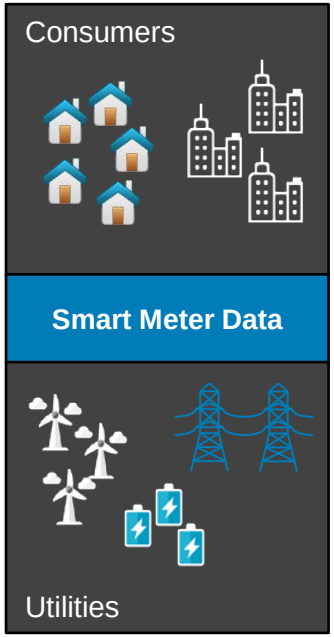
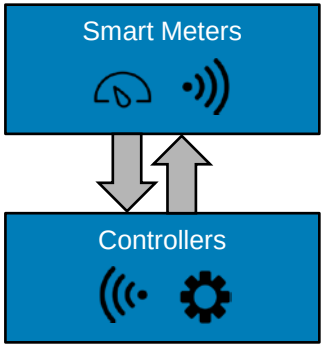
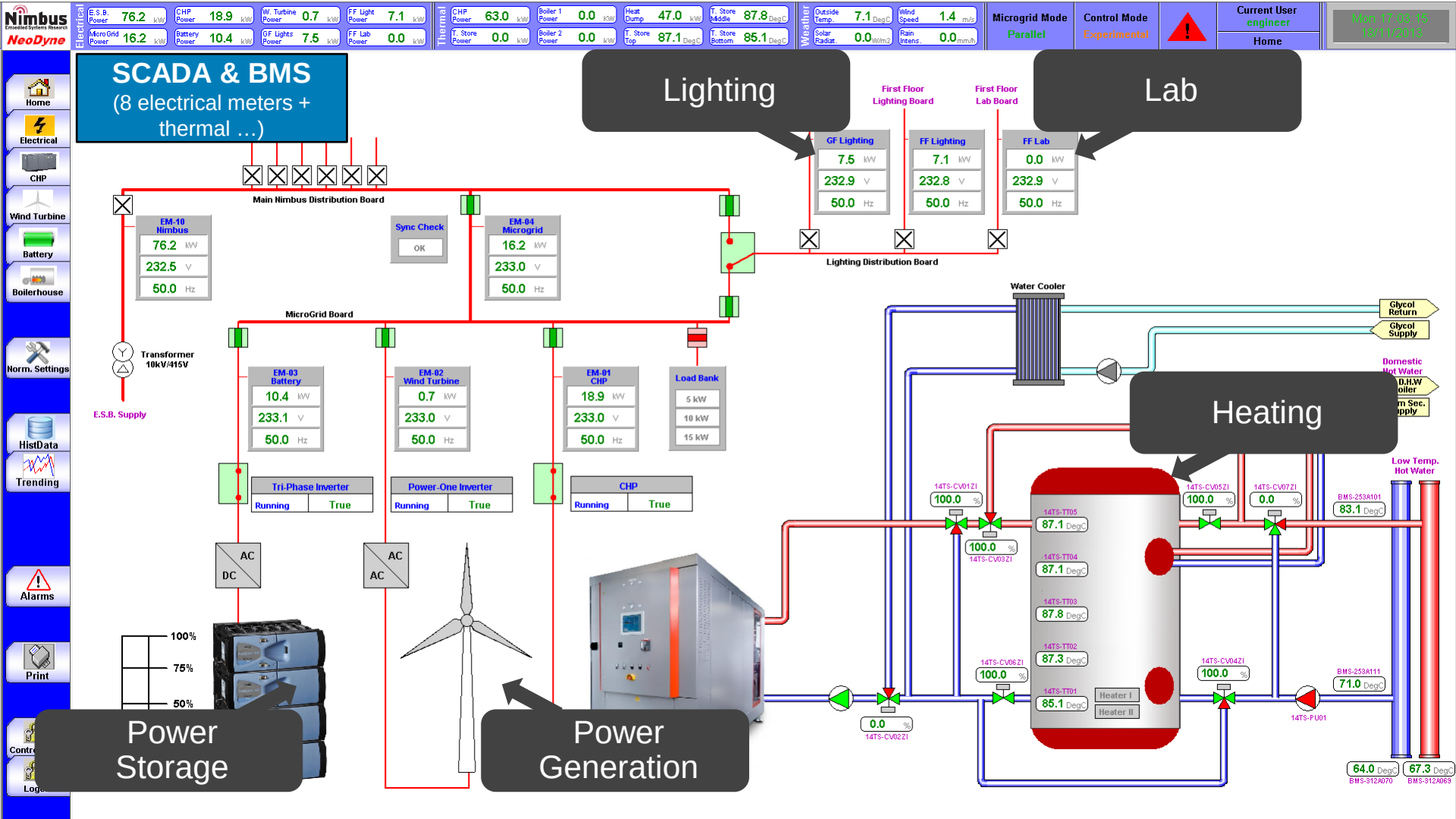

sparks
SMART GRID PROTECTION AGAINST CYBER ATTACKS
Security Analytics
Smart Grid Anomaly Detection
Symposium on Innovative Smart Grid Cybersecurity Solutions, Vienna, Mar 2017
Dr. Niamh O'Mahony, DELL EMC Research Europe, Ireland
DELL EMC

The System

Smart Grid Infrastructure






Nimbus
NeoDyne
Electrical
E.S.B. Power 76.2 kW
CHP Power 18.9 kW
W. Turbine Power 0.7 kW
FF Light Power 7.1 kW
Micro Grid Power 16.2 kW
Battery Power 10.4 kW
GF Lights Power 7.5 kW
FF Lab Power 0.0 kW
Thermal
CHP Power 63.0 kW
Boiler 1 Power 0.0 kW
Heat Dump 47.0 kW
T. Store Middle 87.8 DegC
T. Store Power 0.0 kW
Boiler 2 Power 0.0 kW
T. Store Top 87.1 DegC
T. Store Bottom 85.1 DegC
Weather
Outside Temp. 7.1 DegC
Wind Speed 1.4 m/s
Solar Radiat. 0.0 kW/m2
Rain Intens. 0.0 mm/h
Microgrid Mode
Parallel
Control Mode
Experimental
Current User
engineer
Home
Mon 11.03.15
19/11/2013
Home
Electrical
CHP
Wind Turbine
Battery
Boilerhouse
Norm. Settings
HistData
Trending
Alarms
Print
SCADA & BMS
(8 electrical meters + thermal …)
Lighting
Lab
First Floor Lighting Board
First Floor Lab Board
GF Lighting
7.5 kW
232.9 V
50.0 Hz
FF Lighting
7.1 kW
232.8 V
50.0 Hz
FF Lab
0.0 kW
232.9 V
50.0 Hz
Main Nimbus Distribution Board
EM-10 Nimbus
76.2 kW
232.5 V
50.0 Hz
Sync Check
OK
EM-04 Microgrid
16.2 kW
233.0 V
50.0 Hz
Lighting Distribution Board
MicroGrid Board
Transformer 10kV/415V
E.S.B. Supply
EM-03 Battery
10.4 kW
233.1 V
50.0 Hz
EM-02 Wind Turbine
0.7 kW
233.0 V
50.0 Hz
EM-01 CHP
18.9 kW
233.0 V
50.0 Hz
Load Bank
5 kW
10 kW
15 kW
Tri-Phase Inverter
Running True
Power-One Inverter
Running True
CHP
Running True
AC DC
AC AC
100%
75%
50%
Water Cooler
Glycol Return
Glycol Supply
Domestic Hot Water
Heating
Low Temp. Hot Water
14TS-CV01ZI 100.0 %
14TS-CV03ZI 100.0 %
14TS-CV05ZI 100.0 %
14TS-CV07ZI 0.0 %
BMS-253A101 83.1 DegC
14TS-TT05 87.1 DegC
14TS-TT04 87.1 DegC
14TS-TT03 87.8 DegC
14TS-TT02 87.3 DegC
14TS-TT01 85.1 DegC
Heater I
Heater II
14TS-CV06ZI 100.0 %
14TS-CV04ZI 100.0 %
14TS-CV02ZI 0.0 %
14TS-PU01
BMS-253A111 71.0 DegC
64.0 DegC BMS-312A070
67.3 DegC BMS-312A069
Power Storage
Power Generation

The Attacker

Attack Objectives

Damage Equipment

Disrupt Service

Increase Costs

EU FP7 Programme Contract No. 608224

Attack Objectives

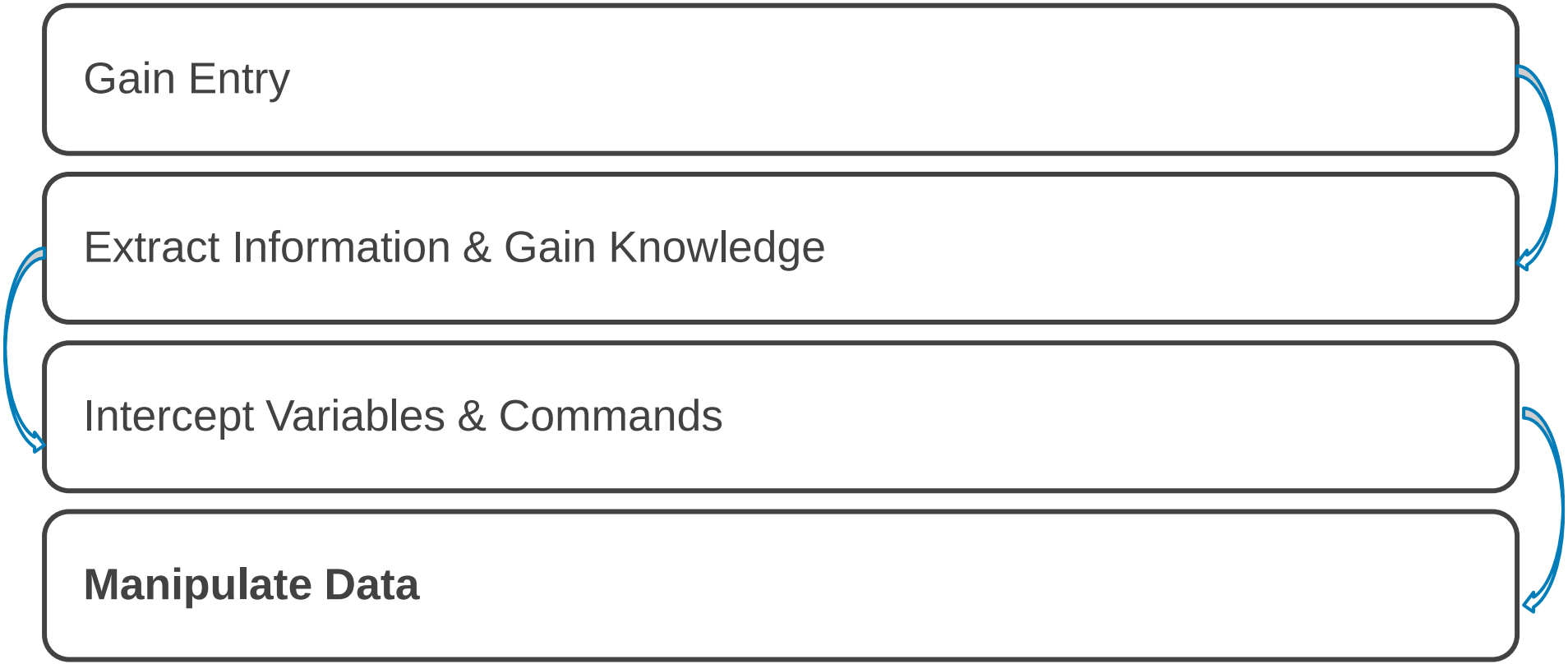
Damage Equipment

Disrupt Service

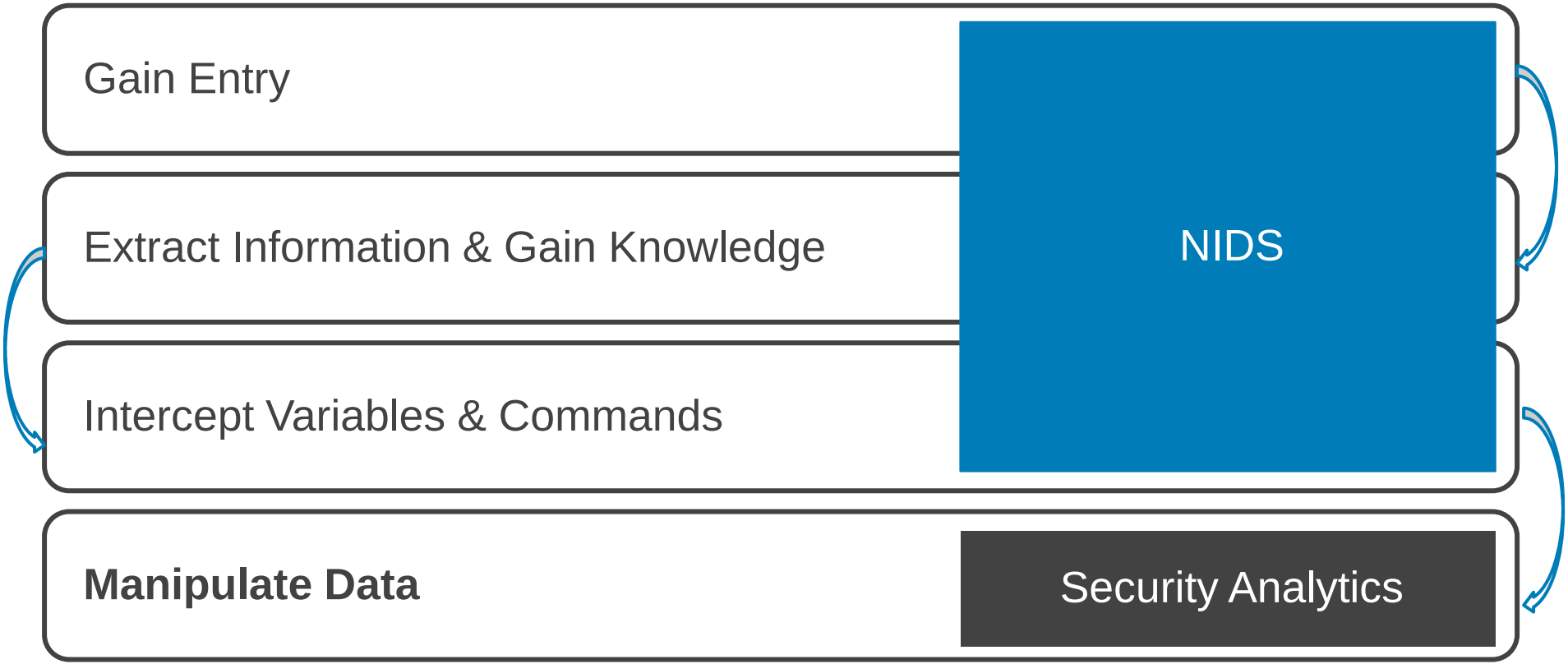
Increase Costs

MAXIMISE IMPACT

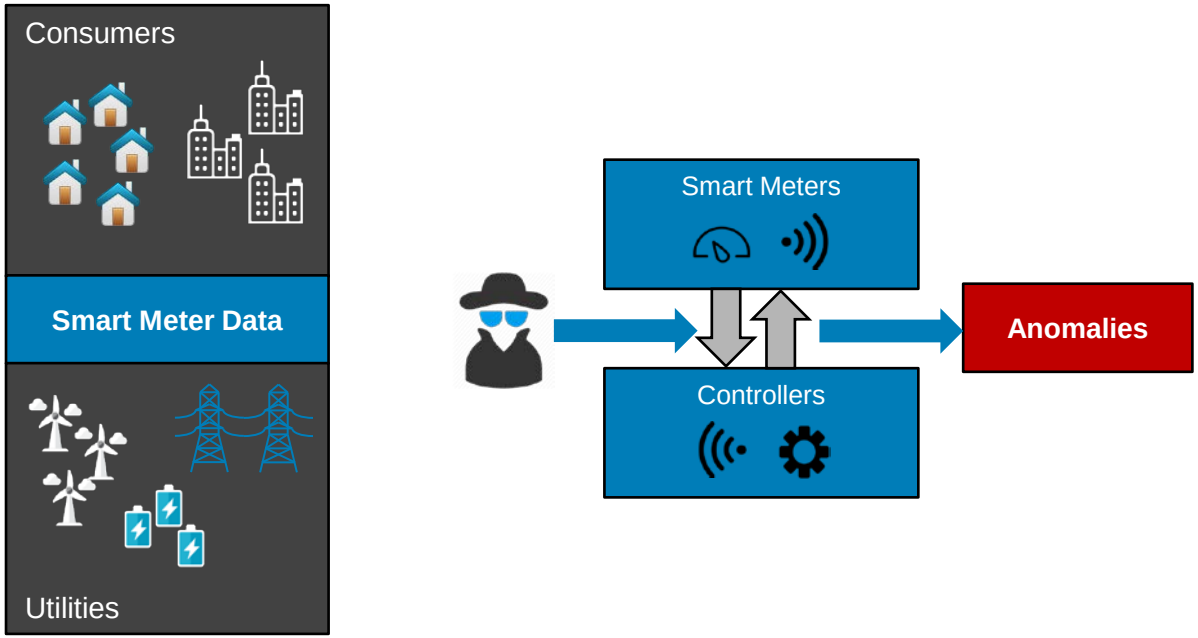
Attack Flow



Attack Flow



“Man-in-the-middle” attacks

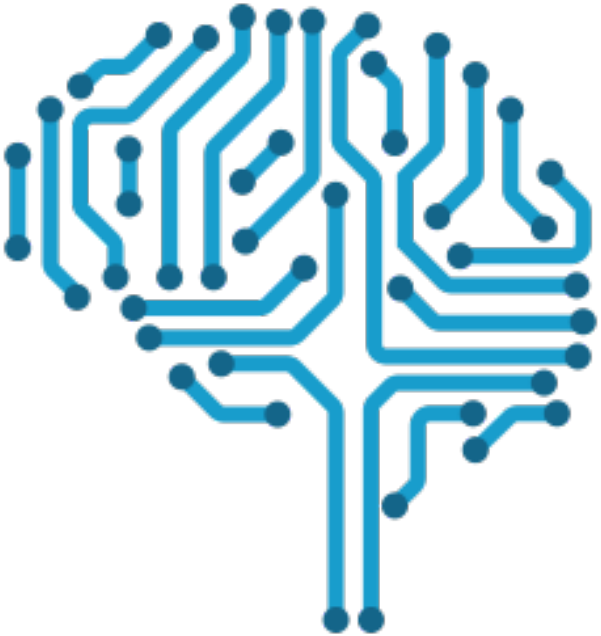


The Solution

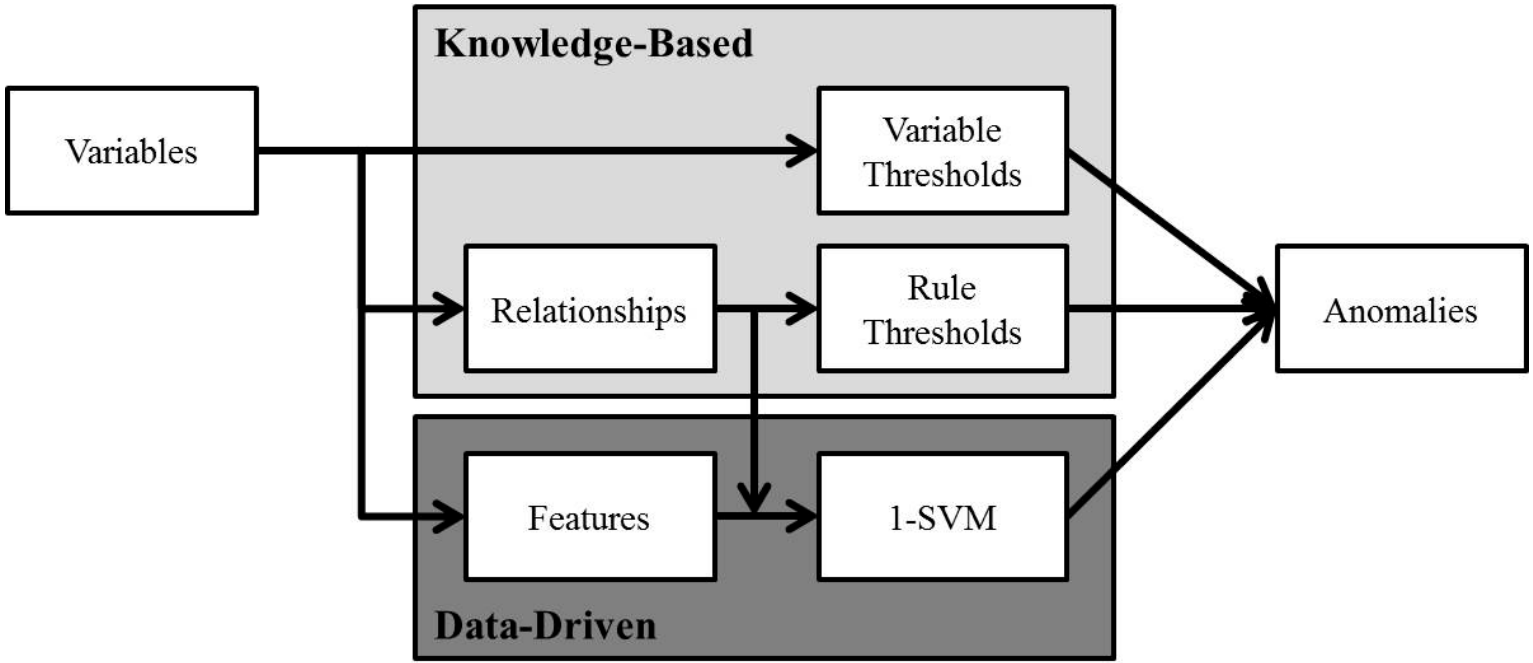
Knowledge-Based Anomaly Detection

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Data-Driven Anomaly Detection



SPARKS Security Analytics



DELL EMC

Detecting SVM anomalies

Data Directory:

BMSdata

File to analyze:

Day/BMS20160208.csv

Plot length (hours):

1 6 23

1 4 7 10 13 16 19 2223

Update Rate (mins/sec):

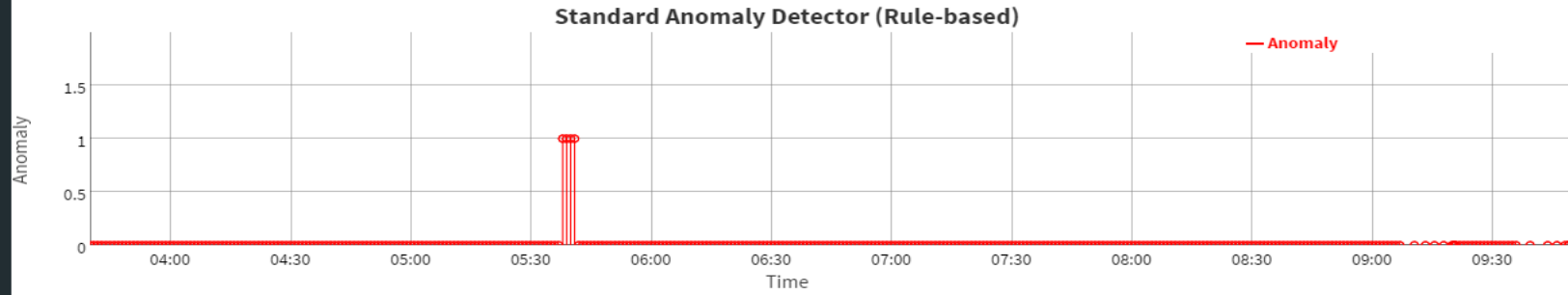
10 20 60

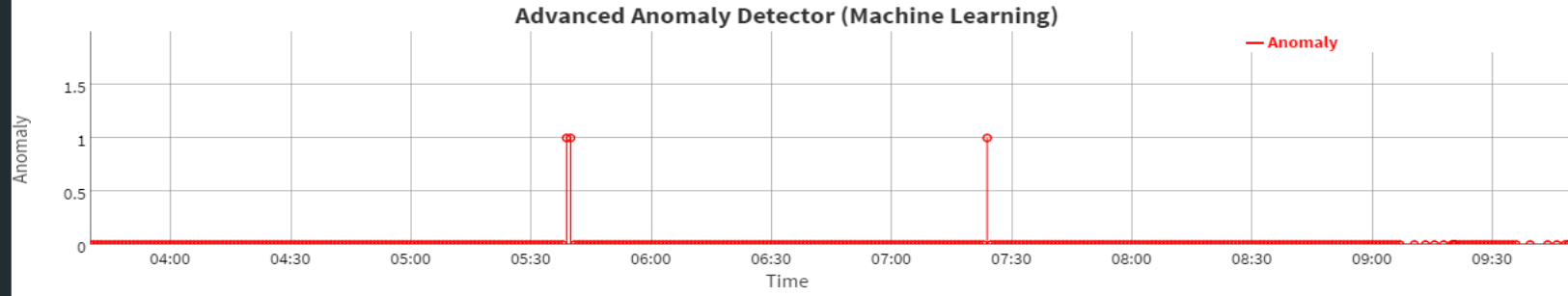
10 20 30 40 50 60

Run Analysis

Summary | Schematic | Sensor Data | Rules

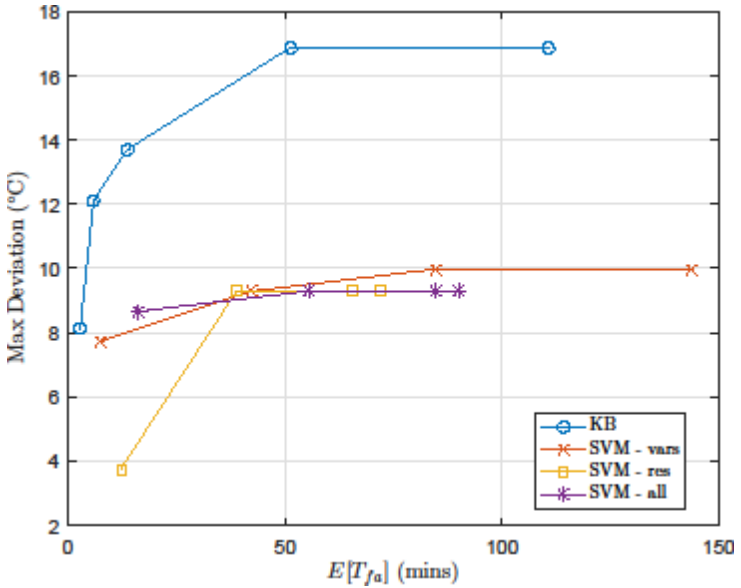
# METERS	SVM ANOMALIES	KB ANOMALIES	MISSING SAMPLES
15	3	4	1.76 %





Performance (Simulation)

- Sensitivity:
  - *Maximum deviation that can be achieved by attacker without detection*
- Usability:
  - *Expected time to false alarm*
- SVM detectors outperform KB
  - lower max dev for same $E[T_{fa}]$




DELL EMC


sparks
SMART GRID PROTECTION AGAINST CYBER ATTACKS