SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust
Centre for Research in Cyber Security

Electric Power and Intelligent Control (EPIC) Testbed

Version: 1.2
Last updated: 23 October 2018
Contact information: itrust@sutd.edu.sg
Website: https://itrust.sutd.edu.sg/

INTRODUCTION

Aim

This documentation provides readers with an in-depth understanding of how the Electric Power and Intelligent Control (EPIC) testbed works, the capabilities it is equipped with as a platform for **research and experimentation, education and training and testing.** Included in this document also are the technical details relating to the operation, components, drawings, equipment list and control and communication network of EPIC.

Background

Electric Power and Intelligent Control (EPIC) is a power grid testbed comprising of four stages of Generation, Transmission, Micro-grid, and Smart Home. Operational since 22 May 2017, EPIC is designed to enable cyber security researchers to conduct experiments to assess the effectiveness of novel cyber defence mechanisms. EPIC is one of the three critical infrastructure testbeds at iTrust that researchers in cyber security leverage on for applied research. The other two testbeds are SWaT and WADI, which simulate water treatment and distribution processes, respectively.

Research and Experimentation

Notable aspects of the testbeds include segmented communications networks, wired and wireless communications, distributed dynamic control, interconnection among the testbeds, and complete access to the control logic inside the PLCs and HMIs. Access to them allows researchers to develop their own code and upload it in the controllers for research and experimentation. It also allows them to demonstrate their technologies in a **safe, controlled and realistic environment.**

Our **EPIC dataset** was collected under 12 different scenarios in normal operation. During the data collection, all network traffic, sensor and actuator data were collected. The dataset (available upon request) is highly sought after, with requests from more than 150 researchers from over 30 countries.

Education and Training

EPIC is being used by students from SUTD's Master of Science Security by Design (MSSD) programme as an **education and training platform** to cement and bring to life concepts introduced in the classroom. It is also offered to organisations in training their **operational technology (OT) personnel** in cyber incidents.

PROCESS AND SYSTEM OVERVIEW

Each of the four stages of EPIC has its own switches, programmable logic controllers (PLCs), power supply unit, protection and communication systems in a fiber optic ring network. WAGO PLCs control the opening/closing of breakers and contain the synchronisation logic for the generators. High-availability Seamless Redundancy and Media Redundancy Protocol (MRP) switches are used in the ring network for redundancy. EPIC observes the IEC 61850 communication protocol for the electrical substation and automation system. Generic Object Oriented Substation Event (GOOSE) and Manufacturing Message Specification (MMS) are used in the ring network for data transfer between relays and the SCADA workstation. EPIC's network and control architecture is show in Figure 1 and 2.

The **Generation** stage consists of a power source from SUTD's grid and three generators. The three generators are rated at 10KW each and provide a total of 30KW of maximum power. At the **Transmission** stage, an autotransformer is used to step up or step down the voltage to the smart home or micro-grid. Smart home consists of two load banks, 15 and 30kVA, with programmable variable resistive, inductive and capacitive loads. The **Micro-grid** consists of photovoltaic cells (PV) and batteries. Breaker interlocks are implemented between transmission, smart home and micro-grid to prevent clash in the voltages and frequency of the system. **Smart meters** with Advanced Metering Infrastructure (AMI) to obtain readings of voltages, current, power factor and power consumption, are installed at several locations throughout EPIC grid. These meters enable the measurement of energy in kWh at the generators, PV, and the autotransformer. Readings from individual meters can be viewed via a web-based workstation that stores data mentioned above and provides a graphical visualisation.

Communications in EPIC are divided into five portions: Generation, Transmission, Micro-Grid, Smart Home and Controls. A total of 110 PV cells are installed on the rooftop with inverters to convert solar energy to electrical energy and feed it into the testbed. The cells provide a total of 34 KW of maximum power. A battery bank with inverters supplements power supply to EPIC in the event of a blackout or low energy conversion owing to cloud cover. Backup-power to the SCADA workstation is available from a separate battery bank is also implemented to enable network communications to continue in the event of a total blackout.

On demand, EPIC supplies power to run both SWaT and WADI testbeds concurrently. This connection is useful for research into the cascading effects of cyber attacks of a power plant to downstream infrastructure. EPIC supports experimental investigation into the cyber security aspects of the distributed cyber components controlling the physical components such as generators and transformers.

A screenshot of the HMI from SCADA workstation is shown in Figure 3.

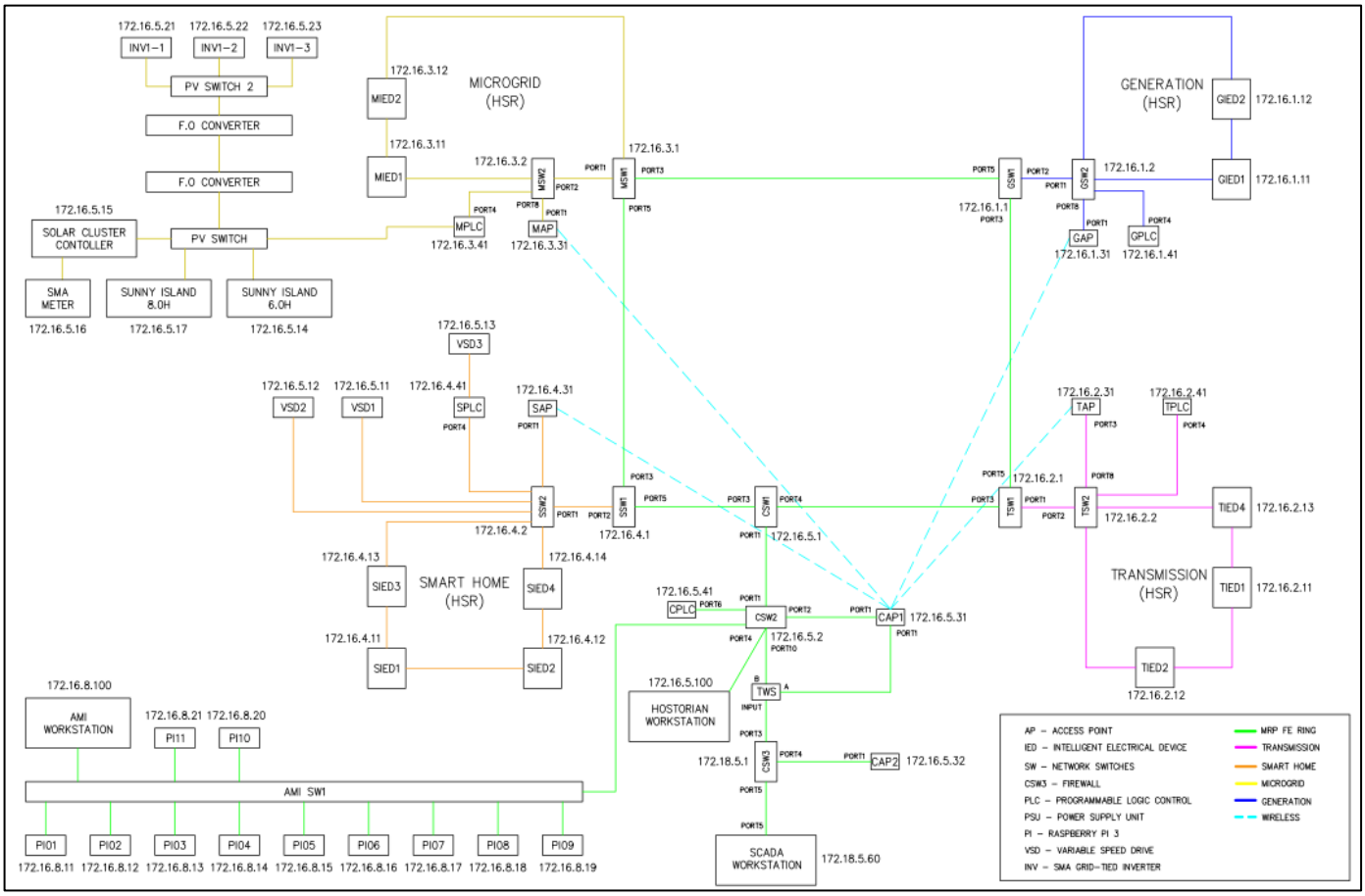

Figure 1: EPIC Network Architecture

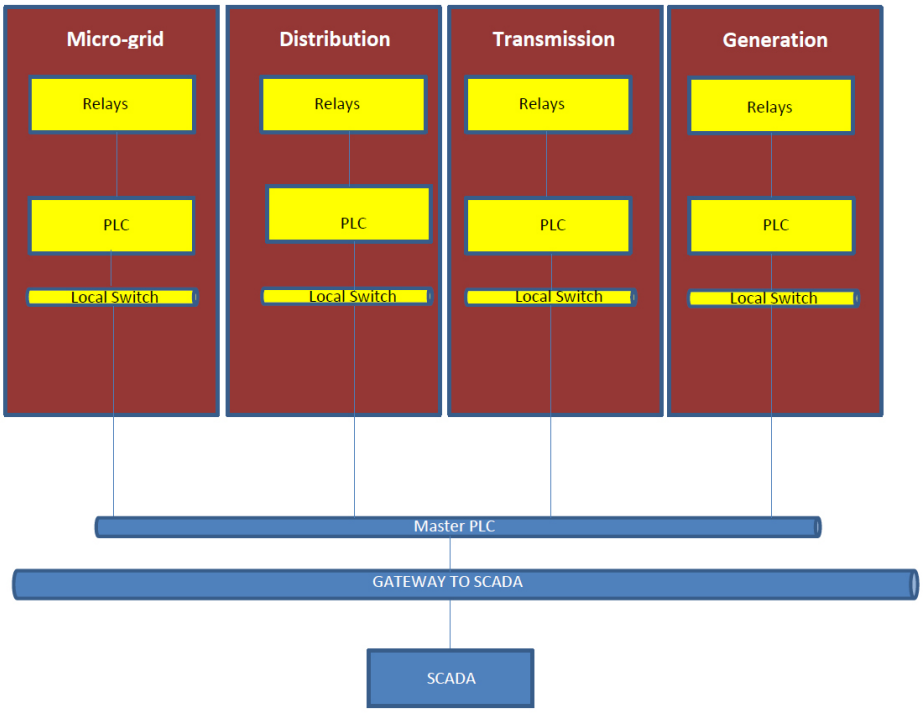

Figure 2: EPIC Control Architecture

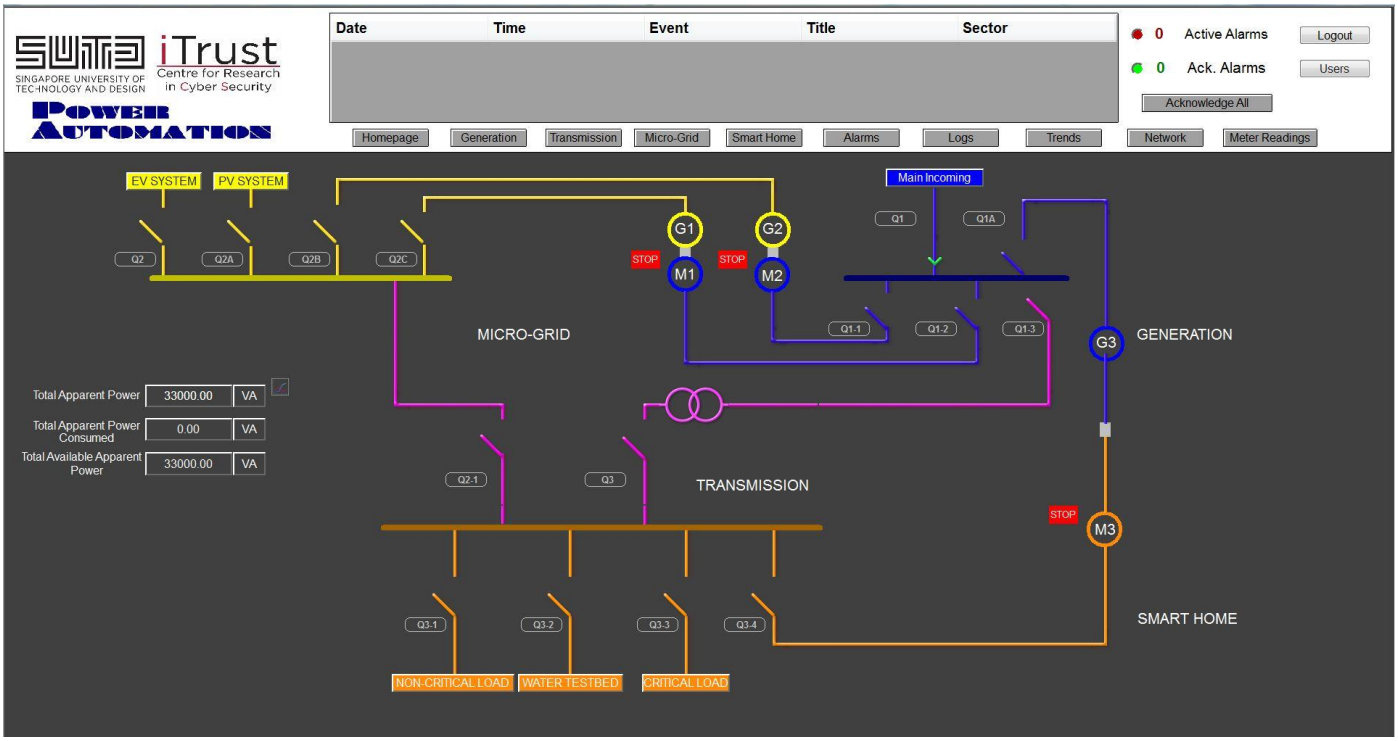

Figure 3: HMI/SCADA screenshot

COMPONENTS (SENSORS)

The following sensor readings are captured and displayed in the protection relay (IED) and AMI faceplates, as shown in Figure 4:

- Line Voltage (measured in V)
- Line Current (A)
- Total Apparent Power (VA)
- Total Real Power (W) and Reactive Power (VAr)
- Frequency (Hz)
- Active Energy (Kwh)
- Power Factor

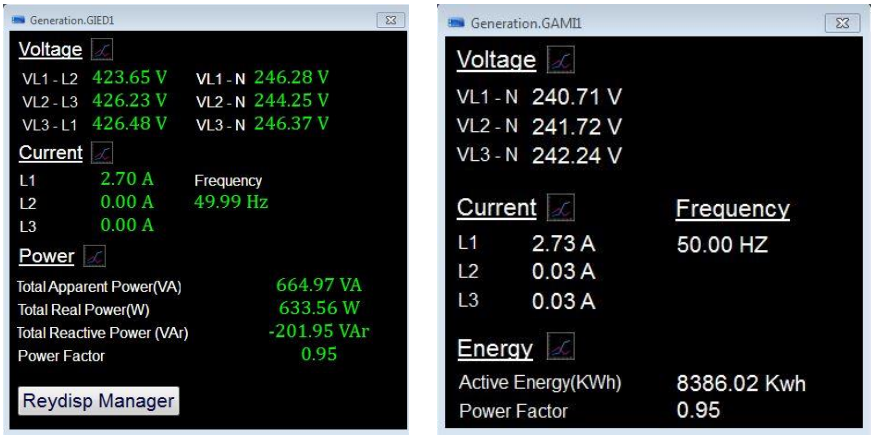

Figure 4: Sensor readings shown in Protection Relay (IED; left) and AMI (right) faceplates

EQUIPMENT

Table 1: Equipment list for EPIC

No.	Item Designation	Brand	Model Number
1	Smart Meters	Wasion	DTZ341 aMeter300
2	Reyrolle Relays	Siemens	7SR1205-2JA87-1CA0/EE
3	Earth Leakage Relay	MH	EL10
4	Circuit Breaker	ABB	DS SACE Tmax XT
5	Access Point	Hirschmann	BAT-R
6	Firewall		EAGLE 30
7	Network Switches		RSL
8	16 Channel Digital Input Module	WAGO	750-1405
9	16 Channel Digital Output Module		750-1504
10	PLC-Controller w 24v input module		750-8202/025-001
11	End Module		750-600
12	Power Supply		787-1622
13	Serial Interface		750-652
14	AET Auto-Transformer	AET	VR105KVA-400V-5-4W/FS-1
15	Batteries Inverters	SMA Solar Technology	S18.0H-11
16	Battery Inverters		S16.0H-11
17	SMA Cluster Controller		CLCON-10
18	SMA Remote Controller		SRC-20
19	Generator	MarelliMotori	MJB 160 XA4
20	SEW VSD	SEW-EURODRIVE	8227136
21	SEW Motor		DRS160MC4/FI/TF/EG7S
22	3.5KW Braking Resistors		BW18-035
23	7.5KW Braking Resistors		BW18-075
24	15KVA Programmable Loadbank	Hebei Kaixiang Electrical Technology	AC400-15KVA-RLC
25	30KVA Programmable Loadbank		AC400-30KVA-RLC
26	1,956mm * 988mm PV panels	Hanwha	SOLAR ONE HSL 72P6-PC-1-310E POLYCRYSTALLINE
27	SMA INVERTER TP10000TL	SMA Solar Technology	SUNNY TRIPOWER 1000TL
28	Fibre Booster	KEYLAN	MCSMLCSFF20
29	KVM Switch	Aten	CS64US
30	Switch 1	HP	HPE 1410-16SWITCH (J9662A)
31	Router 2	SANGOMA	FreePBX Phone System 50
32	Router 1	TP-LINK	TL-WR841N
33	Router 3		8PORT Gigabit Desktop Switch
34	Hydrogen Sensor Display	KELE	LPI-4
35	Toxic & Combustible Gas Detector		GDS SERIES
36	SMA Energy Meter	SMA Solar Technology	EMETER-10

NETWORK PROTOCOL AND MONITORING

Network Protocol

The system has two main protocols in place which allow the communication of data between IED, PLC and SCADA workstation: Manufacturing Message Specification (MMS), a request/response protocol, and Generic Object Oriented Substation Event (GOOSE), a multicast publisher-subscriber protocol. They are part of IEC 61850 protocol suite. The PLCs communicate with the IEDs and SCADA workstation using MMS; the IEDs communicate with each other via GOOSE.

Modbus TCP is used in between VSDs and PLCs as well as between Raspberry Pis to SCADA workstations. Raspberry Pis communicate with energy meters using IEC 62056 Protocol and translate and broadcast the meter data information to Modbus TCP.

IP ADDRESS

The IP addresses of EPIC network are shown below in Table 2.

Table 2: IP Addresses of EPIC network

Hirschmann Switch			
Description	IP Address	Gateway	Class
GSW1	172.16.1.1	172.16.6.1	255.255.0.0
GSW2	172.16.1.2	172.16.6.1	255.255.0.0
TSW1	172.16.2.1	172.16.6.1	255.255.0.0
TSW2	172.16.2.2	172.16.6.1	255.255.0.0
MSW1	172.16.3.1	172.16.6.1	255.255.0.0
MSW2	172.16.3.2	172.16.6.1	255.255.0.0
SSW1	172.16.4.1	172.16.6.1	255.255.0.0
SSW2	172.16.4.2	172.16.6.1	255.255.0.0
CSW1	172.16.5.1	172.16.6.1	255.255.0.0
CSW2	172.16.5.2	172.16.6.1	255.255.0.0
CSW3 (Firewall)	172.18.5.1	0.0.0.0	255.255.0.0

Protection Relay (IED)			
Description	IP Address	Gateway	Class
GIED1	172.16.1.11	172.16.6.1	255.255.0.0
GIED2	172.16.1.12	172.16.6.1	255.255.0.0
TIED1	172.16.2.11	172.16.6.1	255.255.0.0
TIED2	172.16.2.12	172.16.6.1	255.255.0.0
TIED4	172.16.2.13	172.16.6.1	255.255.0.0
MIED1	172.16.3.11	172.16.6.1	255.255.0.0
MIED2	172.16.3.12	172.16.6.1	255.255.0.0
SIED1	172.16.4.11	172.16.6.1	255.255.0.0

SIED2	172.16.4.12	172.16.6.1	255.255.0.0
SIED3	172.16.4.13	172.16.6.1	255.255.0.0
SIED4	172.16.4.14	172.16.6.1	255.255.0.0

WAGO PLC			
Description	IP Address	Gateway	Class
GPLC	172.16.1.41	172.16.6.1	255.255.0.0
TPLC	172.16.2.41	172.16.6.1	255.255.0.0
MPLC	172.16.3.41	172.16.6.1	255.255.0.0
SPLC	172.16.4.41	172.16.6.1	255.255.0.0
CPLC	172.16.5.41	172.16.6.1	255.255.0.0

Hirschmann Access Point (AP)			
Description	IP Address	Gateway	Class
GAP	172.16.1.31	172.16.6.1	255.255.0.0
TAP	172.16.2.31	172.16.6.1	255.255.0.0
MAP	172.16.3.31	172.16.6.1	255.255.0.0
SAP	172.16.4.31	172.16.6.1	255.255.0.0
CAP1	172.16.5.31	172.16.6.1	255.255.0.0
CAP2	172.16.5.32	172.16.6.1	255.255.0.0

Variable Speed Drive (VSD)			
Description	IP Address	Gateway	Class
VSD1	172.16.5.11	172.16.6.1	255.255.0.0
VSD2	172.16.5.12	172.16.6.1	255.255.0.0
VSD3	172.16.5.13	172.16.6.1	255.255.0.0

Work Station			
Description	IP Address	Gateway	Class
SCADA Workstation	172.18.5.60	172.18.5.1	255.255.0.0
Histroian Workstation	172.16.5.100	172.16.6.1	255.255.0.0
AMI Workstation	172.16.8.100	172.16.6.1	255.255.0.0

Solar PV System			
Description	IP Address	Gateway	Class
Sunny Island 8.0H (3 Phase)	172.16.5.17	172.16.6.1	255.255.0.0
Sunny Island 6.0H (1 Phase)	172.16.5.14	172.16.6.1	255.255.0.0
Solar Cluster Controller	172.16.5.15	172.16.6.1	255.255.0.0
SMA Energy Meter	172.16.5.16	172.16.6.1	255.255.0.0
Tripower (305034675)	172.16.5.22	172.16.6.1	255.255.0.0
Tripower (305034729)	172.16.5.23	172.16.6.1	255.255.0.0
Tripower (305035008)	172.16.5.21	172.16.6.1	255.255.0.0

AMI System			
Description	Ip Address	Gatway IP	Class
PI1	172.16.8.11	172.16.6.1	255.255.0.0
PI2	172.16.8.12	172.16.6.1	255.255.0.0
PI3	172.16.8.13	172.16.6.1	255.255.0.0
PI4	172.16.8.14	172.16.6.1	255.255.0.0
PI5	172.16.8.15	172.16.6.1	255.255.0.0
PI6	172.16.8.16	172.16.6.1	255.255.0.0
PI7	172.16.8.17	172.16.6.1	255.255.0.0
PI8	172.16.8.18	172.16.6.1	255.255.0.0
PI9	172.16.8.19	172.16.6.1	255.255.0.0
PI10	172.16.8.20	172.16.6.1	255.255.0.0
PI11	172.16.8.21	172.16.6.1	255.255.0.0
AMI SW1	172.16.8.1	172.16.6.1	255.255.0.0

Auto-Transformer	
Baud Rate	19200
Parity	Even
Data bits	8
Stop bits	1
Slave Address	1

30KVA Loadbank	
Baud Rate	9600
Parity	None
Data Bits	8
Stop Bits	1
Slave Address	1 or 2

15KVA Loadbank	
Baud Rate	9600
Parity	None
Data Bits	8
Stop Bits	1
Slave Address	1 or 2


iTrust
Centre for Research
in Cyber Security