# TNB M10x – In-House Developed Tool for Learning IEC 60870-5-101/104 SCADA Communication Protocols

Azlan Muhamad Sufian, Ir. Ts. Affiezal Adnan

TENAGA NASIONAL
Better. Brighter.

ILSAS
TNB INTEGRATED LEARNING SOLUTION

ICLAD
ILSAS Conference on Learning & Development 2019

# Author’s Profile

- Azlan Muhamad Sufian
- Principal Engineer (SCADA), Grid Solution Expertise, Grid Division

# Author’s Profile

- Ir. Ts. Affiezal bin Adnan
- Training Engineer (Protection- Grid), TNB Integrated Learning Solution Sdn. Bhd. - ILSAS

# Background on SCADA System, IEC-101 & IEC-104

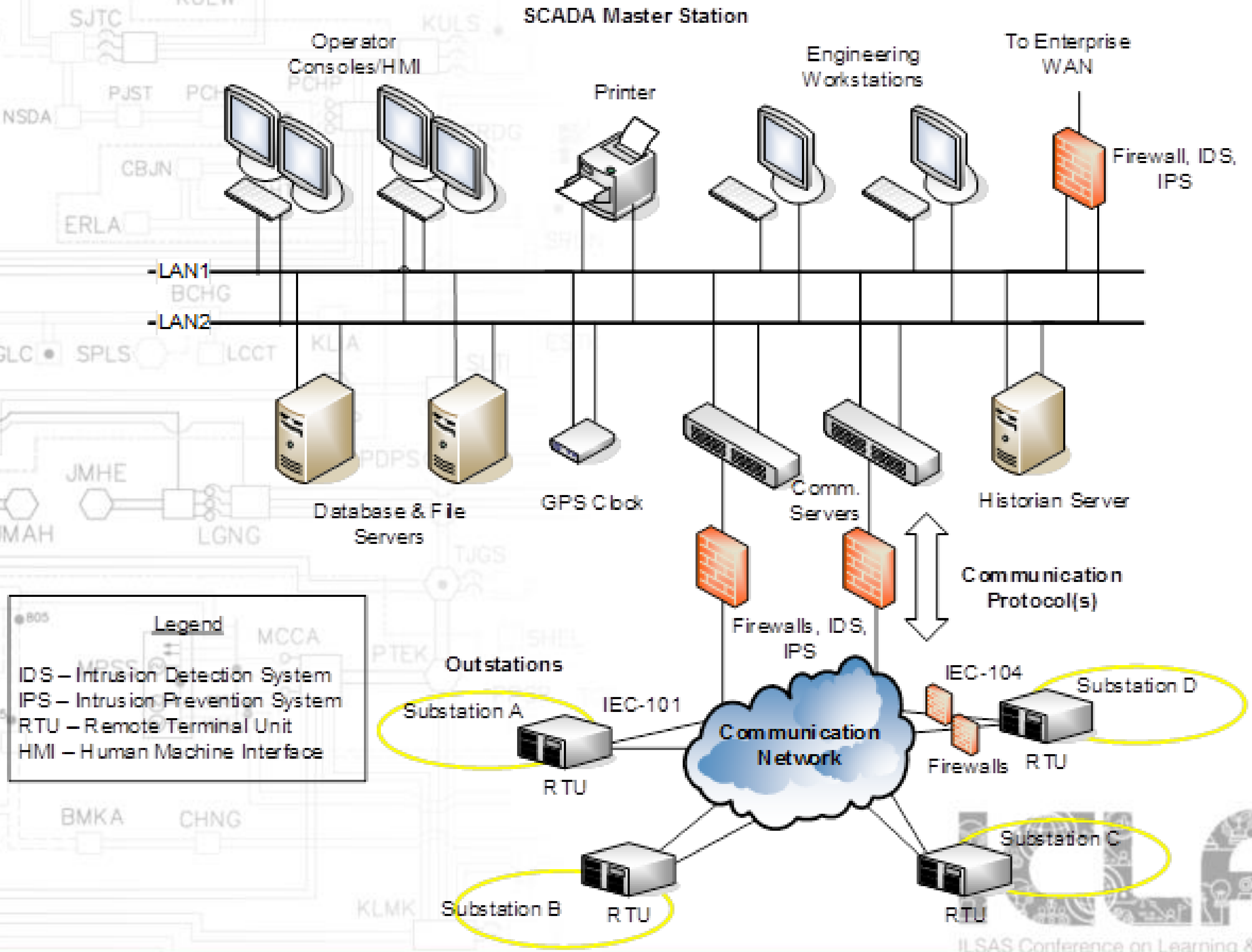
ICLAD

ILSAS Conference on Learning & Development 2019

# Introduction to SCADA System

- SCADA = **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition
- Used to monitor and control remote substations within Peninsular Malaysia National Grid (500kV, 275kV, 132kV, 33kV, 22kV, 11kV substations)
- 3 Main Components
  - Master Station (NLDC, NERCC, MSRCC)
  - Communication Media
  - Remote Terminal Unit (RTU)

# Typical SCADA System Architecture



Legend

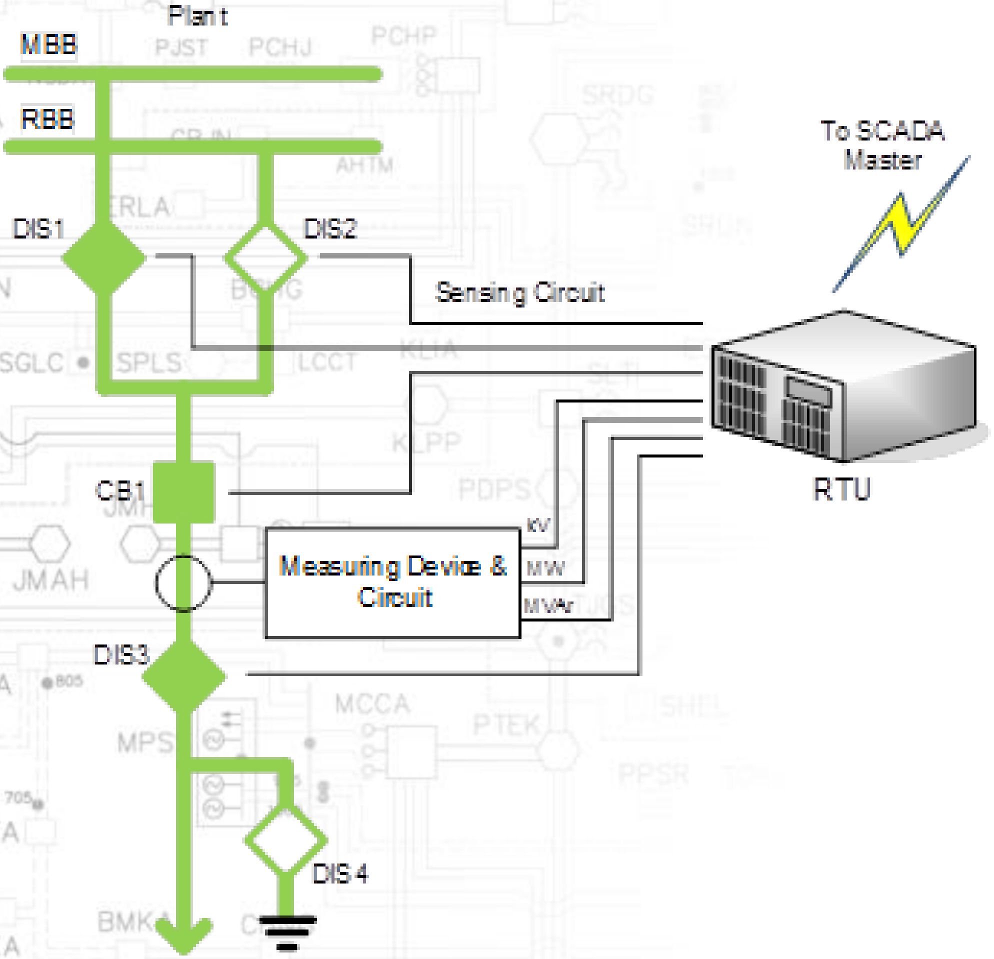
IDS – Intrusion Detection System
IPS – Intrusion Prevention System
RTU – Remote Terminal Unit
HMI – Human Machine Interface

ILSAS Conference on Learning & Development 2019

# SCADA Functions

- Enable Power System Grid Operators (NLDC, NERCC & MSRCC) to
  - Monitor plant status, measurements (Power, Voltage, Current etc.)
  - Operate High Voltage apparatus (Plant Equipment) remotely (Trip and Close Circuit Breakers)
  - Supervise equipment condition by monitoring critical alarms and escalate to maintenance crew

# RTU Interfacing to Plant Equipment



***"RTU is the eyes, ears and hands of the SCADA system"***

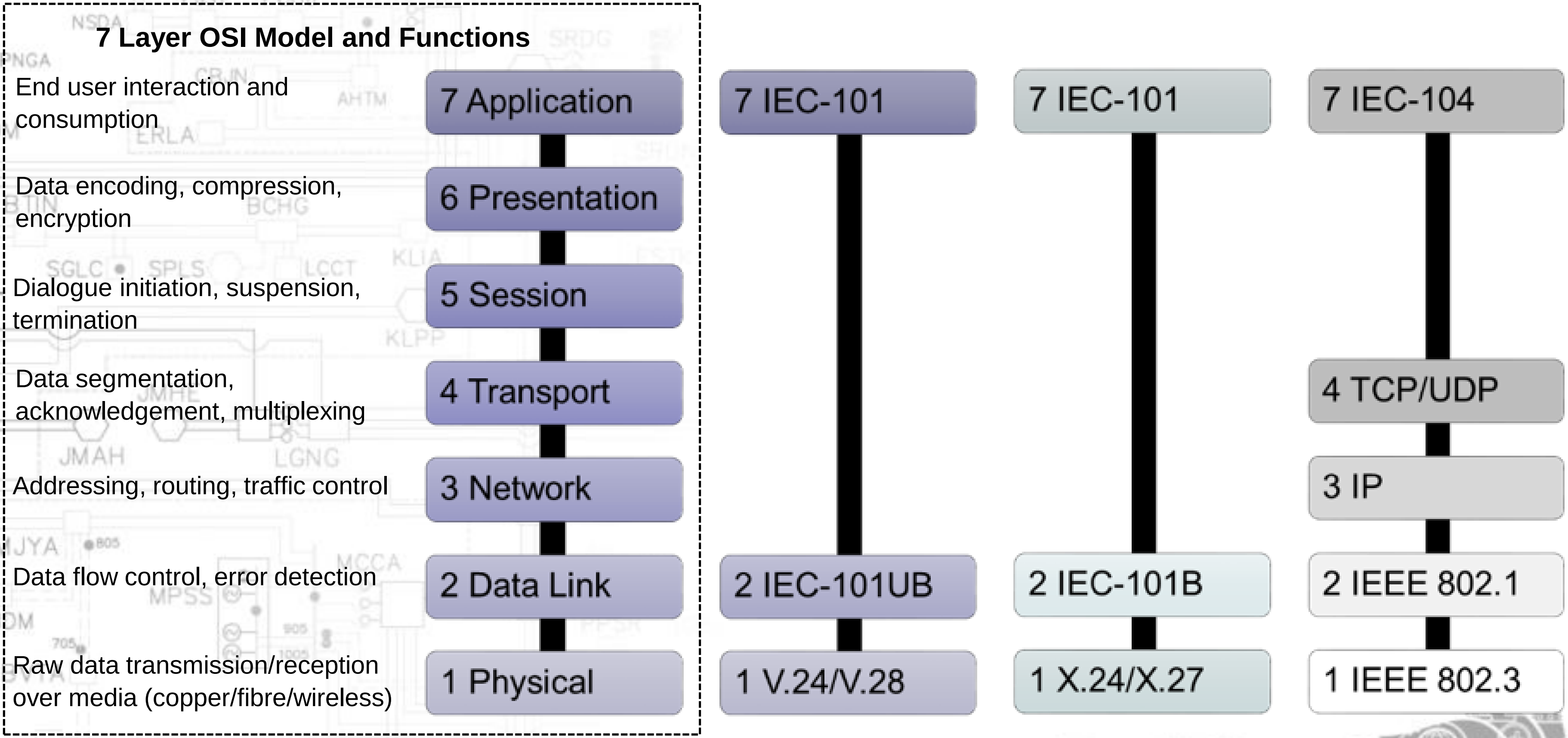
# Introduction to IEC 60870-5-101/104 SCADA Communication Protocols

- A SCADA communication protocol describes the message structure, its semantics, error handling and the procedure of exchanging messages between master and RTU
- IEC 60870-5-101/104 are abbreviated as IEC-101 and IEC104
- IEC-101 utilizes serial communication
- IEC-104 utilizes Ethernet-based communication
- Released in Feb 1990, with latest updates on June 2016 by International Electrotechnical Commission (IEC)
- This standard covers telecontrol equipment for monitoring and controlling geographically widespread processes

# IEC-101, IEC-104 and OSI Model

- OSI (Open System Interconnection) Model is a conceptual model used to characterized and standardized communication functions
- Developed by ISO (International Organization for Standardization)
- Consists of 7 'layers' that are connected to one another (each layer in a device provides relevant info to corresponding layer in the other connected device)
- These layers have specific functions and passes data to one layer above and below it
- Data is encapsulated (additional data headers as added) as it traverses down the layers and de-encapsulated (additional data headers are stripped off) as it travers up the layers.

# IEC-101, IEC-104 and OSI Model



**7 Layer OSI Model and Functions**

| | | | | |
|---|---|---|---|---|
| End user interaction and consumption | 7 Application | 7 IEC-101 | 7 IEC-101 | 7 IEC-104 |
| Data encoding, compression, encryption | 6 Presentation | | | |
| Dialogue initiation, suspension, termination | 5 Session | | | |
| Data segmentation, acknowledgement, multiplexing | 4 Transport | | | 4 TCP/UDP |
| Addressing, routing, traffic control | 3 Network | | | 3 IP |
| Data flow control, error detection | 2 Data Link | 2 IEC-101UB | 2 IEC-101B | 2 IEEE 802.1 |
| Raw data transmission/reception over media (copper/fibre/wireless) | 1 Physical | 1 V.24/V.28 | 1 X.24/X.27 | 1 IEEE 802.3 |

IEC-101 operates in Balance (B) and Unbalanced (UB) modes

# IEC 101/104 Application Functions, ASDU and Mapping to SCADA Functions

| Application Function/ Communication Procedure | IEC-101/104 ASDU* | SCADA Function |
|---|---|---|
| Station initialization | End of initialization (R) | Establishment of communication with RTU |
| Acquisition of events | Single-point information with time tag CP56Time2a (R) | Monitoring of plant equipment status, indications and alarms e.g.<br>• Circuit breaker spring uncharged<br>• Protection relay operated |
| | Double-point information with time tag CP56Time2a (R) | Monitoring of switchgear status, e.g.:<br>• Circuit breaker trip/close<br>• Disconnector open/close |
| | Measured value, short floating point value with time tag CP56Time2a (R) | Monitoring of plant measurements e.g. voltage (kV), active power (MW) and reactive power (MVAr) |
| Station interrogation | • Interrogation command (M)<br>• Single-point information (R)<br>• Double-point information (R)<br>• Measured value, short floating point value (R) | Updating plant equipment data after connection with RTU is established or re-established after communication breakdown |
| Clock synchronization | Clock synchronization command (M) | Synchronizing RTU clock |
| Command transmission | Double command (M) | Operating switchgears e.g.:<br>• Opening/closing circuit breaker<br>• Opening/closing disconnector |

*** Note: (M) / (R) indicates the message is initiated by (M)aster station or (R)TU respectively**

The ASDU (Application Service Data Unit), exchanged between master and RTU defines the specific message data structure and the required parameters to perform a specific protocol application function

# IEC 101/104 Protocol Operation by Analogy

| Control Engineer at Control Centre | SSO at Substation | Equivalent IEC-101/104 Communication Procedure |
|---|---|---|
| Hello | Hello | Station initialization |
| Please report all status and measurements | Roger that<br>CB1 = close,<br>DIS1 = close,<br>DIS2 = open,<br>kV = 133.5<br>MW = 125<br>MVAr = 15.7<br>etc.<br>All status reported | Station interrogation |

Control Engineer (as “SCADA Master”) communicates with Substation Switching Operator (SSO) (as “RTU”) by phone

# Teaching IEC-101 & IEC-104 in ILSAS

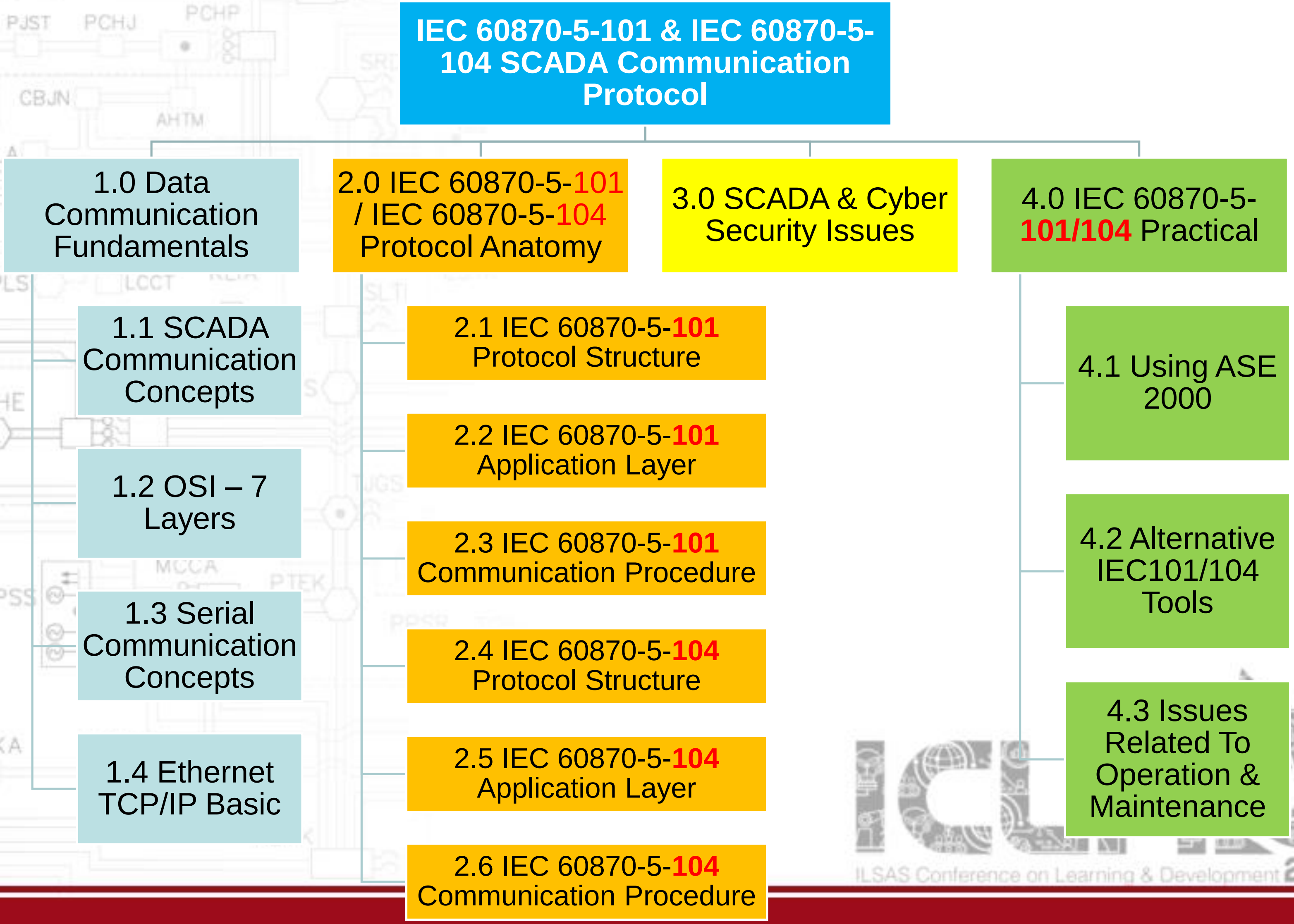
ICLAD

ILSAS Conference on Learning & Development 2019

# Training Need for IEC-101/104

- To provide theoretical knowledge and practical experience for operation and maintenance personnel on IEC-101 and IEC-104 SCADA communication protocol
- More then 90% of TNB SCADA Equipment uses IEC-101/104 as their main communication protocol

# Learning Structure for IEC101/104 in ILSAS



- IEC 60870-5-101 & IEC 60870-5-104 SCADA Communication Protocol
  - 1.0 Data Communication Fundamentals
    - 1.1 SCADA Communication Concepts
    - 1.2 OSI – 7 Layers
    - 1.3 Serial Communication Concepts
    - 1.4 Ethernet TCP/IP Basic
  - 2.0 IEC 60870-5-101 / IEC 60870-5-104 Protocol Anatomy
    - 2.1 IEC 60870-5-101 Protocol Structure
    - 2.2 IEC 60870-5-101 Application Layer
    - 2.3 IEC 60870-5-101 Communication Procedure
    - 2.4 IEC 60870-5-104 Protocol Structure
    - 2.5 IEC 60870-5-104 Application Layer
    - 2.6 IEC 60870-5-104 Communication Procedure
  - 3.0 SCADA & Cyber Security Issues
  - 4.0 IEC 60870-5-101/104 Practical
    - 4.1 Using ASE 2000
    - 4.2 Alternative IEC101/104 Tools
    - 4.3 Issues Related To Operation & Maintenance

ILSAS Conference on Learning & Development 2019

# Challenges in Teaching IEC-101/104 to Adult Learners

- This subject is very conceptual
- Learning by VAK (Visual, Auditory and Kinesthetic)
- Lack of interactive examples for the course
- Lack of hands-on practice
- Limited access to software tool - currently the class uses Kalkitech ASE 2000 as protocol analyzer for IEC-101 and IEC-104 (3 Units of ASE 2000)

# RTU Lab in ILSAS

- The only lab in Peninsular Malaysia with actual RTUs from multiple vendors
  - Foxboro C50
  - Foxboro SCD 5200
  - PDSB Viscon2 C3
  - Dong Fang DF1331
  - Dong Fang DF1725
  - ABB 560
- These RTUs have simulatable Input (via Toggle Switches) and Output (via Visual Lamps)

# SCADA Communication Protocol Classes in ILSAS

- Proprietary protocol from Westinghouse (WISP+)
- IEC-101 Protocol
- IEC-104 Protocol
- DNP3

# Typical SCADA Communication Protocols Training in ILSAS

- Limited number of class size (max. 12 students per class) since current Protocol Analyzers are limited to 3 licenses (4 students per group)
- Theory-based learning (vs. flipped class, student-led learning)
- Now made possible with M10x allowing increased No. of students per class

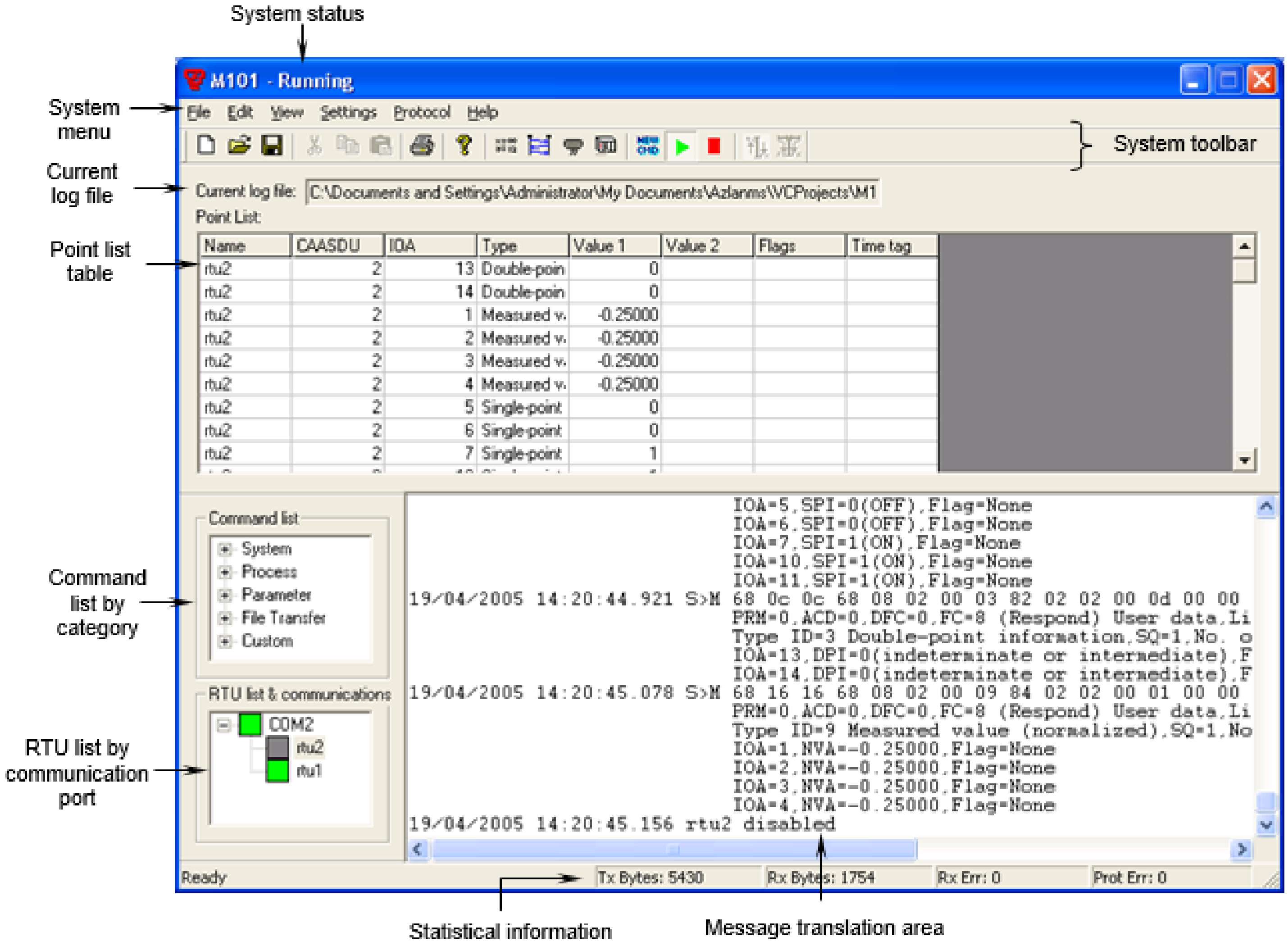
# TNB M10x Application

ILSAS Conference on Learning & Development 2019

# TNB M10x Application

- Work started in 2003 by a small team in TNB Transmission Division (now TNB Grid Division), called M101
- Using Microsoft Visual C++
- Primarily used for RTU Protocol Conformance Testing on IEC-101
- In 2017, NLDC developed support for IEC-104
- M101 renamed to M10x to reflect added support for IEC-104

# Screenshot of M10x and its Main GUIs



Current log file: C:\Documents and Settings\Administrator\My Documents\Azlanms\VCProjects\M1

Point List:

| Name | CAASDU | IOA | Type | Value 1 | Value 2 | Flags | Time tag |
|---|---|---|---|---|---|---|---|
| rtu2 | 2 | 13 | Double-poin | 0 | | | |
| rtu2 | 2 | 14 | Double-poin | 0 | | | |
| rtu2 | 2 | 1 | Measured v. | -0.25000 | | | |
| rtu2 | 2 | 2 | Measured v. | -0.25000 | | | |
| rtu2 | 2 | 3 | Measured v. | -0.25000 | | | |
| rtu2 | 2 | 4 | Measured v. | -0.25000 | | | |
| rtu2 | 2 | 5 | Single-point | 0 | | | |
| rtu2 | 2 | 6 | Single-point | 0 | | | |
| rtu2 | 2 | 7 | Single-point | 1 | | | |

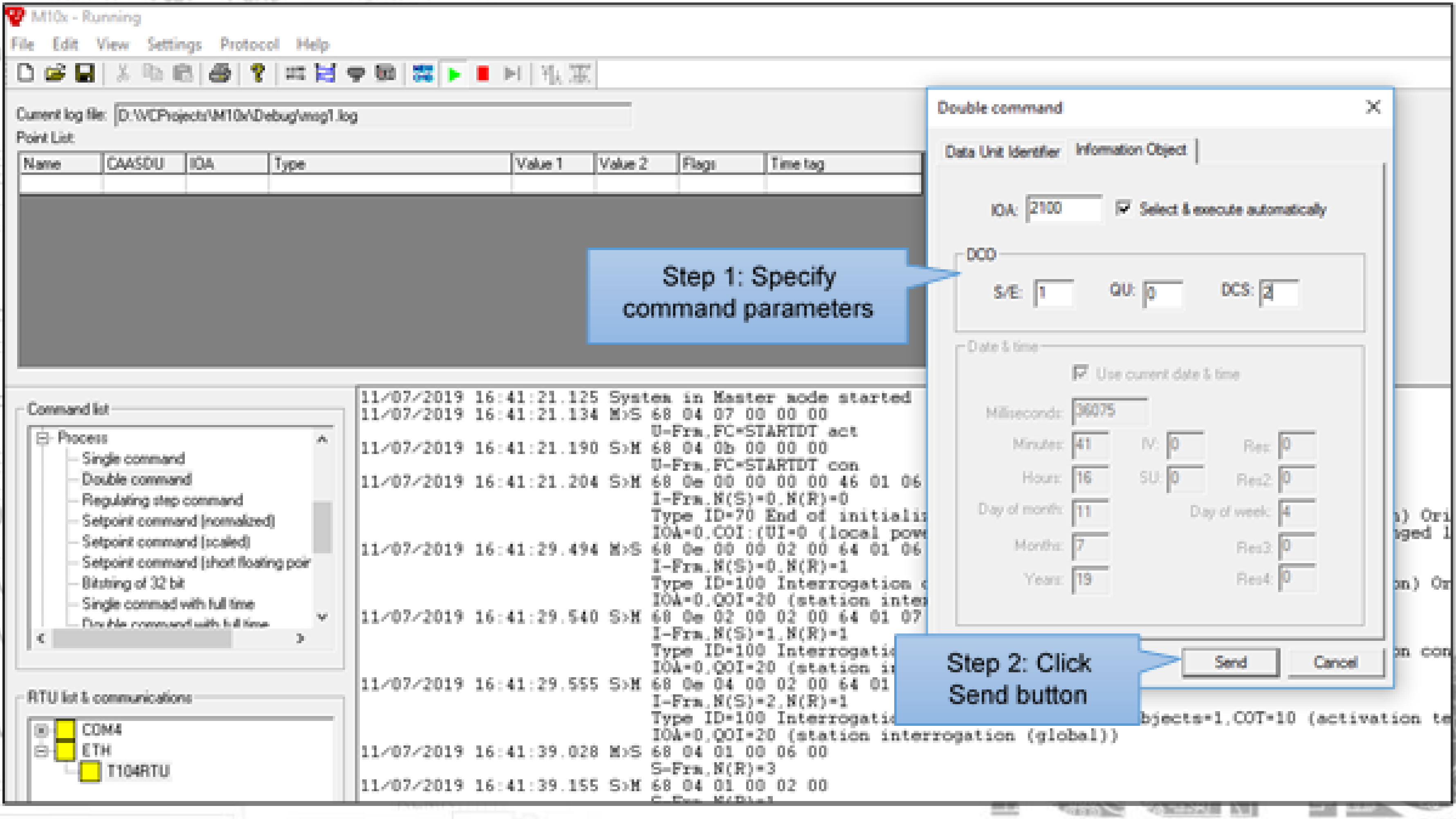
```
                                IOA=5,SPI=0(OFF),Flag=None
                                IOA=6,SPI=0(OFF),Flag=None
                                IOA=7,SPI=1(ON),Flag=None
                                IOA=10,SPI=1(ON),Flag=None
                                IOA=11,SPI=1(ON),Flag=None
19/04/2005 14:20:44.921 S>M 68 0c 0c 68 08 02 00 03 82 02 02 00 0d 00 00
                                PRM=0,ACD=0,DFC=0,FC=8 (Respond) User data,Li
                                Type ID=3 Double-point information,SQ=1,No. o
                                IOA=13,DPI=0(indeterminate or intermediate),F
                                IOA=14,DPI=0(indeterminate or intermediate),F
19/04/2005 14:20:45.078 S>M 68 16 16 68 08 02 00 09 84 02 02 00 01 00 00
                                PRM=0,ACD=0,DFC=0,FC=8 (Respond) User data,Li
                                Type ID=9 Measured value (normalized),SQ=1,No
                                IOA=1,NVA=-0.25000,Flag=None
                                IOA=2,NVA=-0.25000,Flag=None
                                IOA=3,NVA=-0.25000,Flag=None
                                IOA=4,NVA=-0.25000,Flag=None
19/04/2005 14:20:45.156 rtu2 disabled
```

Tx Bytes: 5430 | Rx Bytes: 1754 | Rx Err: 0 | Prot Err: 0

# M10x Use in Training

- RTU is preconfigured with suitable I/O representing Circuit Breakers, Isolators etc.
- Various scenarios are presented to the trainees to achieve using M10x
  - Retrieve all RTU data
  - Simulate RTU events (status and alarms)
  - Simulate RTU measurements
  - Sending Command to Trip/Close Circuit Breakers/Isolators
  - Setting RTU Clock
  - Simulate communication breakdown and recovery

# Example: Command Transmission – Closing Circuit Breaker



Current log file: D:\VCProjects\M10x\Debug\msg1.log

Point List:

IOA: 2100 ☑ Select & execute automatically

DCO

S/E: 1 QU: 0 DCS: 2

Date & time

☑ Use current date & time

Milliseconds: 36075

Minutes: 41 IV: 0 Res: 0

Hours: 16 SU: 0 Res2: 0

Day of month: 11 Day of week: 4

Months: 7 Res3: 0

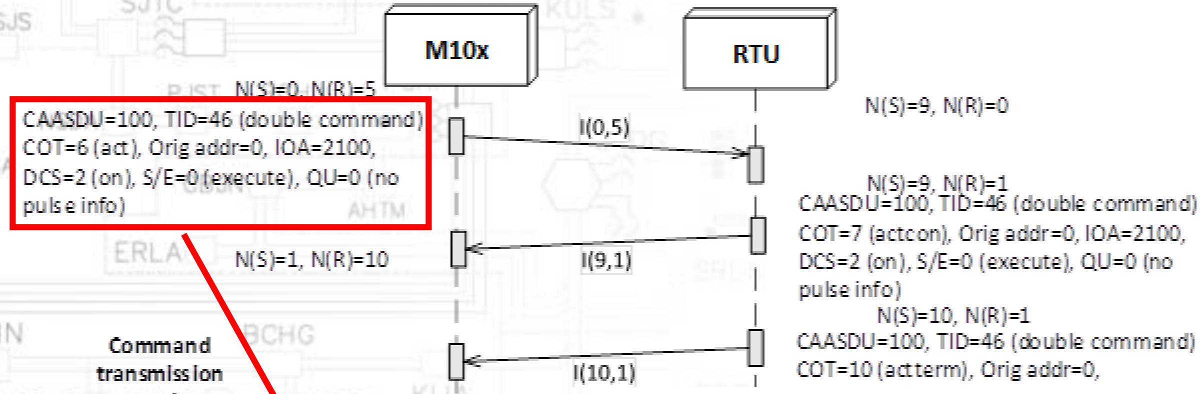
Years: 19 Res4: 0

```
11/07/2019 16:41:21.125 System in Master mode started
11/07/2019 16:41:21.134 M>S 68 04 07 00 00 00
                            U-Frm,FC=STARTDT act
11/07/2019 16:41:21.190 S>M 68 04 0b 00 00 00
                            U-Frm,FC=STARTDT con
11/07/2019 16:41:21.204 S>M 68 0e 00 00 00 00 46 01 06
                            I-Frm,N(S)=0,N(R)=0
                            Type ID=70 End of initiali
                            IOA=0,COI:(UI=0 (local pow
11/07/2019 16:41:29.494 M>S 68 0e 00 00 02 00 64 01 06
                            I-Frm,N(S)=0,N(R)=1
                            Type ID=100 Interrogation c
                            IOA=0,QOI=20 (station inter
11/07/2019 16:41:29.540 S>M 68 0e 02 00 02 00 64 01 07
                            I-Frm,N(S)=1,N(R)=1
                            Type ID=100 Interrogati
                            IOA=0,QOI=20 (station i
11/07/2019 16:41:29.555 S>M 68 0e 04 00 02 00 64 01
                            I-Frm,N(S)=2,N(R)=1
                            Type ID=100 Interrogati               bjects=1,COT=10 (activation te
                            IOA=0,QOI=20 (station interrogation (global))
11/07/2019 16:41:39.028 M>S 68 04 01 00 06 00
                            S-Frm,N(R)=3
11/07/2019 16:41:39.155 S>M 68 04 01 00 02 00
```

Step 1: Specify command parameters

Step 2: Click Send button

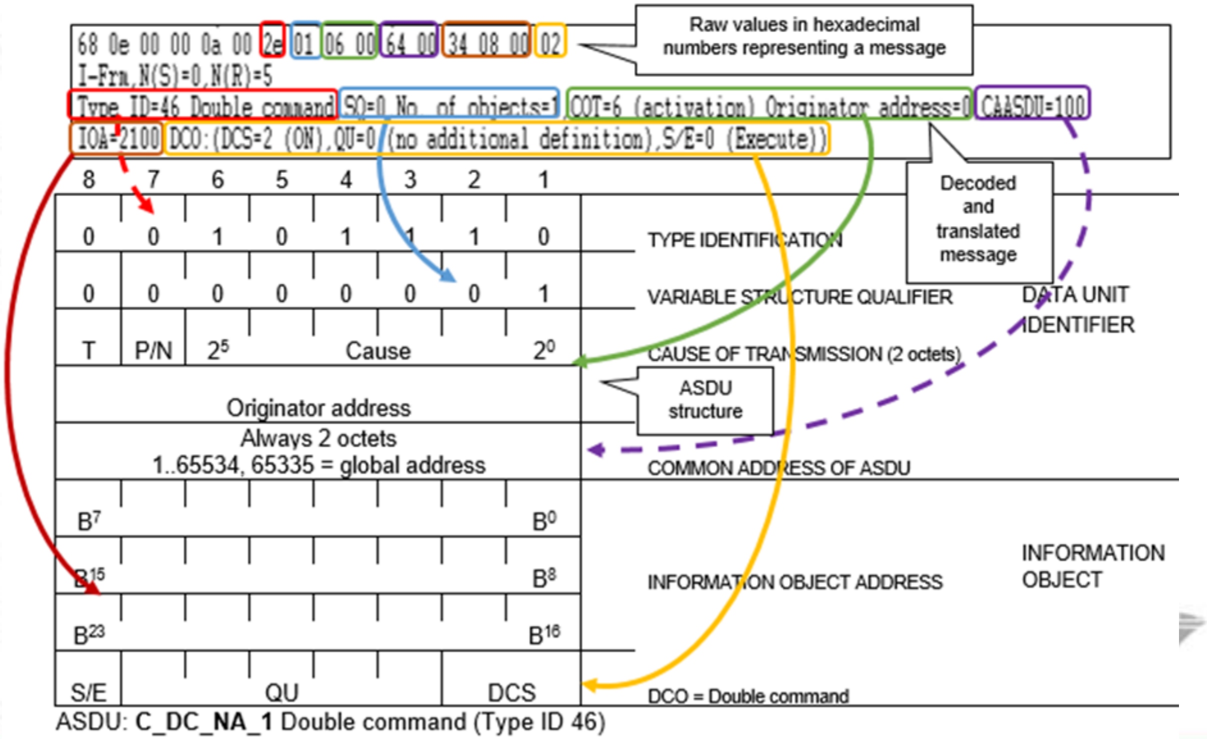
# Command Transmission Procedure and Dissection of Double Command ASDU



CAASDU=100, TID=46 (double command) COT=6 (act), Orig addr=0, IOA=2100, DCS=2 (on), S/E=0 (execute), QU=0 (no pulse info)

CAASDU=100, TID=46 (double command) COT=7 (actcon), Orig addr=0, IOA=2100, DCS=2 (on), S/E=0 (execute), QU=0 (no pulse info)

CAASDU=100, TID=46 (double command) COT=10 (actterm), Orig addr=0,



```
68 0e 00 00 0a 00 2e 01 06 00 64 00 34 08 00 02
I-Frm,N(S)=0,N(R)=5
Type ID=46 Double command SQ=0 No. of objects=1 COT=6 (activation) Originator address=0 CAASDU=100
IOA=2100 DCO:(DCS=2 (ON),QU=0 (no additional definition),S/E=0 (Execute))
```

Raw values in hexadecimal numbers representing a message

Decoded and translated message

| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | TYPE IDENTIFICATION | DATA UNIT IDENTIFIER |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | VARIABLE STRUCTURE QUALIFIER | |
| T | P/N | $2^5$ | | Cause | | | $2^0$ | CAUSE OF TRANSMISSION (2 octets) | |
| Originator address | | | | | | | | | |
| Always 2 octets<br>1..65534, 65335 = global address | | | | | | | | COMMON ADDRESS OF ASDU | |
| $B^7$ | | | | | | | $B^0$ | | |
| $B^{15}$ | | | | | | | $B^8$ | INFORMATION OBJECT ADDRESS | INFORMATION OBJECT |
| $B^{23}$ | | | | | | | $B^{16}$ | | |
| S/E | QU | | | | | DCS | | DCO = Double command | |

ASDU structure

ASDU: C_DC_NA_1 Double command (Type ID 46)

Trainees can analyze message transaction and drill down individual message to inspect the ASDU parameters to understand the protocol operation

# Comparison with other Protocol Analyzer

| Feature | Other Protocol Analyzer | TNB M10x |
|---|---|---|
| Supported protocols | IEC-101 (Balanced & Unbalanced), IEC-104, DNP3, Modbus | IEC-101 (Unbalanced), IEC-104 |
| Mode | Master & Slave Simulation, Eavesdrop | Master Simulation, Eavesdrop |
| Slave topology | Point-to-point, party line (IEC-101), star | Point-to-point, party line (IEC-101) |
| Point list | Available | Available |
| Message Translation | Available | Available |
| Logging | Available (proprietary format) | Available (text file) |

- Most of standard features are supported
- Unsupported features are optional or not required by TNB

# Benefit of TNB M10x

- Low CAPEX (Free)
- In-house development, can be further customized to fit evolving requirements
- Free software that trainee can take home and use in daily work (Grid Maintenance)

# Conclusion

- M10x is a cost effective tool that are used in order to increase competency for IEC-101 and IEC-104
- Trainees are more hands-on and can really re-inforce their understanding in IEC-101 and IEC-104
- Low cost means that
  - trainees that straight away use the tool immediately after training
  - retraining is not required after relocation of staff if M10x becomes a standard tool in TNB
  - In-house training module by ILSAS, external training provider not required
- In-house development means that the tools can be further customized to meet users' needs

# Demo on M10x

ILSAS Conference on Learning & Development 2019

# Thank You

# Thank You

**Main Branch:**

TNB Integrated Learning Solution Sdn Bhd – ILSAS,
Jalan IKRAM-UNITEN, 43650 Bandar Baru Bangi,
Selangor, Malaysia.
Tel: (+6)03-892272222
Fax: (+6)03-89263505
Email: infoILSAS@tnb.com.my
Website: www.tnbilsas.com.my

**Malim Nawar Branch:**

TNB Integrated Learning Solution Sdn Bhd – ILSAS,
PO Box 1, 31700 Malim Nawar, Perak, Malaysia.
Tel:  (+6)05-4775960
Fax:  (+6)05-4775954

Certified to ISO 9001:2008
Cert. No. : AR3912

Class 'A' Training Provider

Human Resource Minister Award 2007 Winner—Best Training Provider Category