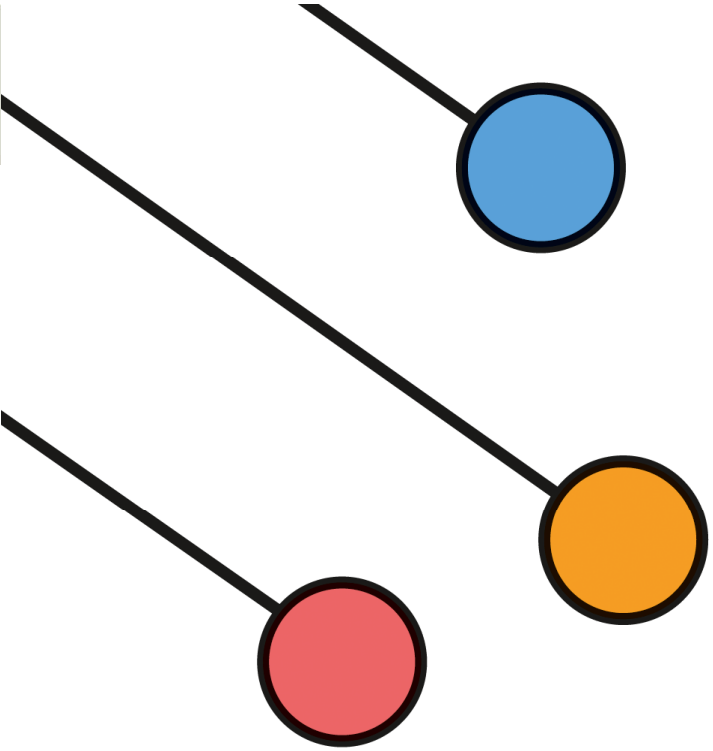


s|u|c|c|e|s|s

securing critical
energy infrastructures

European Commission

DNV·GL

SUCCESS – Innovation Event

22nd September 2016

Terni

Ganesh Sauba

DNV GL

Netherlands

WP1:Threats to security of smart meters and devices

- Task 1.1: Identification of existing threats - DNV GL
- Task 1.2: Thread Modelling and Analysis of potential new threats - SYN
- Task 1.3: Threat Classification and Risk Analysis - ISMB

Task 1.1 : Identification of existing threats

1. Identification of security threats
2. Extensive literature view
3. Weakness analyse
4. Information security aspects of smart meters

Task 1.2: Thread Modelling and Analysis of potential new threats

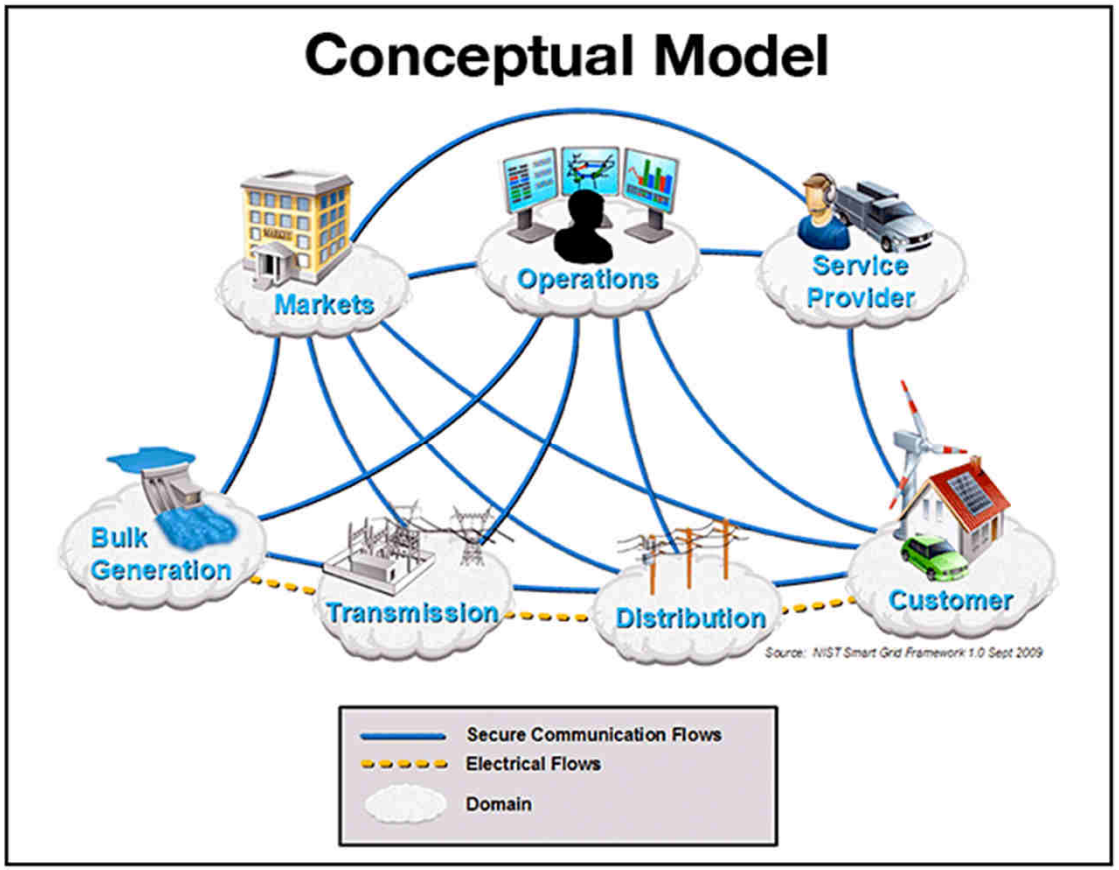
Perform threat and risk modelling in order to:

1. Identify and validate behavioural signatures of well-known and potentially new smart grid asset threats
2. Grant SUCCESS the capability of detecting possibly malicious behaviours against the various components of Smart Grid networks (including NAN assets and AMI, SCADA and DMS infrastructure) and classify them as being actual threats or false positives.

Task 1.3 : Threat Classification and Risk Analysis

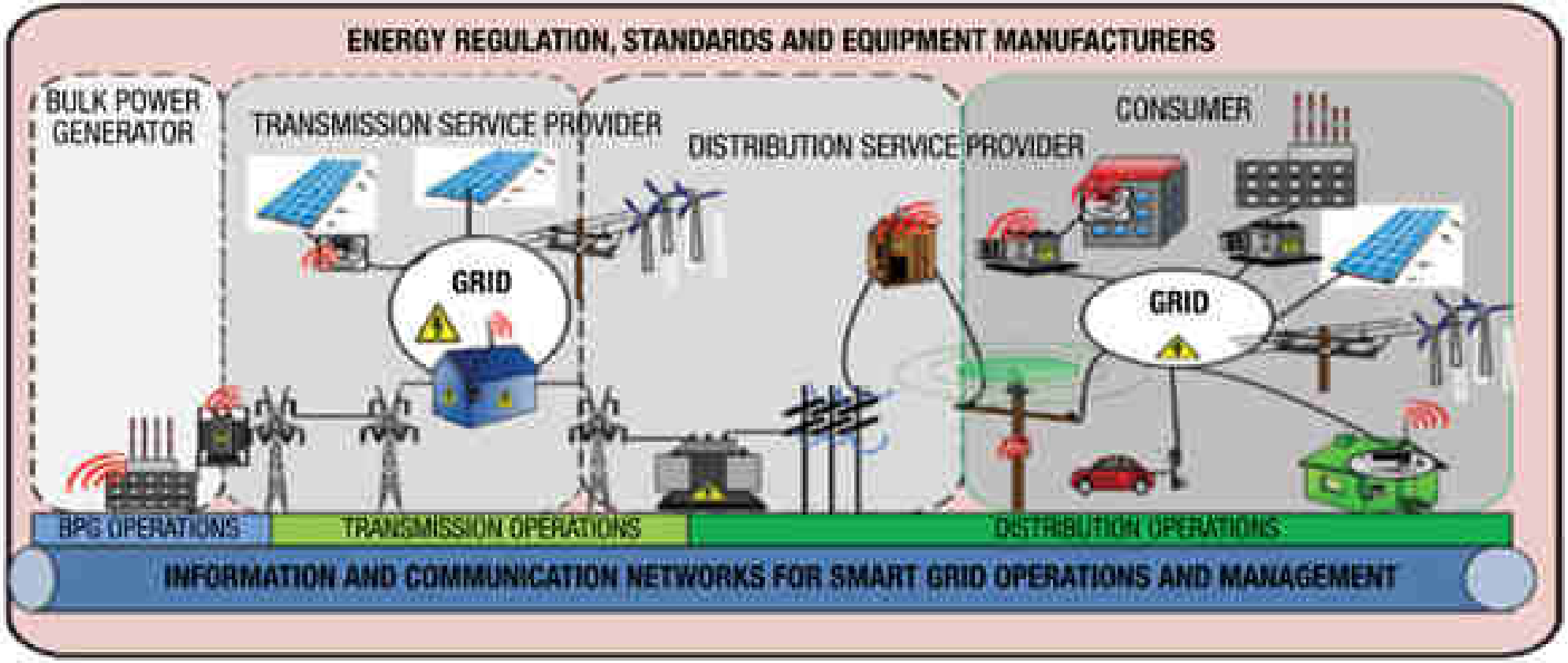
1. Categorise the afore-identified threats into vulnerability classes related to the affected actors.
2. Analysis performed to identify the impact that a potential successfully realized threat will bear to the system

Simplified Conceptual Model



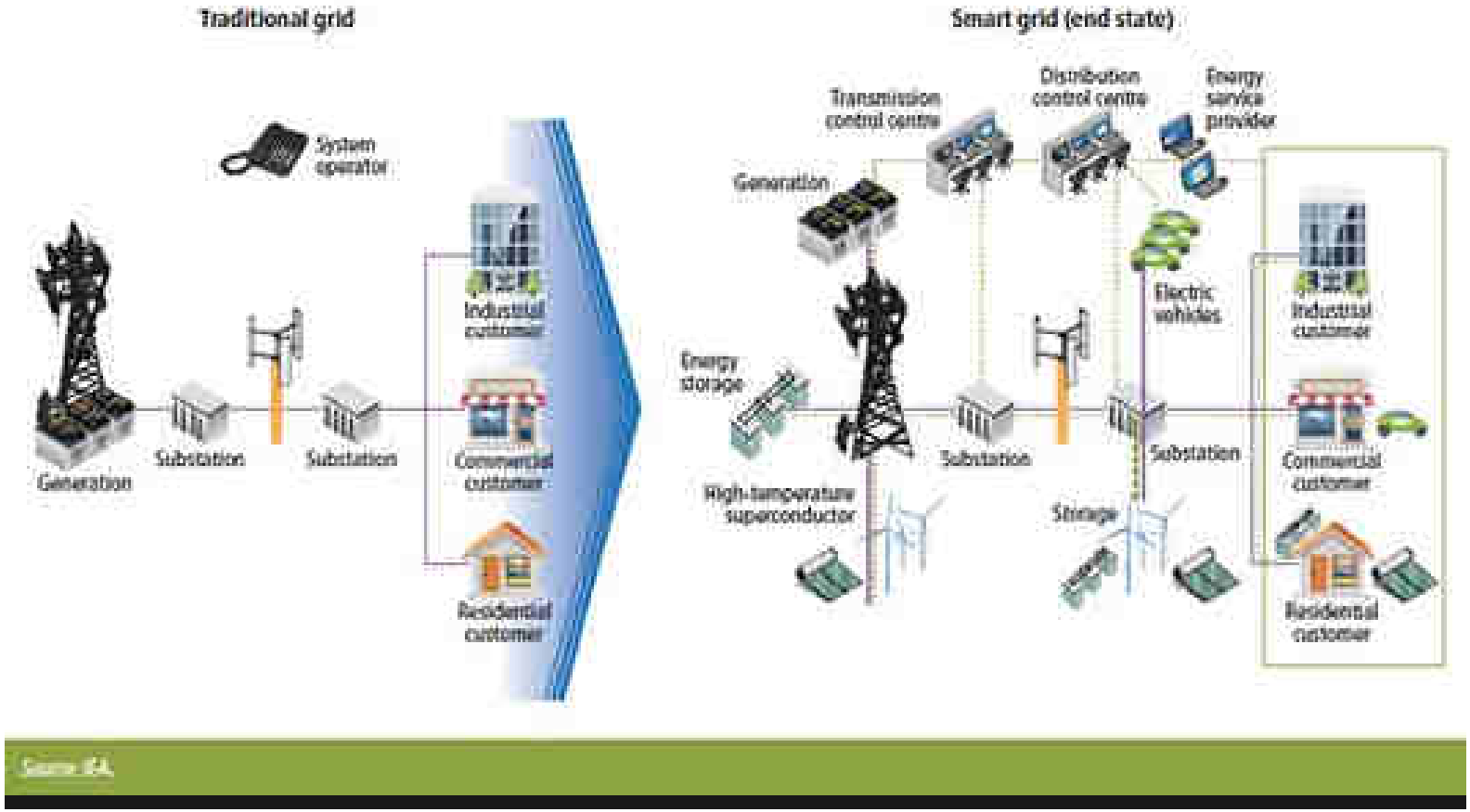
Source: JDS Management

Typical Electricity Value Chain

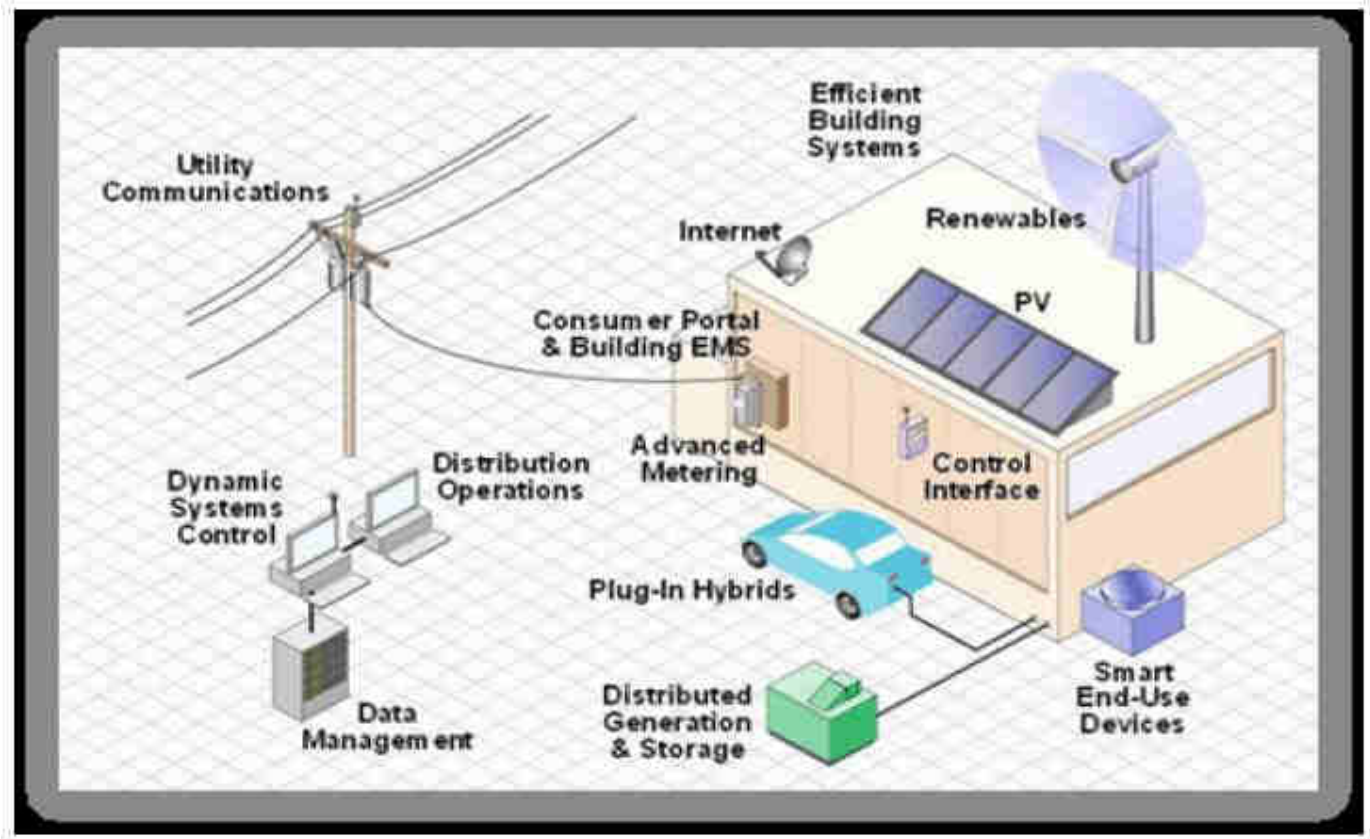


Source NIST

Traditional v/s Smart Grid



Vulnerability Points



Source: cnet

Acknowledgements

- Colleagues in the SUCCESS consortium
- Colleagues at DNV GL
- Information Sources used in this presentation
- European Commission Research Executive Agency
- Horizon 2020 Programme
- Grant Agreement 700416

Horizon 2020
European Union funding
for Research & Innovation

Thank you.

ganesh.sauba@dnvgl.com

