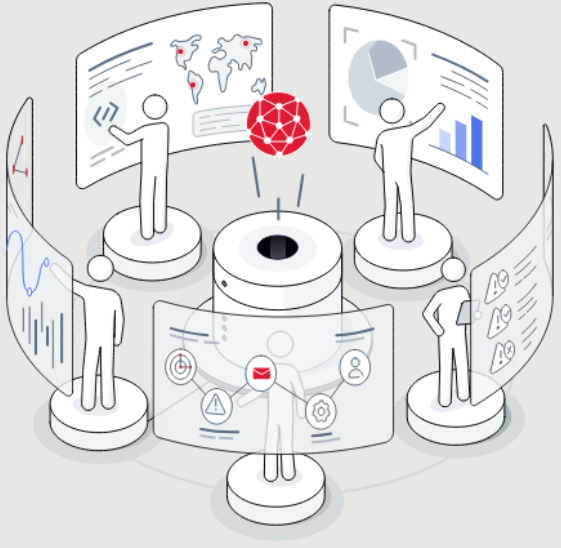
- Incident Response process is triggered immediately when an issue / suspected issue is picked up.
- Incident Reporting process is triggered with the least positive information obtained.
- Communicate to Management first. Then industry stakeholders must be informed on a need-to-know basis.

GRIDCo's OT Incident Management

Step 4: Post-incident Activity.

Test your plan.

- Documented Simulations driven by Business Continuity and Compliance teams
- Simulations in OT carried out. Results recorded and compared with expected outcomes.
- Lessons Learnt log is kept.
- Plan is reviewed annually.



GRIDCo's OT Incident Management Process Improvement

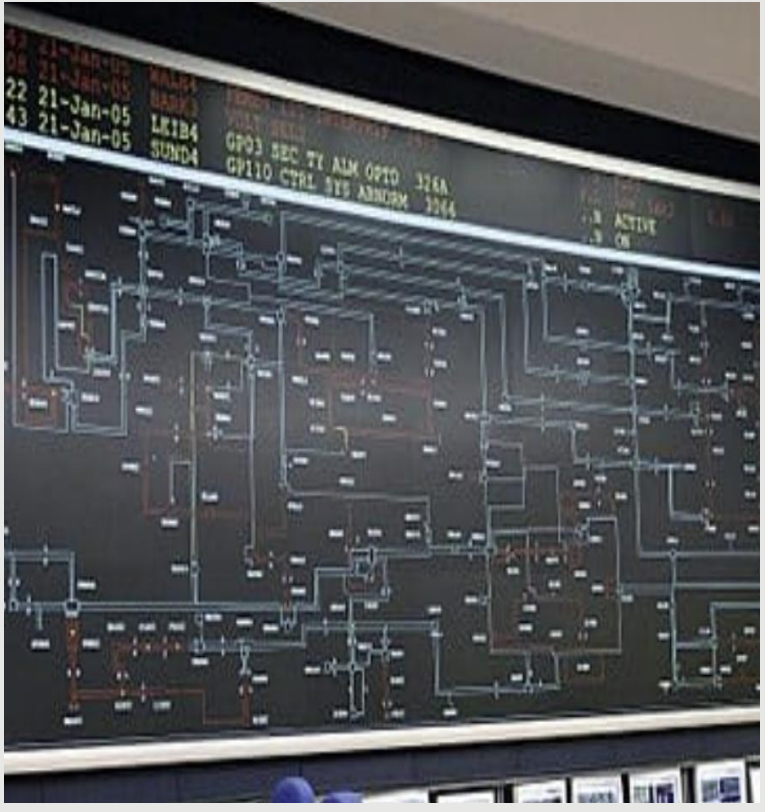
We used Lean Six Sigma Approach we learnt through the USAID-sponsored Business Innovation Project to improve our incident management processes.

The Process has been incorporated into our IRP

- Know your Suppliers and Third Parties:
  - Have categorized database of all Suppliers, Vendors, and Contractors, and engage them through that database.
- Undertake periodic assessment of their cybersecurity compliance status
- Vendors legally accept responsibility for their undeclared vulnerabilities
- Pre-tender cybersecurity assessment – for specific activities

A Case Study: SCADA Upgrade Project

- Scope: Upgrade of the SCADA System including deployment of DR Site Control Centre.
- Ensured Security-by-design during scoping and Requirements gathering.
- Pre-qualification (Cybersecurity) of Tenderers
- Tenderer accepts responsibility for undeclared vulnerabilities
- FAT at Vendor's Factory: OILs are documented for resolution
- Site Acceptance Testing – before project sign-off, includes CS Reviews and regression testing. Firewall config & Setup, HW and OS hardening, AD systems security and in Redundancy, Firewall Configs reviews.
- Actual Red-Team attack-attempts, both internally and remotely – staged breach.



Conclusion

- The Energy sector OT Cybersecurity threat landscape is rapidly evolving and expanding.
- Attacks are now many and more frequent: Power sector is one of the most targeted.
- Actors are increasingly getting, and using, sophisticated Malware tools.
- Interruptions / Disruptions have dire consequences (financial, security, social, political...)
- **Supply chain has become one of the most challenging vulnerabilities to address.**
- Unfortunately, cyber-supply chain accountability are usually not well-defined, and CISOs have little or no control over their supply chain.
- No matter how challenging, companies can start by identifying and mapping critical assets using a maturity framework (like NIST) to assess their maturing level, and take steps to treat critical gaps.
- **Incident management / response is as important as incident prevention.**

Tony Assan
Chief Information Security Officer