Harnessing Machine Learning and Automations Against Advance Cyber Threats for Smart Grids

The 3rd International Symposium on Smart Grid

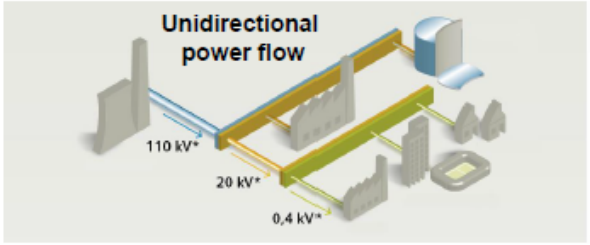
16-19 September 2019

Dr. Haiyu Li (Manchester University)

Smart Grids?

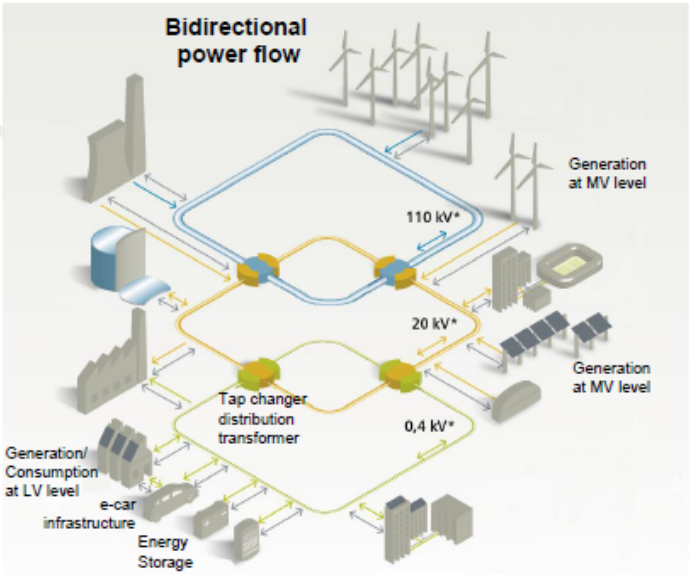
- AC or DC ? -> Reduce loss for efficiency transmission ?
- Integration of low carbon technology (LCTs), -> needs high level of automations and controls for better energy utilisation & efficiency

Today



- ❑ Radial system
- ❑ Simple protection
- ❑ Simple or no automation
- ❑ Simple or no communication

Tomorrow

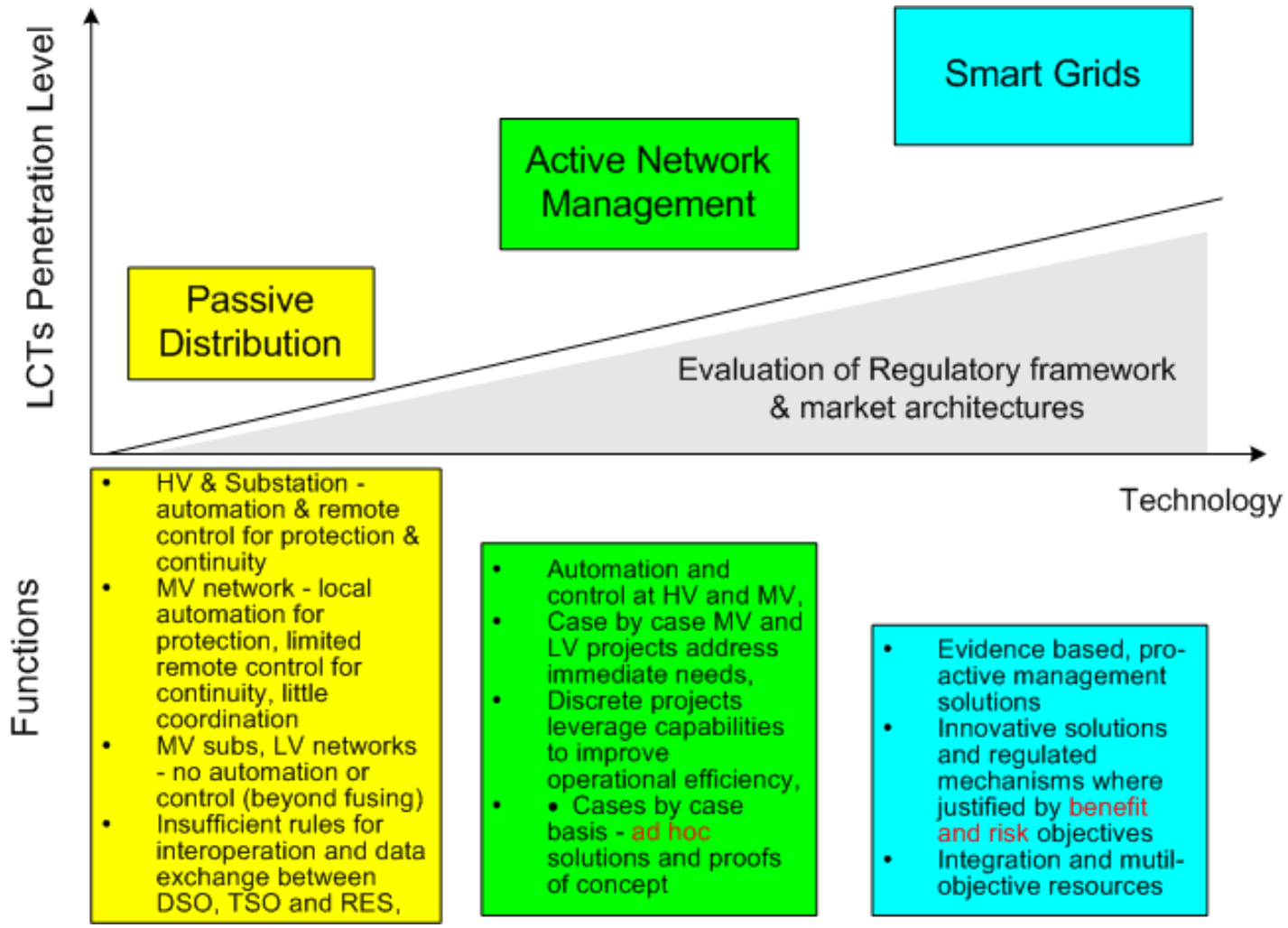


- ❑ Meshed system
- ❑ Adaptive protection
- ❑ High automation degree
- ❑ Bidirectional communication

Smart Grids?

Picture Source: Siemens AG 2013 from IntelliSub Europe, Nov 2013

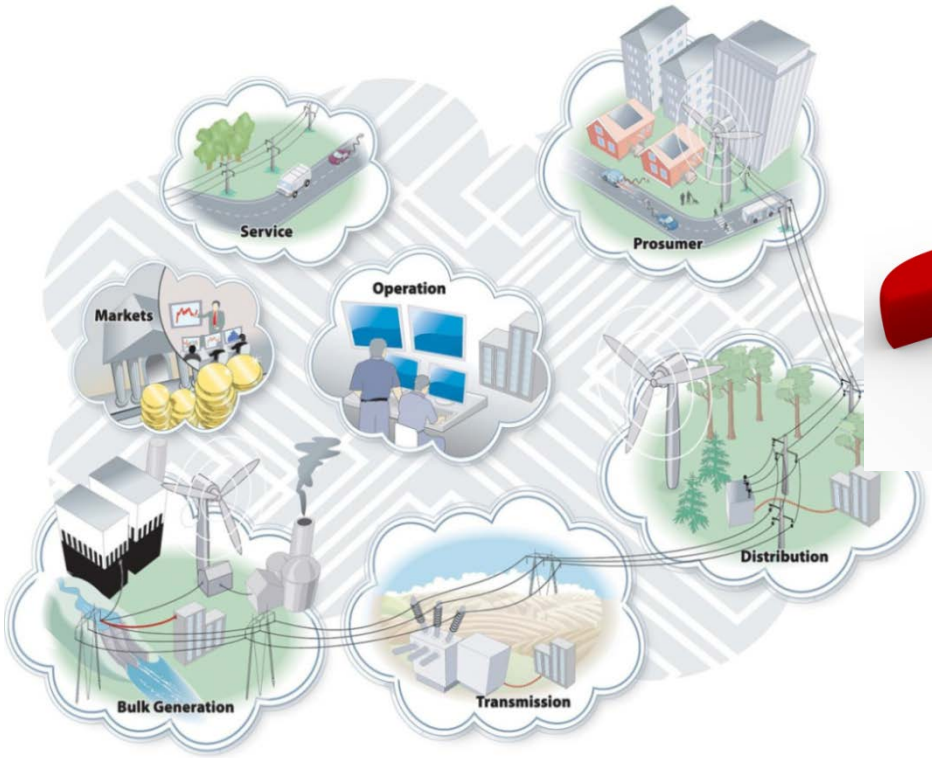
What Smart Grids Can Offer?



Source with editing : IntelliSub Europe, Nov 2013

Smart Grids = ICT + Power ?

The integration of kW/MW and kBit/Mbits to make the electricity networks that can cost efficiently integration of low carbon technology (LCT) as well as actions of all users connected to it …



How?

Picture Source: ISGT Europe 2010 Panel Session (PN 1): "Standards for Smart Grid"

Introduction and Motivation

- The Paris climate conference in late 2015 (COP21) has reached an agreement to aim to hold global warming well below 2°C and to pursue efforts to limit it to 1.5°C.
- UK ambition target of cutting 37% , 57% and 100% (zero) gas emission cut by 2020, 2030 and 2050, respectively.
- To address this crucial environmental challenge, UK NG and SPEN have started to digitise its energy systems – a step change in how use digital technologies that allows for two-way communication between the utility and its customers.

Introduction and Motivation

- Application of computing, digital communication, artificial intelligence and wide area monitoring technologies effectively increase the lifetime, efficiency and utilisation of electricity energy infrastructure as well as improve the ability and quality of monitoring and control of energy systems

- Digital substations with controls, computers, automation, and new digital technologies and computer-based Protection, Automation and Control (PAC) equipment working together play a crucial role in proving data collectors, sensors and information to the Supervisor Control And Data Acquisition (SCADA) system as well as the Wide-area Protection, Automation and Control (WPAC) systems.

Introduction and Motivation

- Since digital substations are enablers for the network power flow to be controlled and directed safely and securely from generation to demand, these makes them a highly attractive target for cyber-attackers aimed at disrupting operations.

- Ukraine power grid cyberattack took place in 23rd December 2015. It was considered to be the first known successful cyberattack on a power grid. Hackers were able to successfully compromise information systems of three energy distribution companies and temporarily disrupt electricity supply to the end consumers.

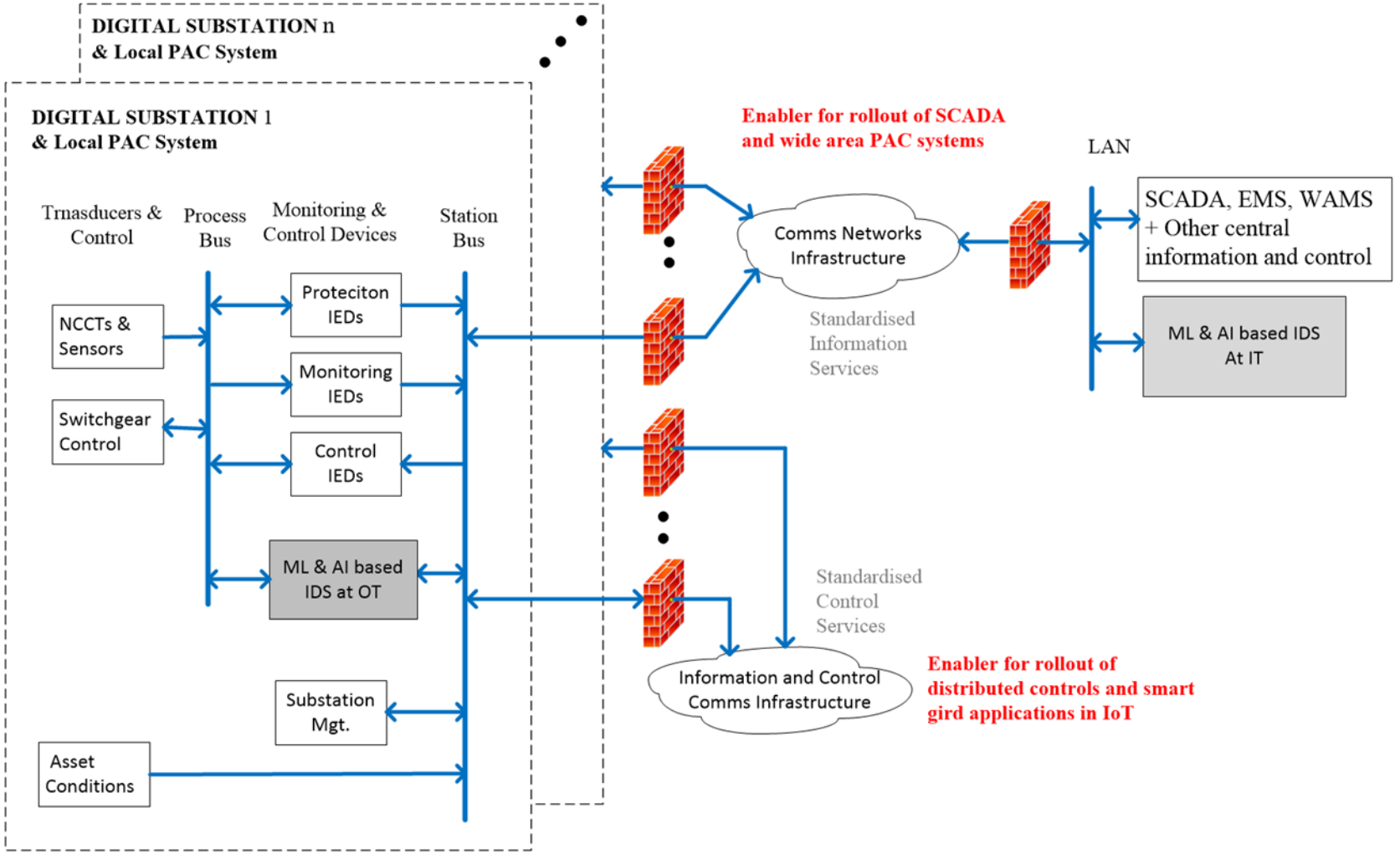
Introduction and Motivation

- In a worst case scenario these attacks can result in network infrastructure shut down completely, triggering economic and financial disruptions or even loss of life and massive environmental damage,

- The increase in cyber risk and concern about the resilient of electricity network PAC systems against advanced cyber treats has led to a need to address the cyber security challenges for smart grids or digital grids where may used the Internet of Things technologies (IoT),

- Motivation: Harness machine learning and artificial intelligent to build a defence system against advanced cyber threats.

Power Systems with OT and IT



Cyber Security Life Cycle

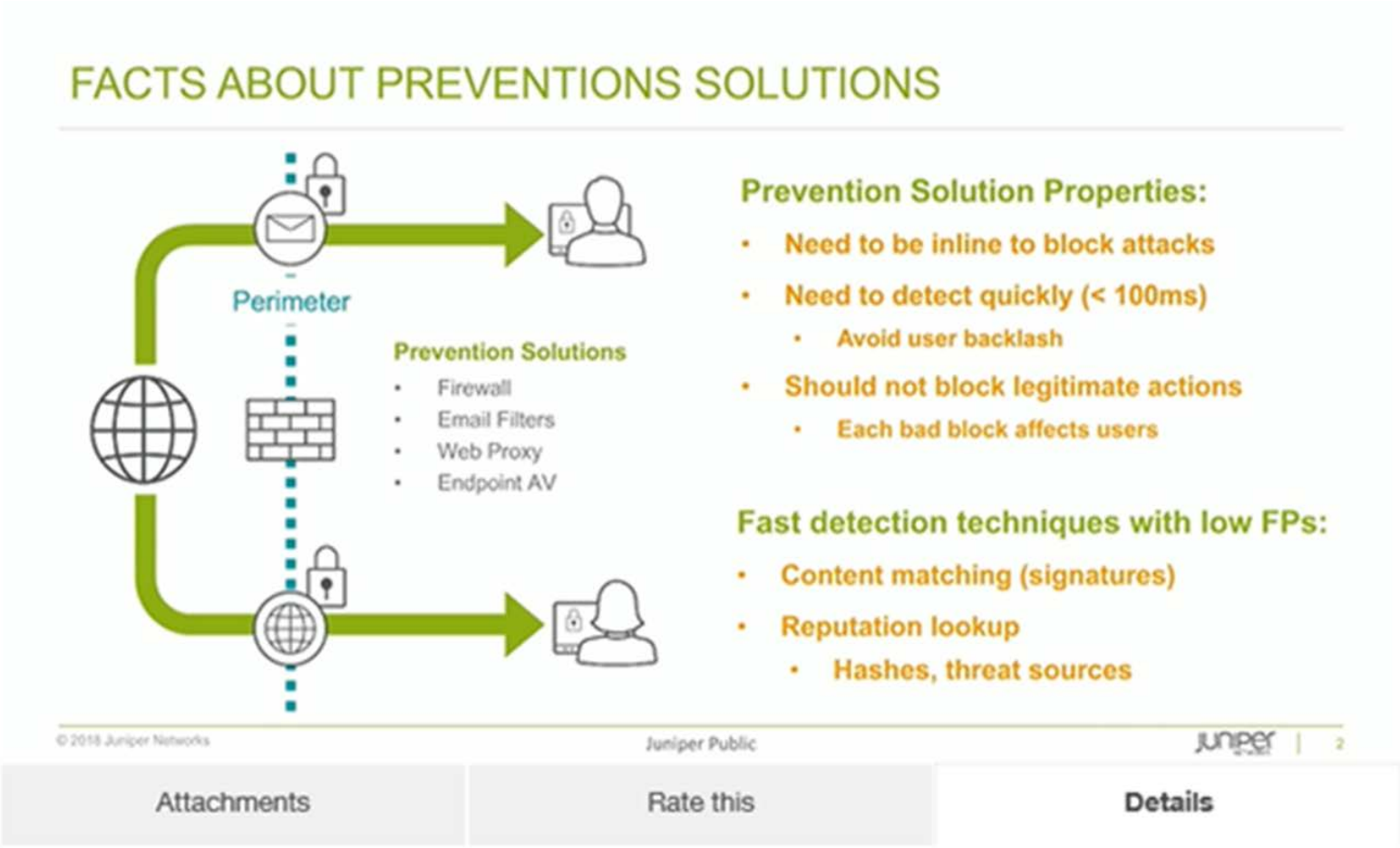
- **Cyber Prevention**: using already developed cyber security technologies, such as firewalls, spam email filtering, IEC62351 (security for power communication networks), IEC 62443 (security for industrial control system networks), etc.

- **Intrusion Detection System (IDS)**: Use different cyber instruction detection technologies, such as network traffic analysis, signalling statistical analysis, machine learning or artificial intelligent technologies to detect and identify known or unknown threats.

- **The response/defence system**: deploying suitable countermeasures, such as spam blocking or data recovering, to mitigate or remediate the risk for the system.

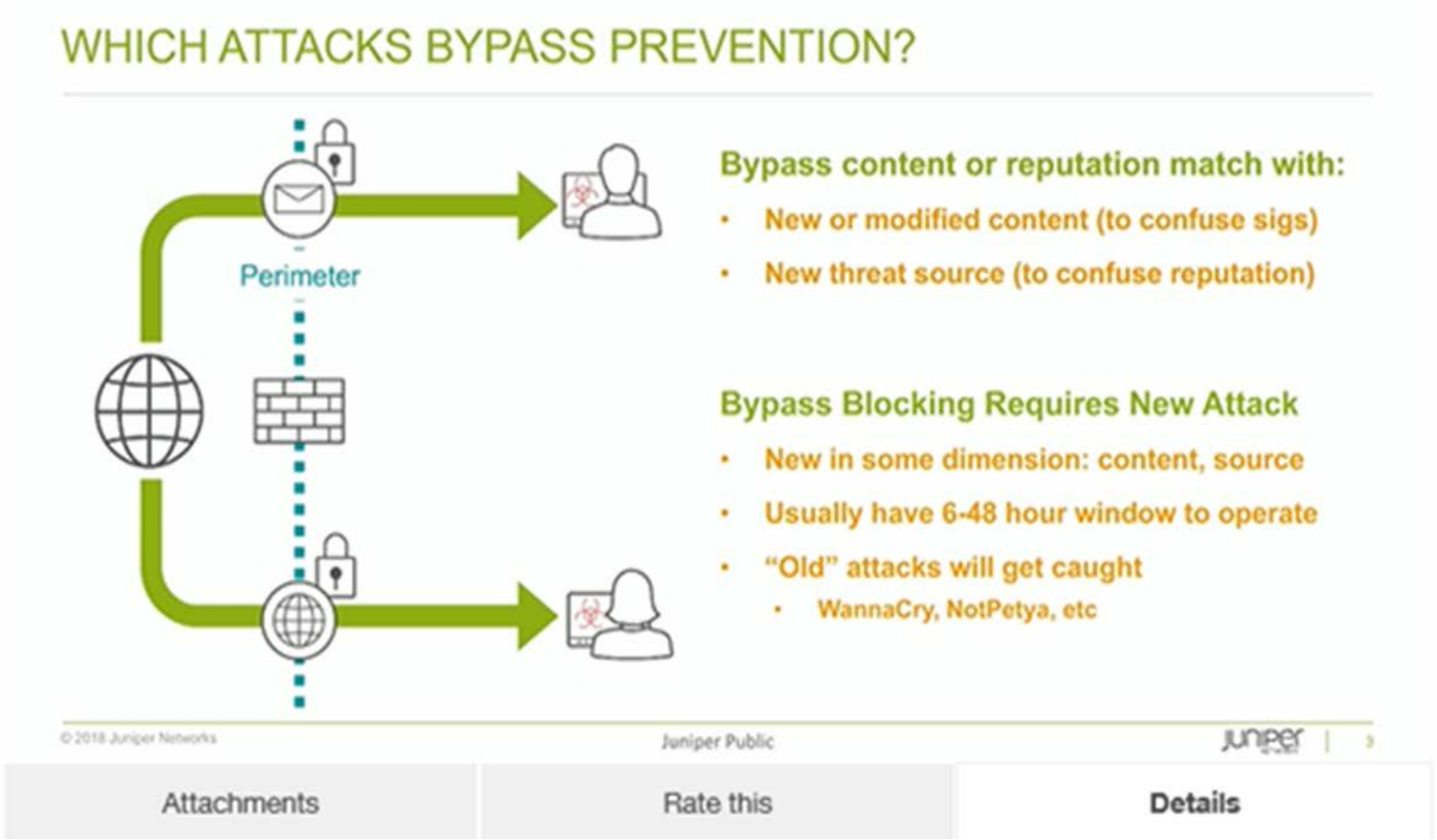
- **Cyber Security Improvement**: The lessons learnt help the system designers to improve cyber Intrusion Detection System (IDS) and implement new countermeasure against the cyber threats.

Machine learning and Automations



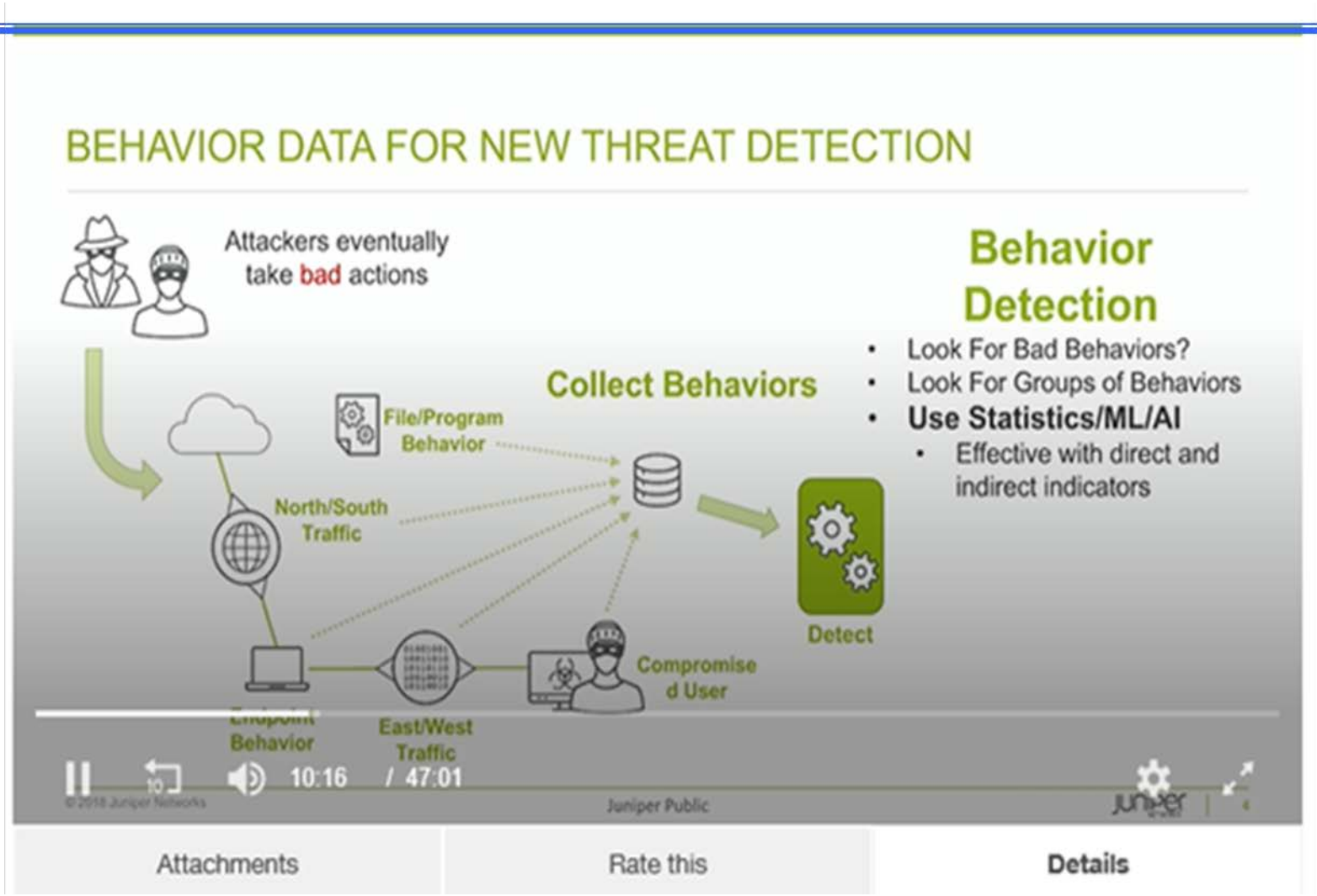
Source: BrigtTalk Website April 2019

Machine learning and Automations



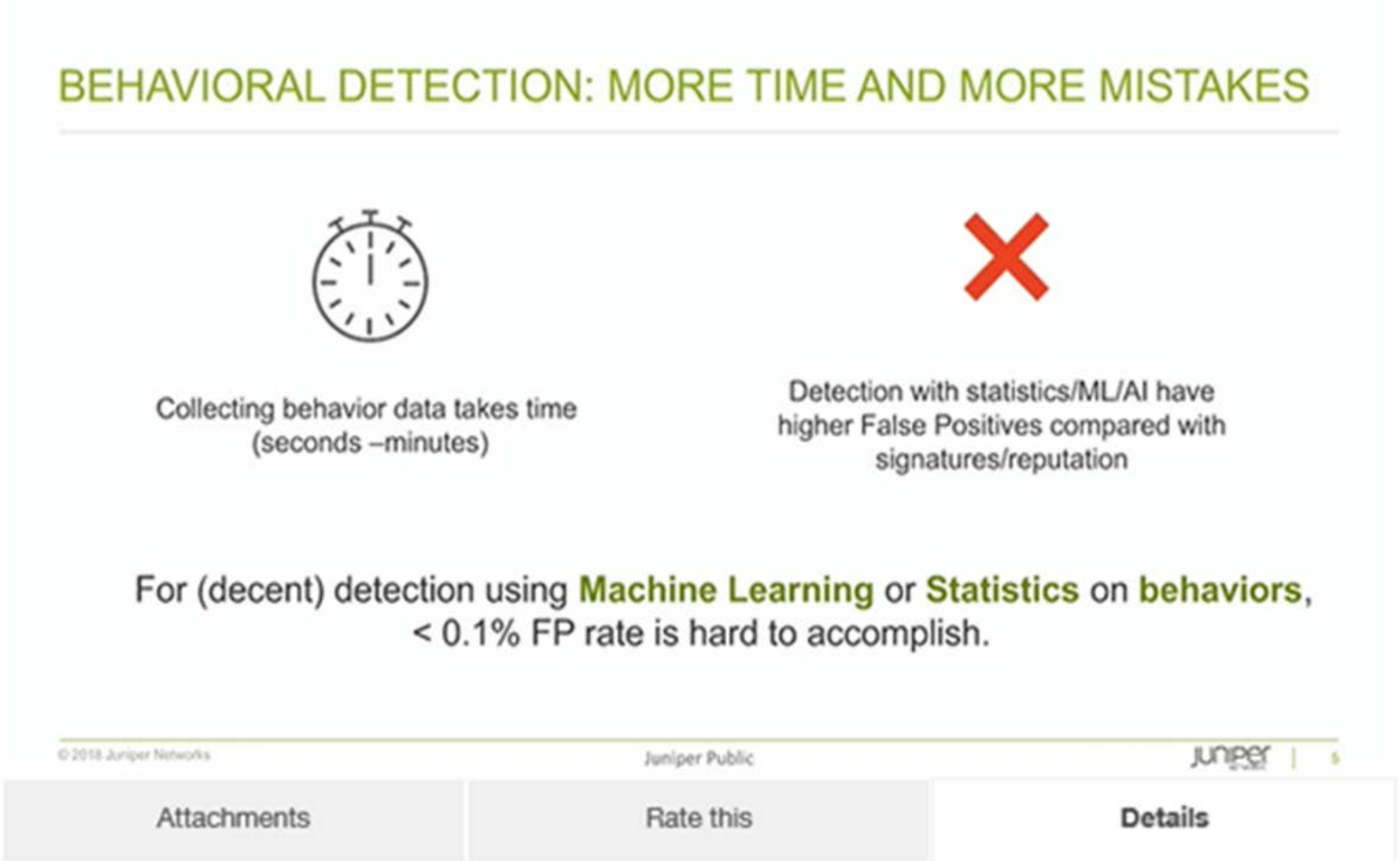
Source: BrigtTalk Website April 2019

Machine learning and Automations



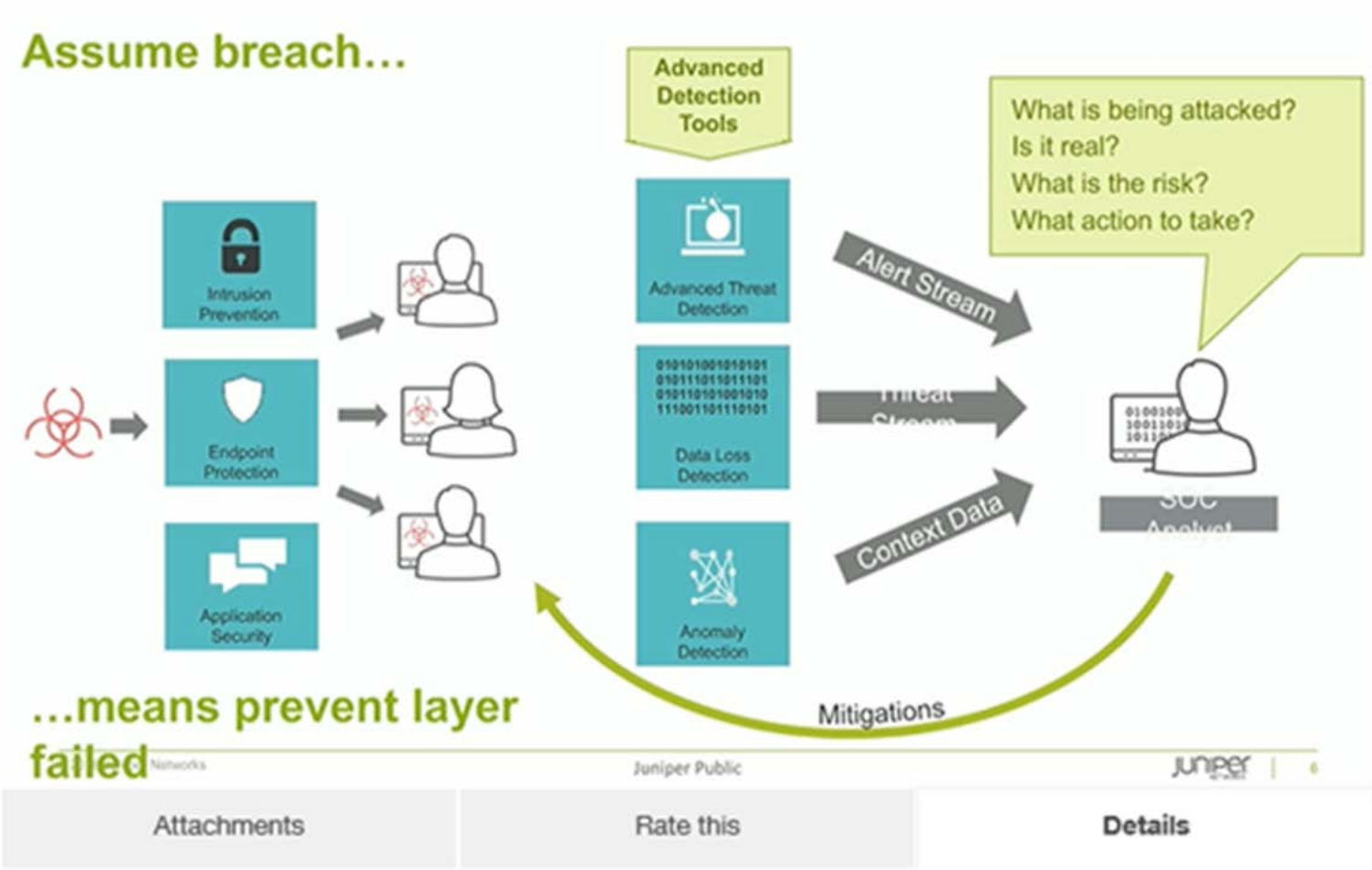
Source: BrigtTalk Website April 2019

Machine learning and Automations



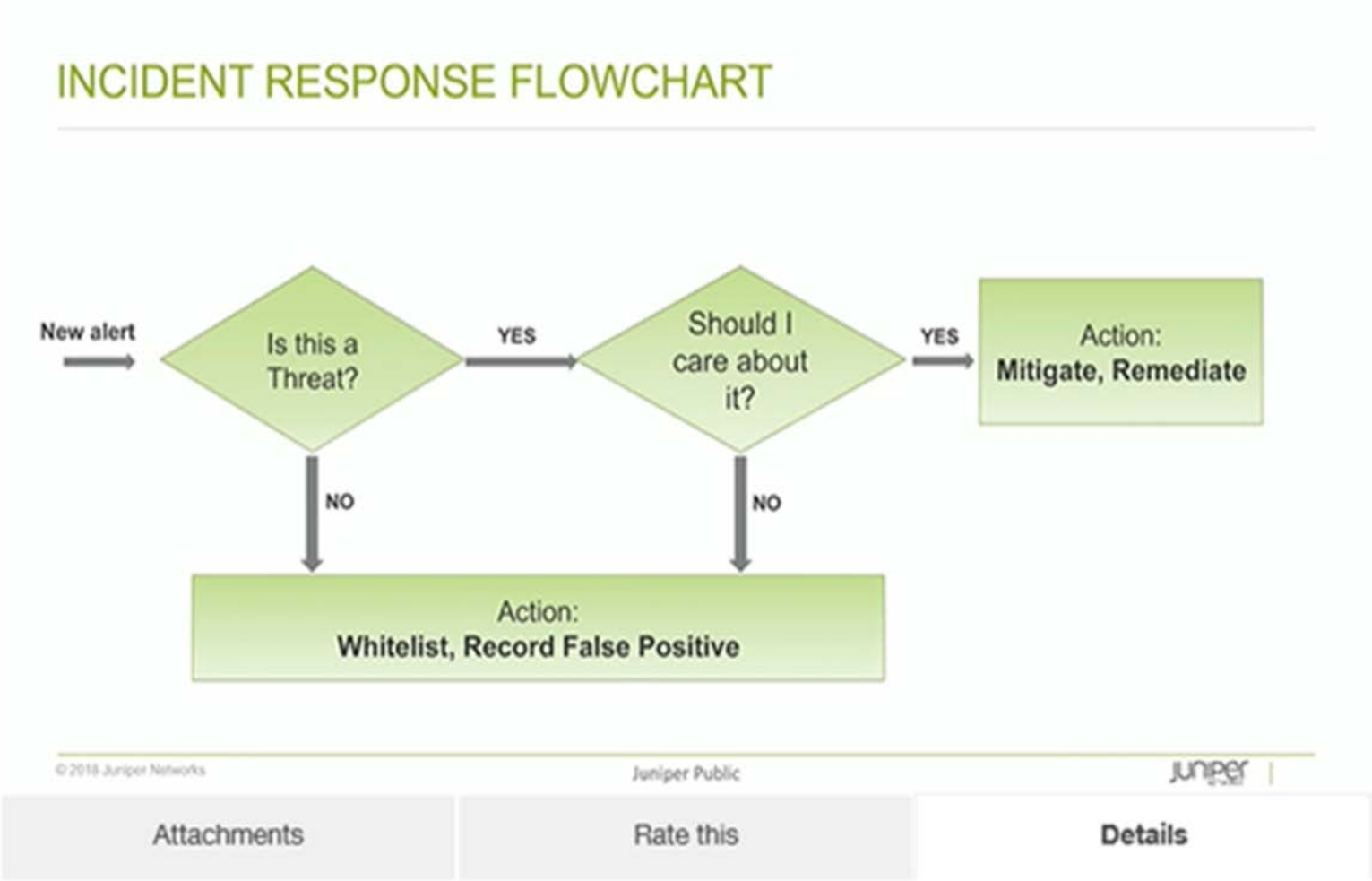
Source: BrigtTalk Website April 2019

Machine learning and Automations



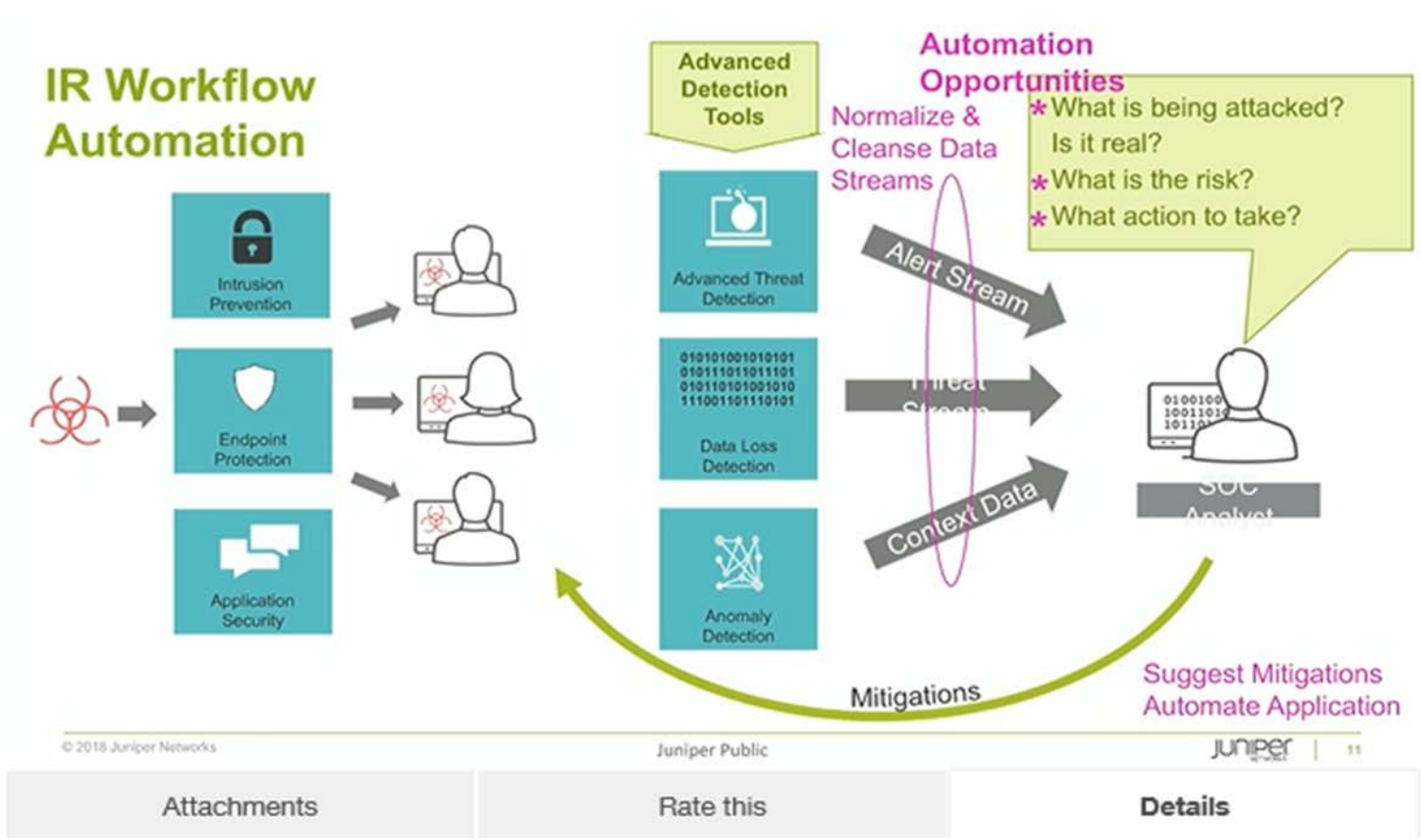
Source: BrigtTalk Website April 2019

Machine learning and Automations



Source: BrigtTalk Website April 2019

Machine learning and Automations



Source: BrigtTalk Website April 2019

Machine learning and Automations

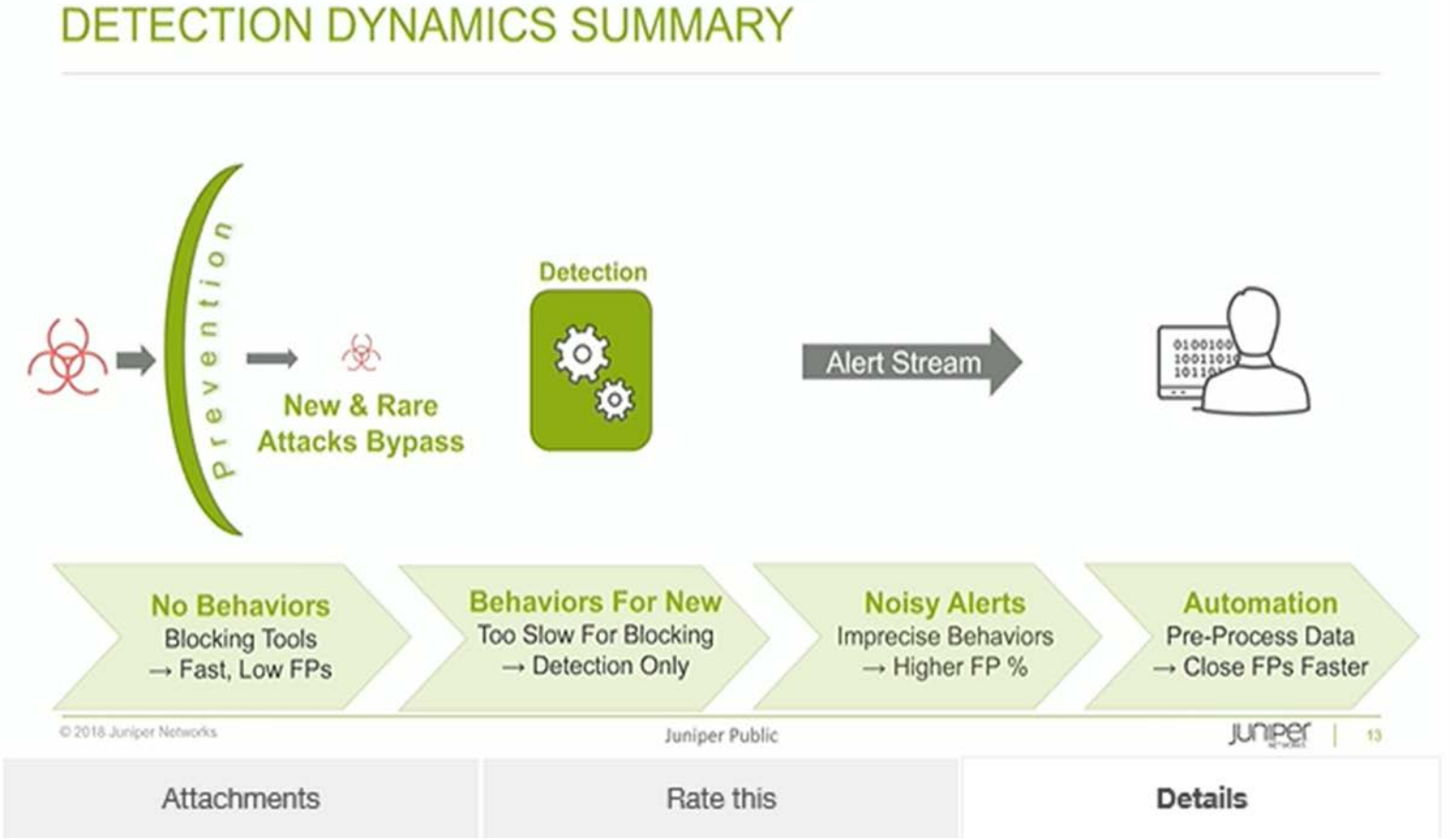
REALIZE IR IMPROVEMENTS THROUGH AUTOMATION

Malware Investigation Tasks	Manual Effort
Identify Host and User	10 min
Collect AV and EDTR data for given host	25 min
Collect network data (NGFW, SWG)	25 min
Analyze & Correlate	35 min
Determine progression and scope	15 min
Contain the threat	10 min
TOTAL TIME	**2 hours**

Search: "Juniper Security Calculator" for interactive version

Source: BrigtTalk Website April 2019

Machine learning and Automations



Source: BrigtTalk Website April 2019

Cyber Security and Resilience

- Recent events have highlighted the risk related to cyber security and this concerns in particular digital protection, automation and control systems

- Overreliance on GPS as a time source can lead to reduced network security and therefore to build resilience for time synchronisation is of vital importance to future digital substation roll out,

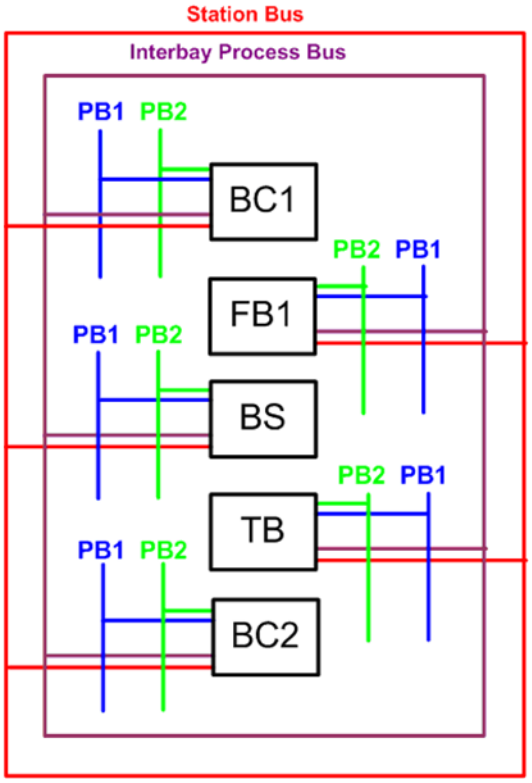
- The behaviour of digital substation solutions in response to abnormal network traffic resulting from equipment failure or unexpected messages from cyber-attack on the process bus or station bus is unknown

This led NG to funded Manchester to carry out the development of Cyber Resilient Electrical Substation Technologies (CREST)

NG AS3, VSATT and SPEN FITNESS

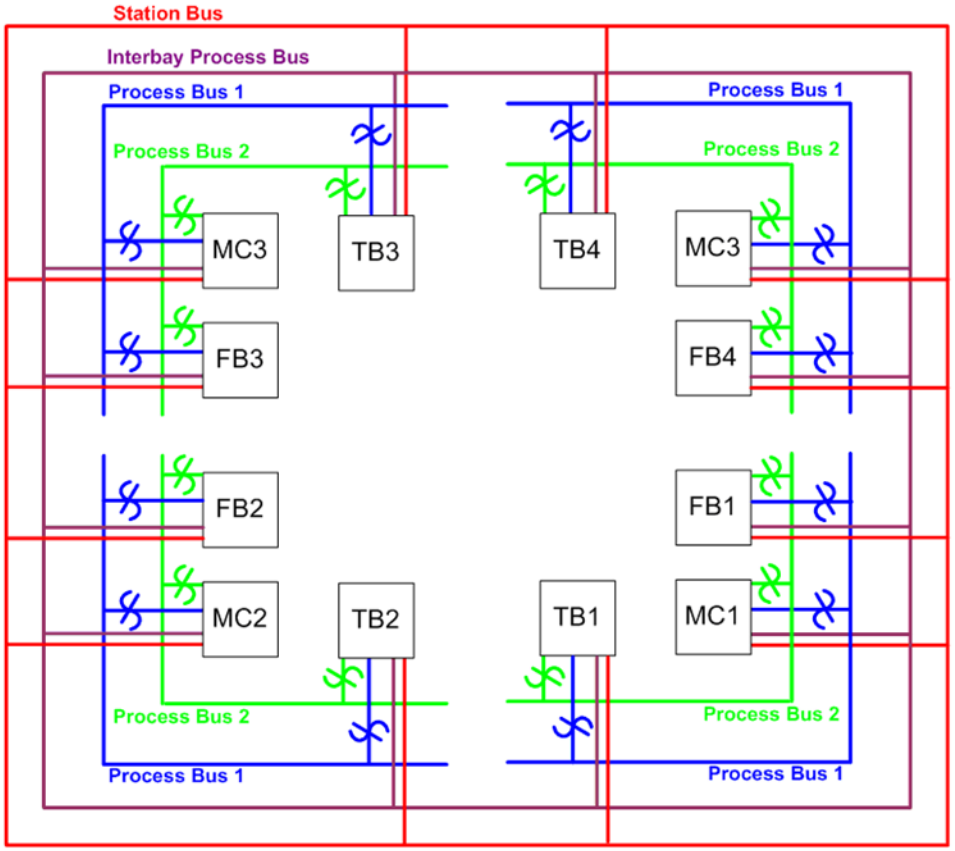
- **AS3 architectures**

Double Busbar



BC: Bus Coupler Bay FB: Feeder Bay
BS: Bus Section Bay PB: Bay Process Bus
TB: Transformer Bay

Mesh Corner



Filter Switch mechanism (Optional) MC: Mesh Corner Bay FB: Feeder Bay TB: Transformer Bay

NG AS3, VSATT and SPEN FITNESS

- **VSATT platform**

(5) Substation Configuration Language (SCL)

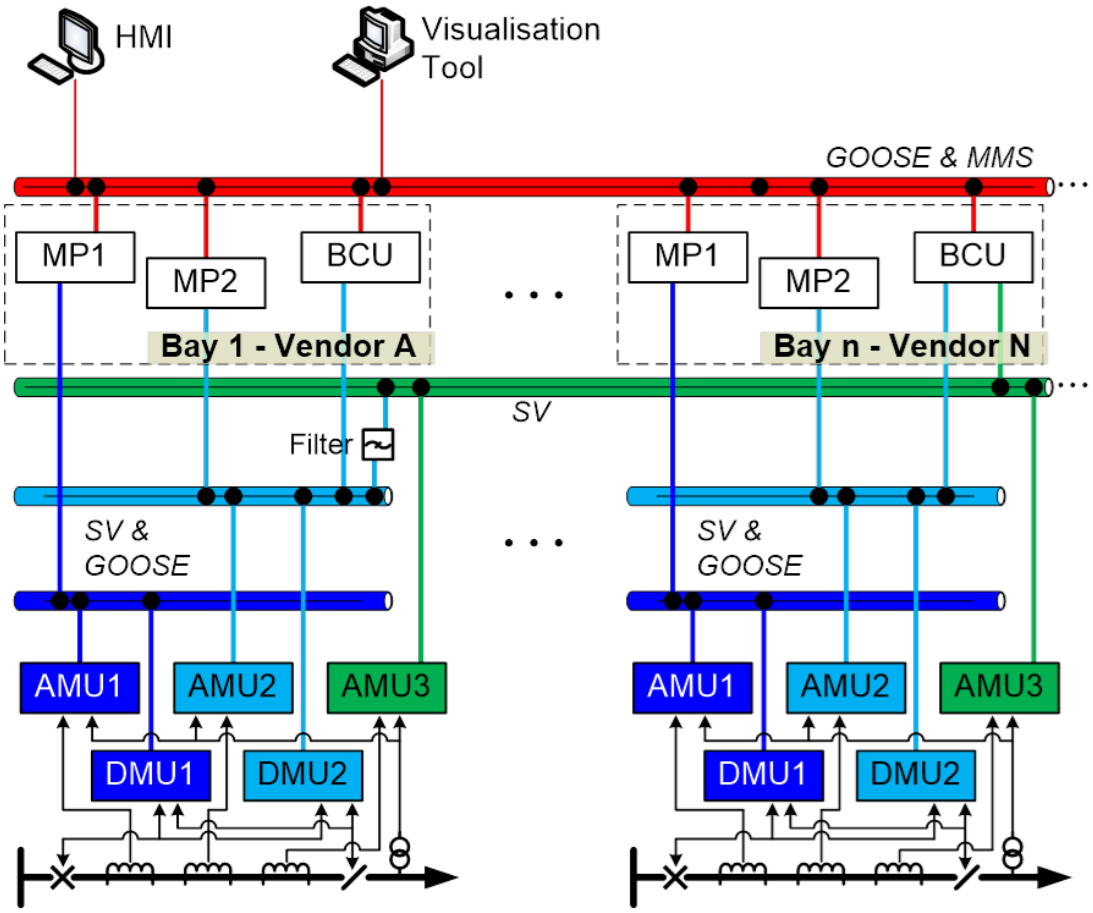
(6) Data flow visualisation

(4) Station Bus (8-1 GOOSE and MMS) based on AS^3 Architecture

(3) Multi-vendor Bay Level – Standard Bay Solutions

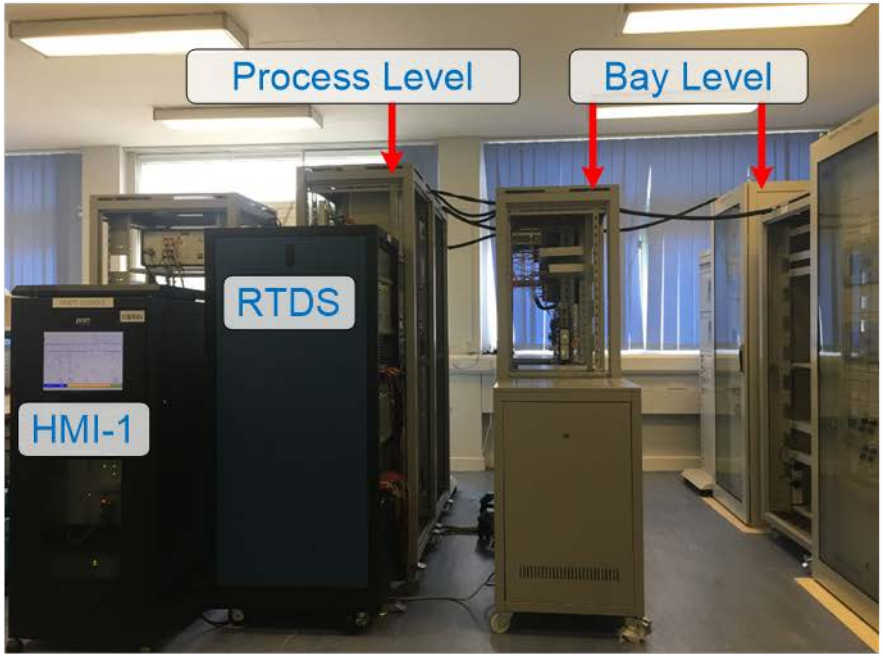
(2) Standard Process Bus Interfaces (9-2LE SV and 8-1 GOOSE) and Inter-bay Process Bus / Measurement Bus (9-2LE SV and high-quality measurements) based on AS^3 Architecture

(1) Virtual Substation Modelling Platform – Real Time Digital Simulator (RTDS)

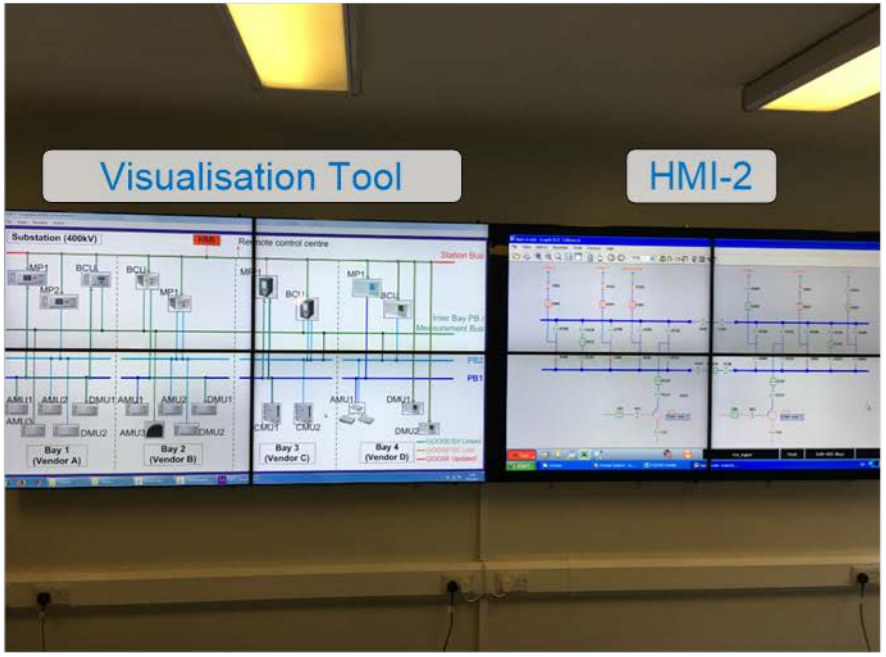


NG AS3, VSATT and SPEN FITNESS

- **VSATT platform in the Manchester Lab**



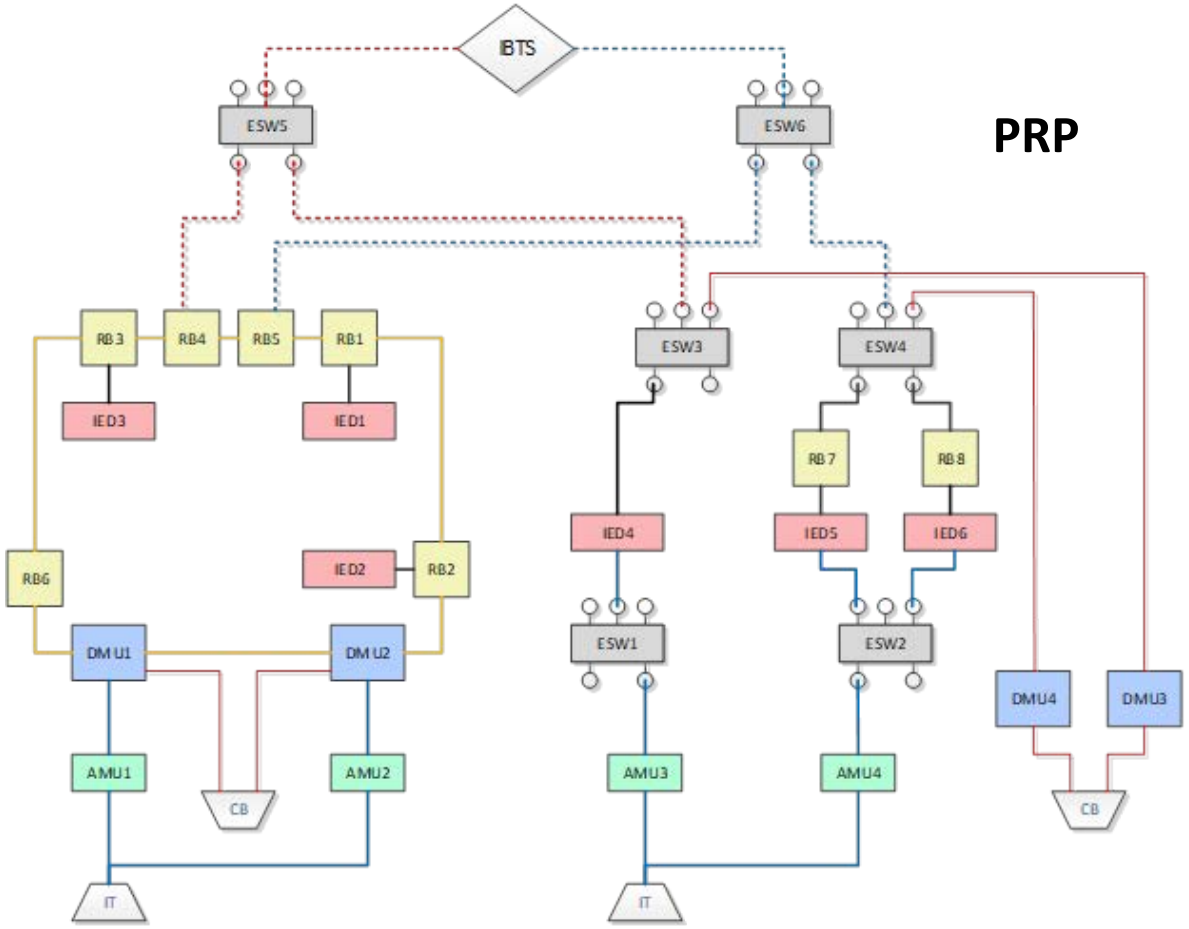
(a) Hardware Platform



(b) Monitoring Tools

NG AS3, VSATT and SPEN FITNESS

- **FITNNESS architecture (simplified diagram)**



CREST Project

AS3 and VSATT platform

- NG AS3 and VSATT projects have demonstrated the viability of implementing digital substation solutions and have validated the interoperability between solutions from several vendors.

CREST project

- However, the increase in cyber risk and concern about the resilience of digital P&C solutions has led to a need to better understand how the IEDs now being used in National Grid substations might be attacked and the extent of their vulnerability. The scope of this project can be divided into the following parts.

CREST Project

Scopes/Methods:

- Review and report on literature, including cyber security issues and new emerging cyber-attack detection/defence technologies in substation protection, automation and control systems,

- Trial different Intrusion Detection Systems (IDS) on the VSATT platform to identify vulnerabilities of AS3 based digital substations,

- Develop and demonstrate ML an AI based cyber intruciton detection, defence and recovery methods for IEC 61850 based substation protection and control schemes.

CREST Project

Scopes/Methods:

- Develop a specification and/or best practice guidance for cyber-resilient digital substation solutions considering in particular how relevant international cyber security standards should be implemented and identify any gaps not currently covered by international standards.

Summary

- **Smart Grids / Digital Grids**
- **Issues, challenges and motivation**
- **Machine learning and automation**
- **Cyber security and resilience requirements**
- **Research efforts and activities since 2003**
  - 2003 – 2007: supervising a PhD project
  - "Modelling and Evaluation of UCA/IEC 61850 Based Utility Communication
  - Management for Power System Monitoring and Control",
  - 2008-2010: Architecture Designs and reliability analysis for NG AS3 project,
  - 2014-2017: Developing Virtual Site Acceptance Testing and Training (VSATT) Platform
  - 2016 – 2020: Lab testing and site data analysis for FITNESS (real life digital substation ,
  - 2019 – 2021: To develop Cyber resilient technologies (CREST) for P&C
- **What is next?**

  This talk is about - Machine learning and AI technologies

Thank You?

Questions?

Dr Haiyu Li (Manchester University)
haiyu.li@manchester.ac.uk
Tel: +44-161-3064694, mob: +44 7775024526