Not Protectively Marked

Smart Grid – Professional Security Services Perspective

Chris Rees

25th May 2016

MWR LABS

MWR LABS

1. Introduction

2. Smart Grid Topology and Domains

3. Security Considerations

4. Summary

MWR LABS

+ Chris Rees
+ Principal Managing Consultant at MWR
+ Based in Singapore
+ Been working in IT Security 10 years+
+ Provide perspective from a Professional Security Services firm

++

Domain Model

Generation

Generation optimization
Renewable integration
Distributed generation mgmt
Microgrids
Protection & control

Transmission

Grid diagnostics & visualization
Reliability & demand forecasting
Grid protection & control
Fault detection & restoration
Wide area measurement system
Substation digitization
Transformers & voltage mgmt.
Distribution & outage mgmt. system
Geospatial information system

Distribution

Asset monitoring
Backup power mgmt. & control
Energy management system
Plant load management
Protection & control
Sub-metering TOU Reporting

Power Consumers

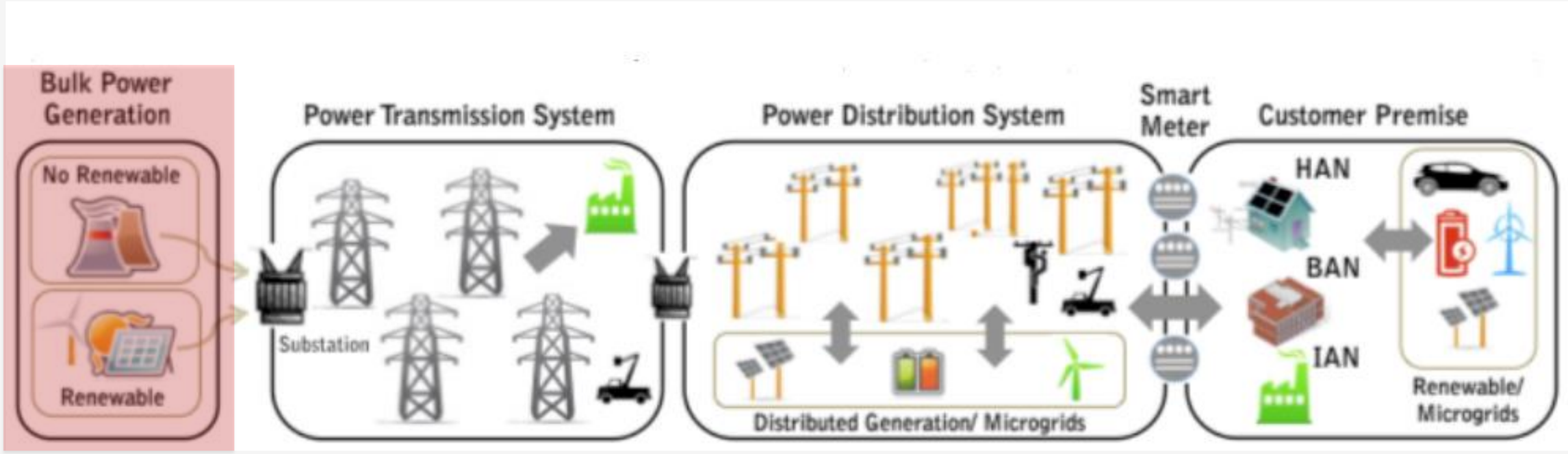
Smart meters
Wireless AMI
Smart appliances

MWR LABS

Smart Grid Topology and Domains

Generation Domain

- Backbone/Core networks
- Utility Local Area Networks
- Substation Networks



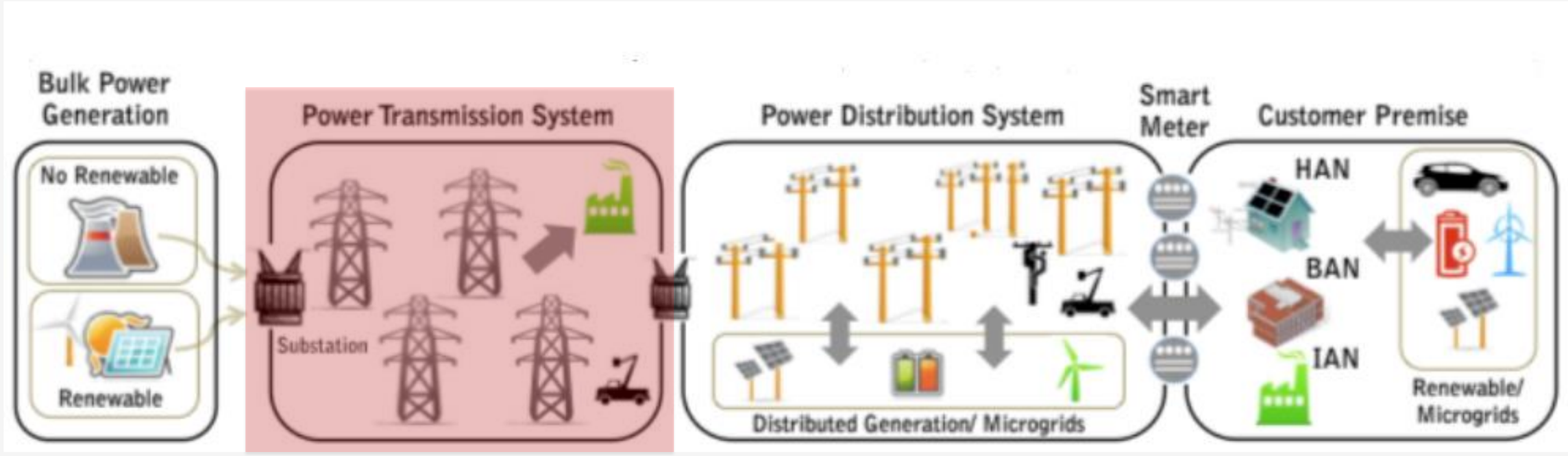
MWR LABS

Smart Grid Topology and Domains

++

Transmission Domain

+ Regional/Metropolitan Area Networks (MAN)/PLC
+ TSO balancing supply and demand
+ Substation RTU's connected to SCADA/DMS/EMS

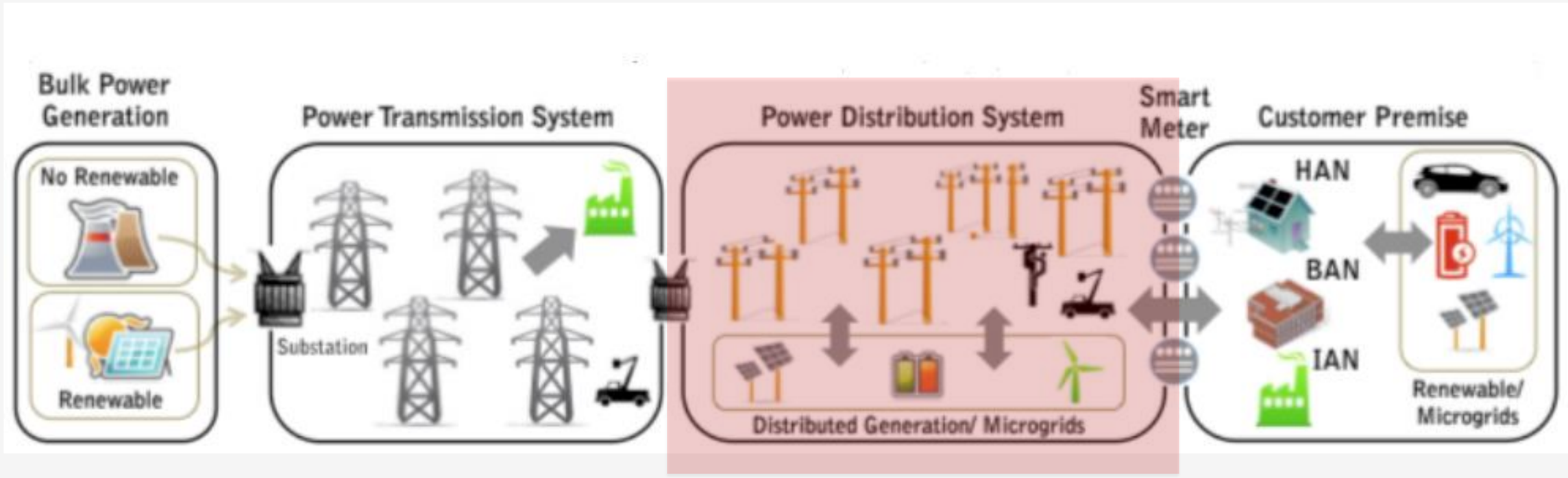


Smart Grid Topology and Domains

MWR LABS

++ Distribution Domain

+ Extended/Neighbourhood Area Network (EAN/NAN)
+ Advanced Metering Infrastructure (AMI)/PLC
+ Field Area Network (FAN)



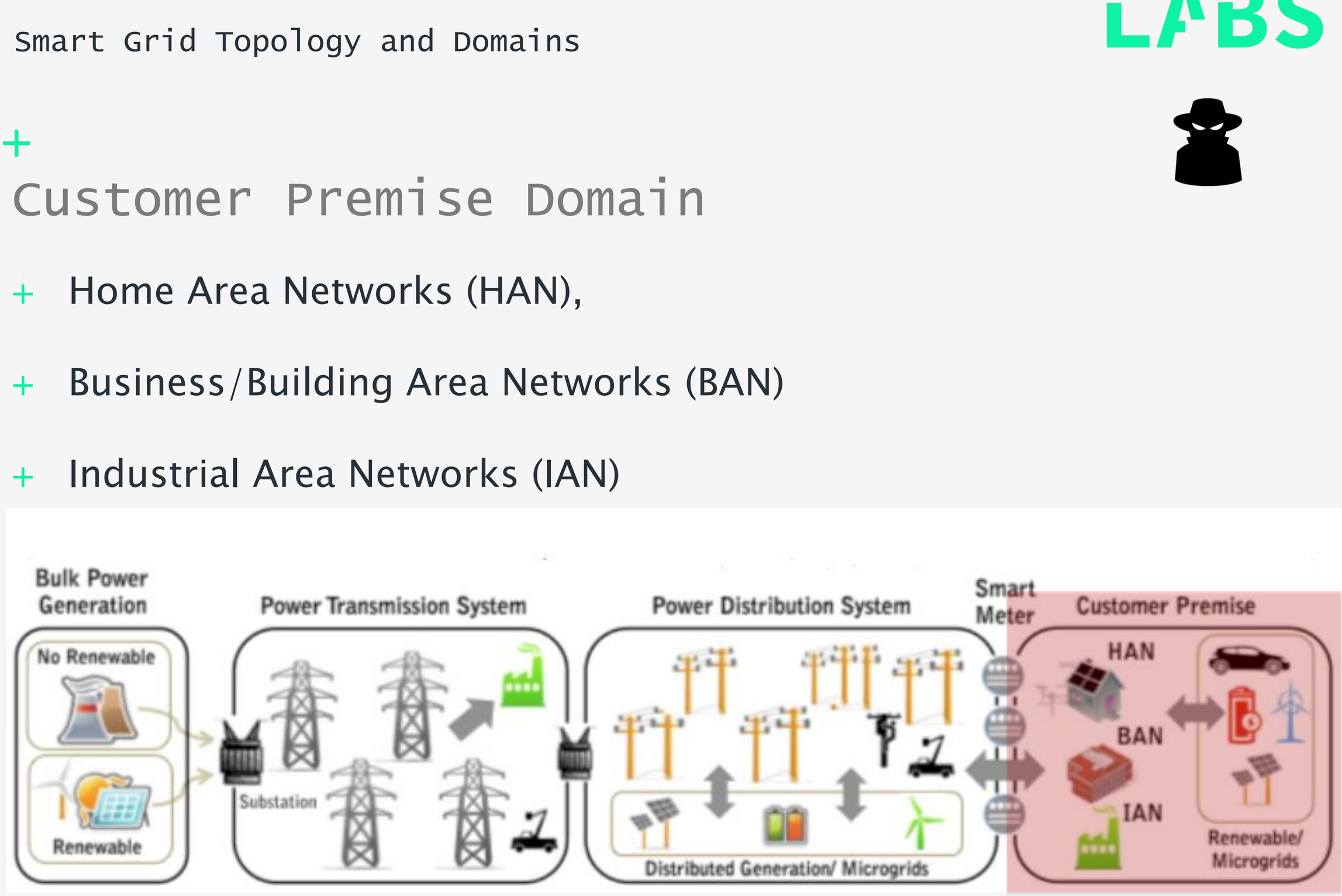
MWR LABS

Smart Grid Topology and Domains

++

Customer Premise Domain

+ Home Area Networks (HAN),
+ Business/Building Area Networks (BAN)
+ Industrial Area Networks (IAN)

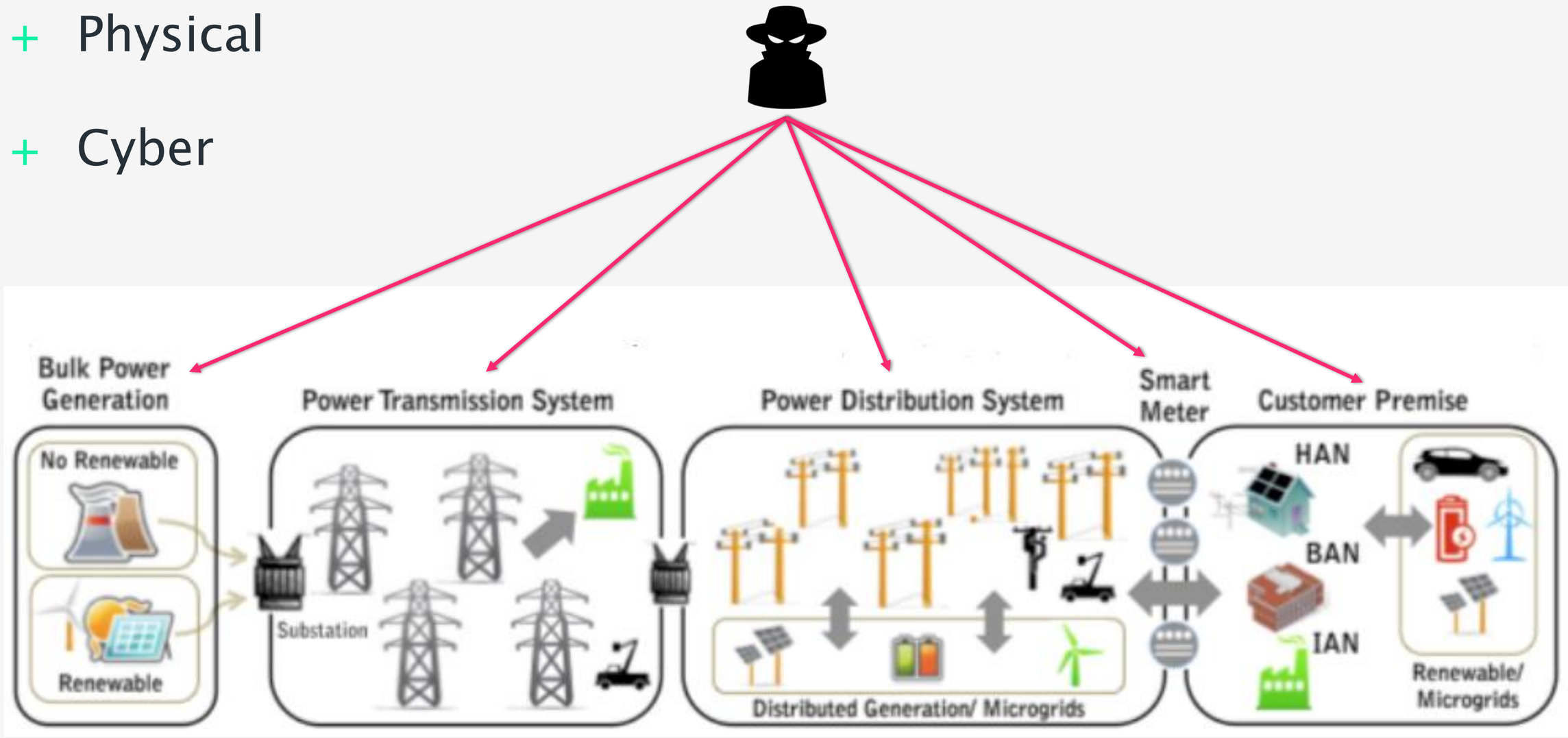


MWR LABS

Smart Grid Security Considerations

Adversarial Threats

+ Physical
+ Cyber



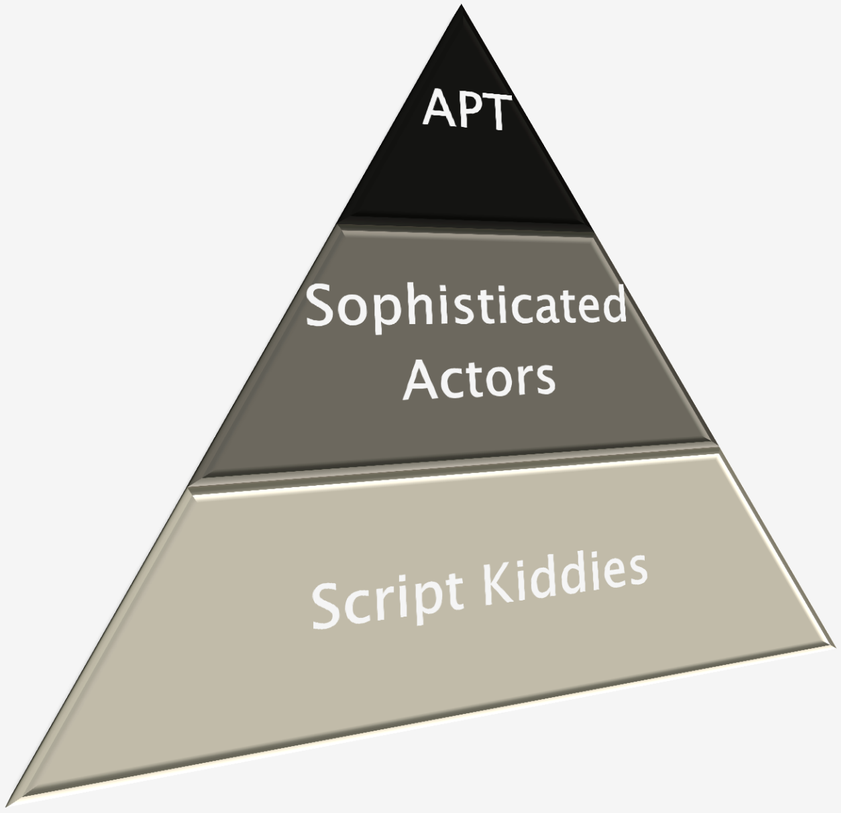
MWR LABS

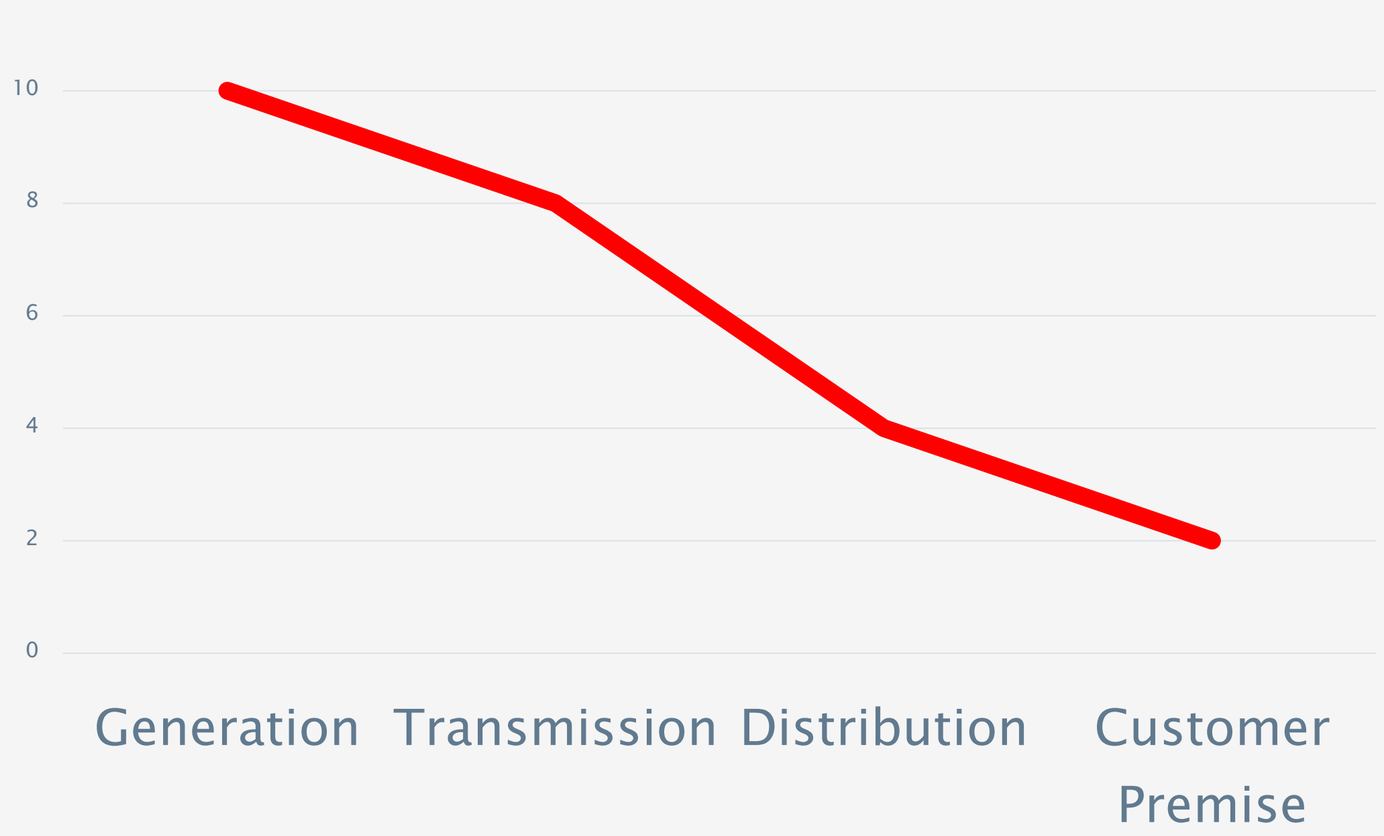
Smart Grid Security Considerations

++

who?

Threat Actor Capability



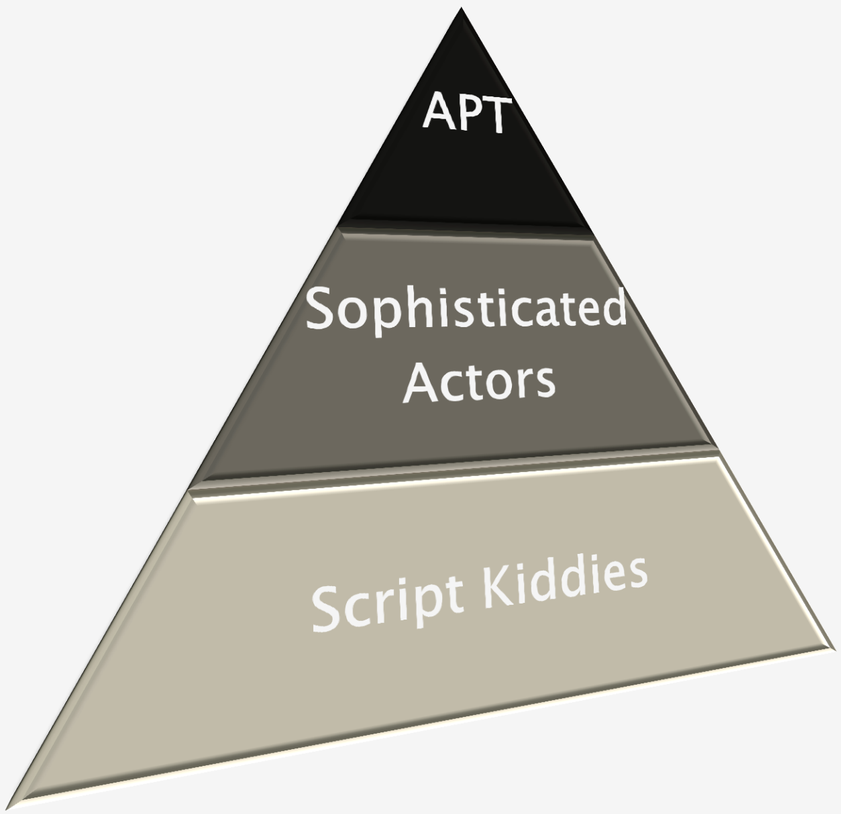


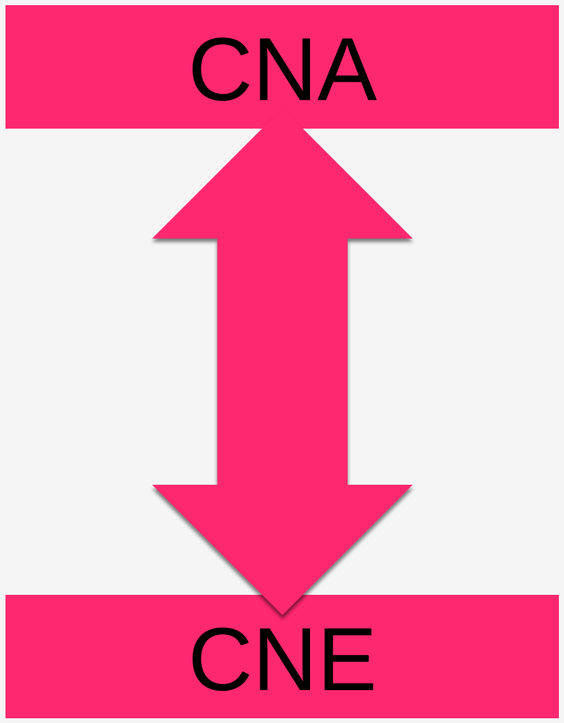
MWR LABS

Smart Grid Security Considerations

++

Why?



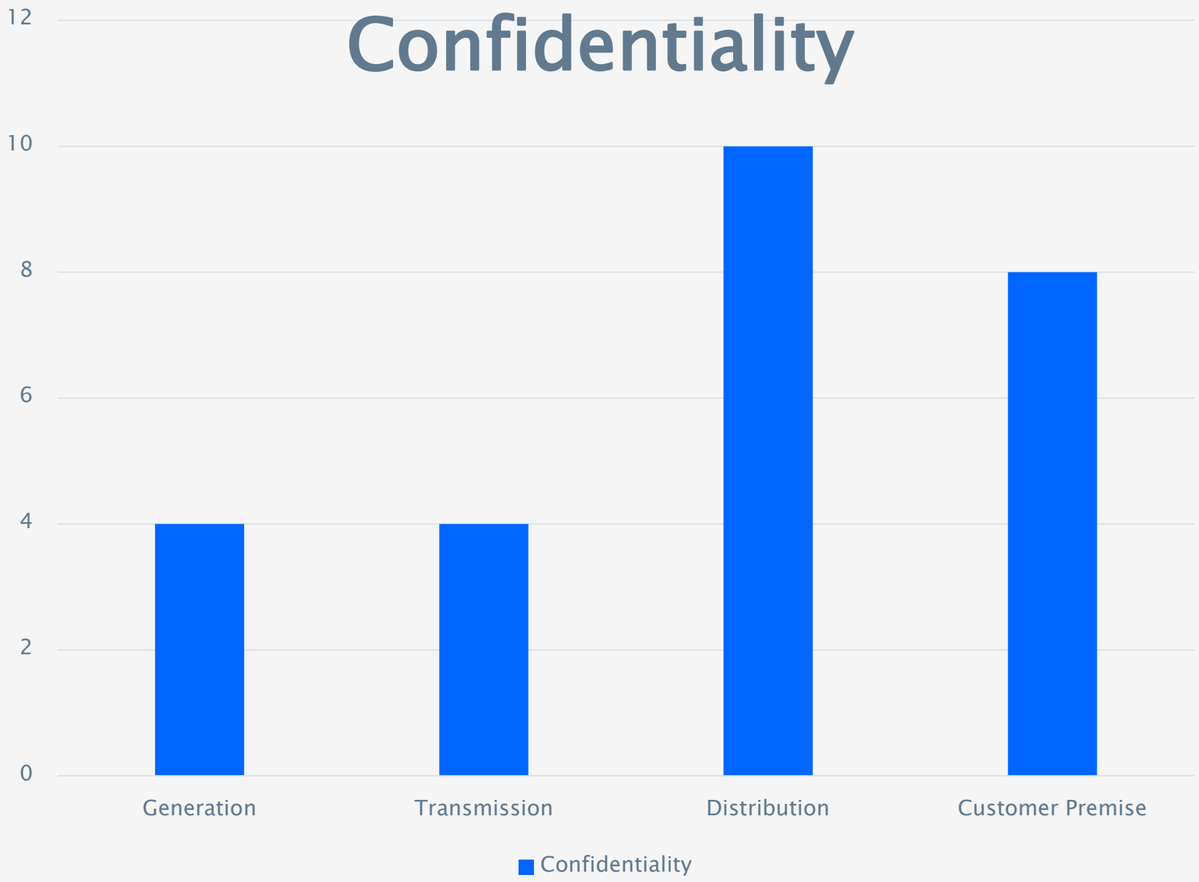


MWR LABS

Smart Grid Security Considerations

++

Why?



MWR LABS

Smart Grid Security Considerations

++

Why?

MWR LABS

Smart Grid Security Considerations

++

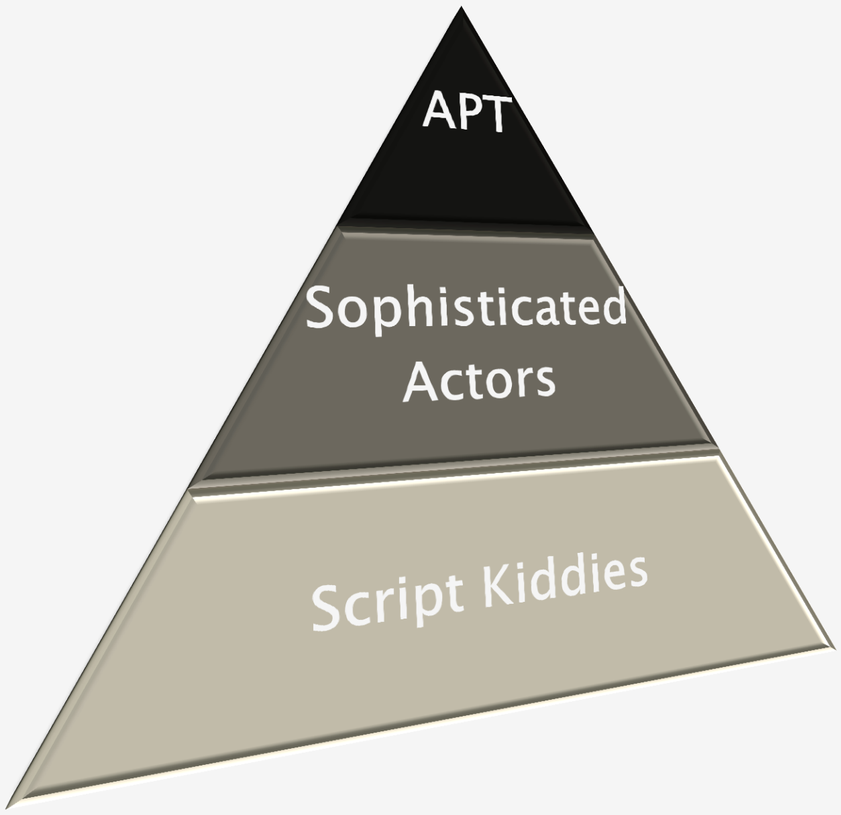
Why?

MWR LABS

Smart Grid Security Considerations

++

How?



Tactics, Techniques, and Procedures (TTPs) @

Tactics - The employment and ordered arrangement of forces in relation to each other

Techniques - Non-prescriptive ways or methods used to perform missions, functions, or tasks

Procedures - Standard, detailed steps that prescribe how to perform specific tasks

The term TTP is used to refer broadly to the actions that one might take in a particular problem domain.

42

* JP 1-02, DoD Dictionary of Military and Associated Terms, 8 Nov. 2010, available at http://www.dtic.mil/doctrine/

MWR LABS

Summary

++

Smart Grid Cyber Security Strategies

+ Strategies will differ depending on domain/threats
+ Adopt threat-centric approach to cyber-physical security
+ More focus on detection and response
+ Cyber security awareness training
+ All domains face traditional IT security risks (protect)
+ Procurement product evaluations need to include security
+ Security research community needs to focus on developing new tooling

MWR LABS

Questions?