Improving ROI on Big Data through Formal Security and Efficiency Risk Management for interoperating OT and IT systems

Partha Datta Ray
CTO, Albeado Inc.
partha.dattaray@albeado.com

Grid-Interop

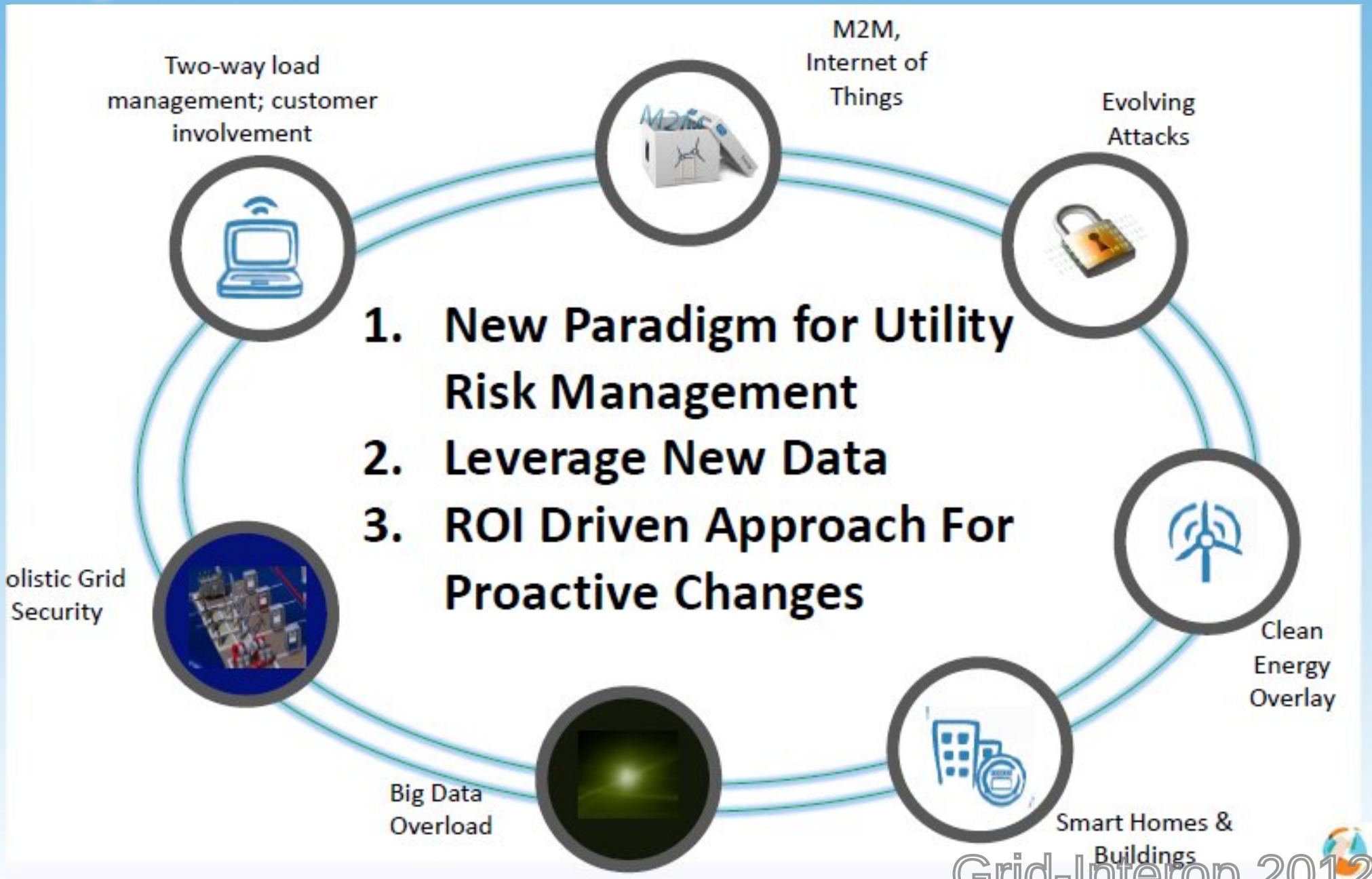
Driving to Grid 2020

Agenda

- Background
- Changing Security Landscape
- Interconnected OT & IT
- Addressing Interconnected OT & IT Threats
- Distributed & Pervasive Security Model
- ROI Analysis & Metrics
- Conclusion

Grid-Interop
Driving to Grid 2020

Background



Grid-Interop
Driving to Grid 2020

Changing Security Landscape

Big Data & The New Paradigm

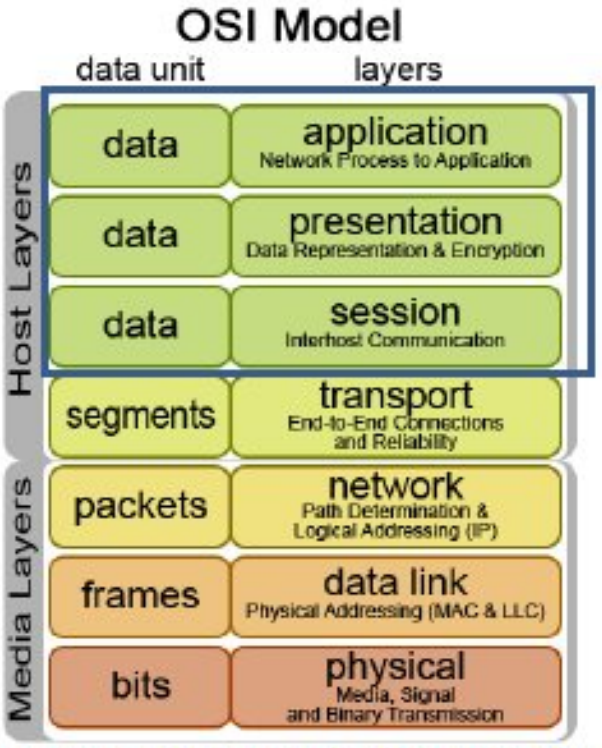
	Current State	Anticipated Transformation
OT & IT Systems	• End points, perimeters • Separate and in siloes	• Systemic and Pervasive • Unified and Holistic
Security Context	• Malware signature • OSI layers1 - 7	• Signature less, Business Context • GWAC layers 4 - 6
Security, Efficiency, Compliance	• Uncorrelated • No leverage in analysis and actions	• Aggressively correlated • Full leverage
Reliability	• Protect against equipment failures, operational errors, and natural disasters	• Leverage anomaly monitoring and exception response against attack, fraud

Grid-Interop

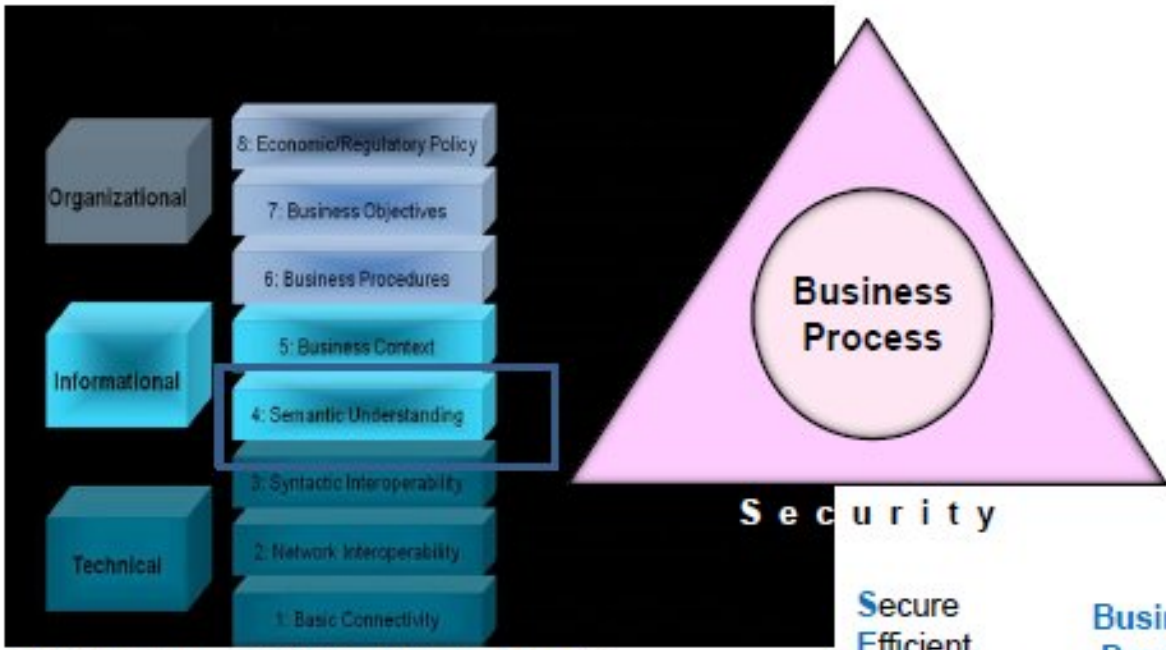
Driving to Grid 2020

Interconnected OT & IT Now a necessity

- Integration of IT and OT(Operational Technology) systems is a requirement for leveraging Smart Grid investments.
  - Delivery of smart customer services such as outage event intelligence
  - Efficient integration of renewable sources
  - Customer energy consumption analysis and control in real time
  - Increased coordination of business activities in interlinked utility domains -



OSI Stack Source: Wikimedia Commons/Dino.korah



GWAC Stack Source: GridWise Architectural Council

Grid-Interop™

Driving to Grid 2020

Addressing Interconnected OT & IT Threats

A formal **Risk Management** system will be needed to make the analysis of such Big Data **manageable, scalable, and effective** by prioritizing inputs to the processes which are found to be more relevant and consequential.

Current methods
- Intrusion Detection
- Intrusion Prevention

Point or perimeter defense solutions

Privacy, Higher Security

Operate at layers 1 – 7 of the Open Systems Interconnect (OSI) model

Future methods
- Current methods
- Anomaly in business context

Plus

Signature less, persistent control Message Security

Low Latency

High Availability

Focus on OSI layers 5-7
GWAC levels 4-8

Grid-Interop™

Driving to Grid 2020

Distributed & Pervasive Security:

Collaborating, Self-similar runtimes

Grid State (V, I, f, Φ, P, ...)

IEDs, RTUs, Meters , etc.

Control

Data

OT + IT

Apps &Services (CB, DMS, SCADA)

Security State (Services. Network, Devices)

BIG DATA

OT

IT

OT

IT

OT Big Data Prioritization

IT Big Data Prioritization

Domain Knowledge Base

Systemic Security, Efficiency, Compliance (SEC) Engine

Inference and Control Engine

Report

Alerts

Security and Risk Control Postures

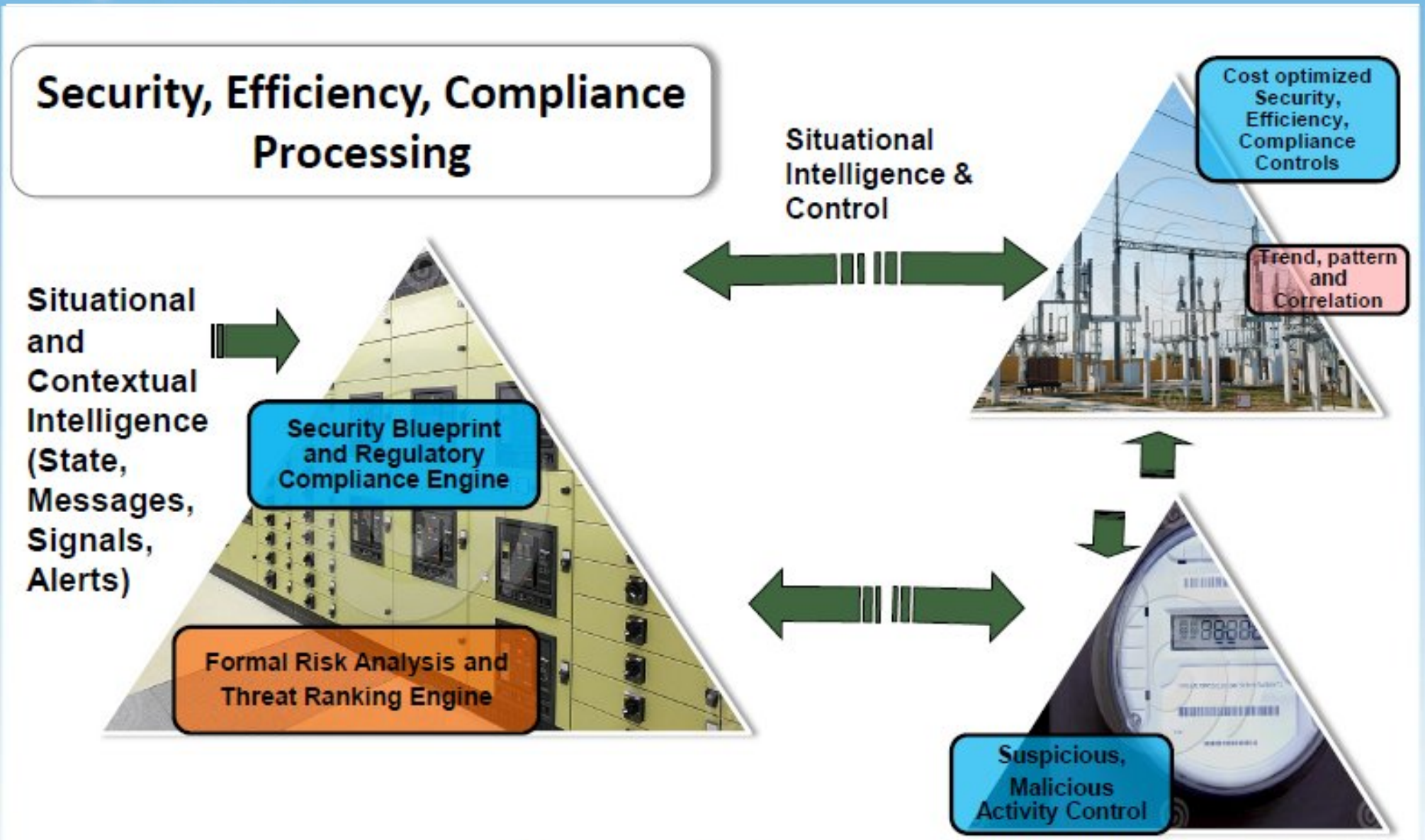
Albeado Confidential

Grid-Interop™

Driving to Grid 2020

Distributed & Pervasive Security:

Collaborating, Self-similar runtimes



Grid-Interop

Driving to Grid 2020

ROI Analysis & Metrics

Awareness of the new OT-IT integration requirement and a systemic way of evaluating Security, Efficiency and Compliance requirements needs to be derived.

Use cases then drive the ROI model to help prioritize the investments required.

Threat	Estimated Financial Loss	Actual Financial Loss	Estimated Posture Cost	Actual Posture Cost	Freq.
Electric Theft	Estimate	Derive	Estimate	Derive	N
Denial of Service	Estimate	Derive	Estimate	Derive	N
Meter Tamper	Estimate	Derive	Estimate	Derive	N
Water Leak	Estimate	Derive	Estimate	Derive	N
Gas Leak	Estimate	Derive	Estimate	Derive	N

ROI analysis aspect of the risk management system can guide the inference engines and decision control systems to recommend and actuate control activations.

Conclusion

IT and OT domains integration effectiveness will depend on

- Correlated view and analysis of IT and OT events
- Integrated Risk Management guiding big data analysis
- Consistent ROI and Risk Management metrics
- Systemic Security, Efficiency & Compliance engine