SCADA TROJANS

ATTACKING THE GRID

RUBEN SANTAMARTA

/Rootəd° CON 2011

3-4-5 Marzo 2011
Madrid

¿What are we going to talk about?

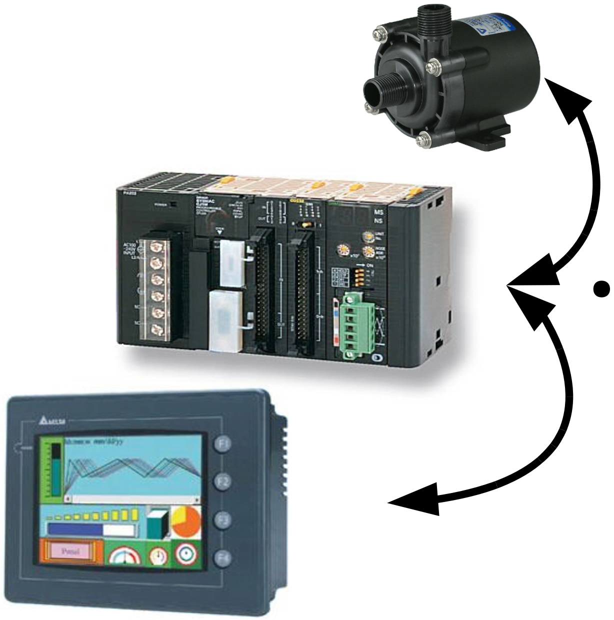
- SCADA / EMS
- TROJANS
- ATTACKS VECTORS
- REVERSE ENGINEERING
- ELECTRICAL ENERGY SYSTEM

THEORY

1. SCADA

Supervisory Control And Data Acquisition (Supervisión, Control y Adquisición de Datos).

- FIELD DEVICES
- PLC/RTU/IED
- HMI / SCADA SERVER

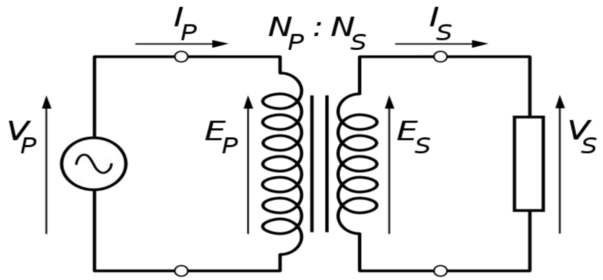


- PROTOCOLS

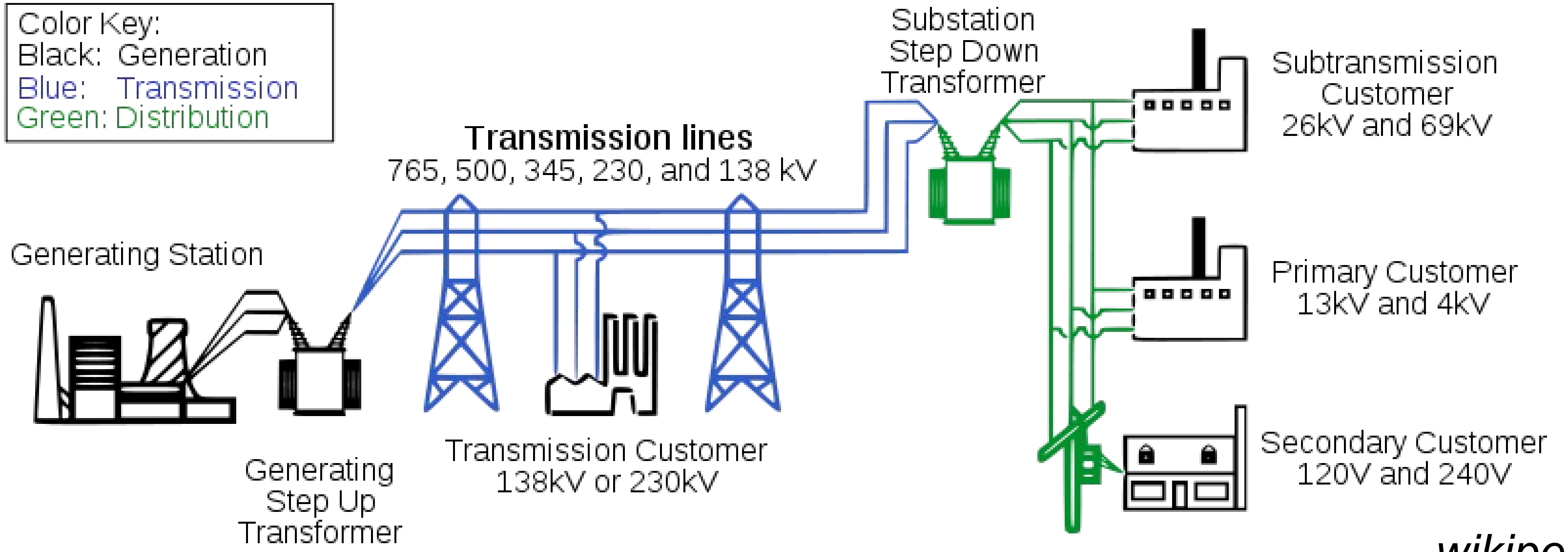
2.Electrical Energy System I

Biggest industrial system ever

- TRANSFORMER INVENTION – WIN!
  +V -I → Transmission over long distances



$$\frac{V_P}{V_S}=\frac{I_S}{I_P}=\frac{N_P}{N_S}$$

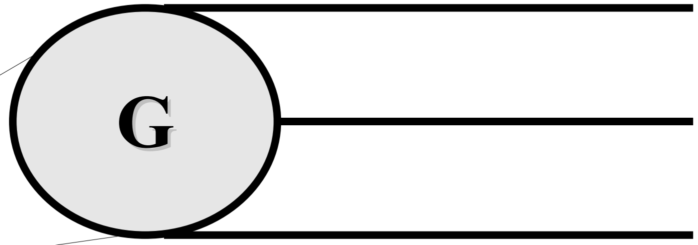


wikipedia

2.Electrical Energy System II

Generation

Primary Source → Station → Three-Phase AC Generator → Step up Transformer → Transmission lines

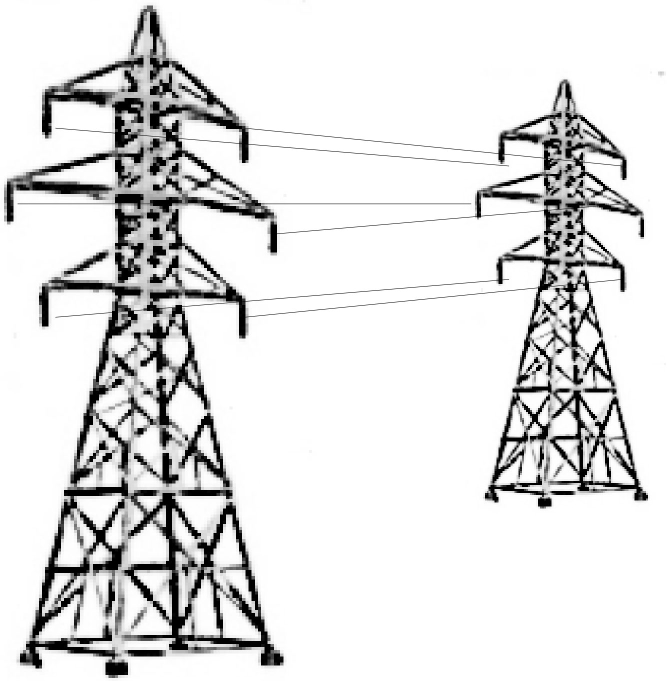


- Nuclear
- Hydroelectric
- Photovoltaic/Wind
- Biomass
- ...

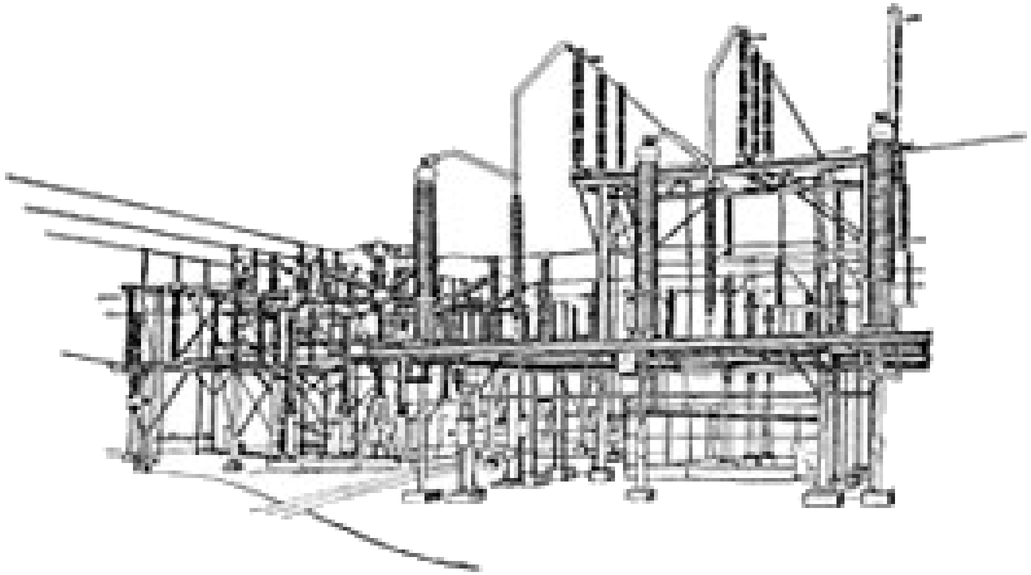
2.Electrical Energy System III

Transmission

Power Lines



Substations



2.Electrical Energy System IV

Transmission – Substations I

RUNNING METASPLOIT AGAINST A SUBST. :)

2.Electrical Energy System IV

Transmission – Substations II

A Substation is a place where we can found

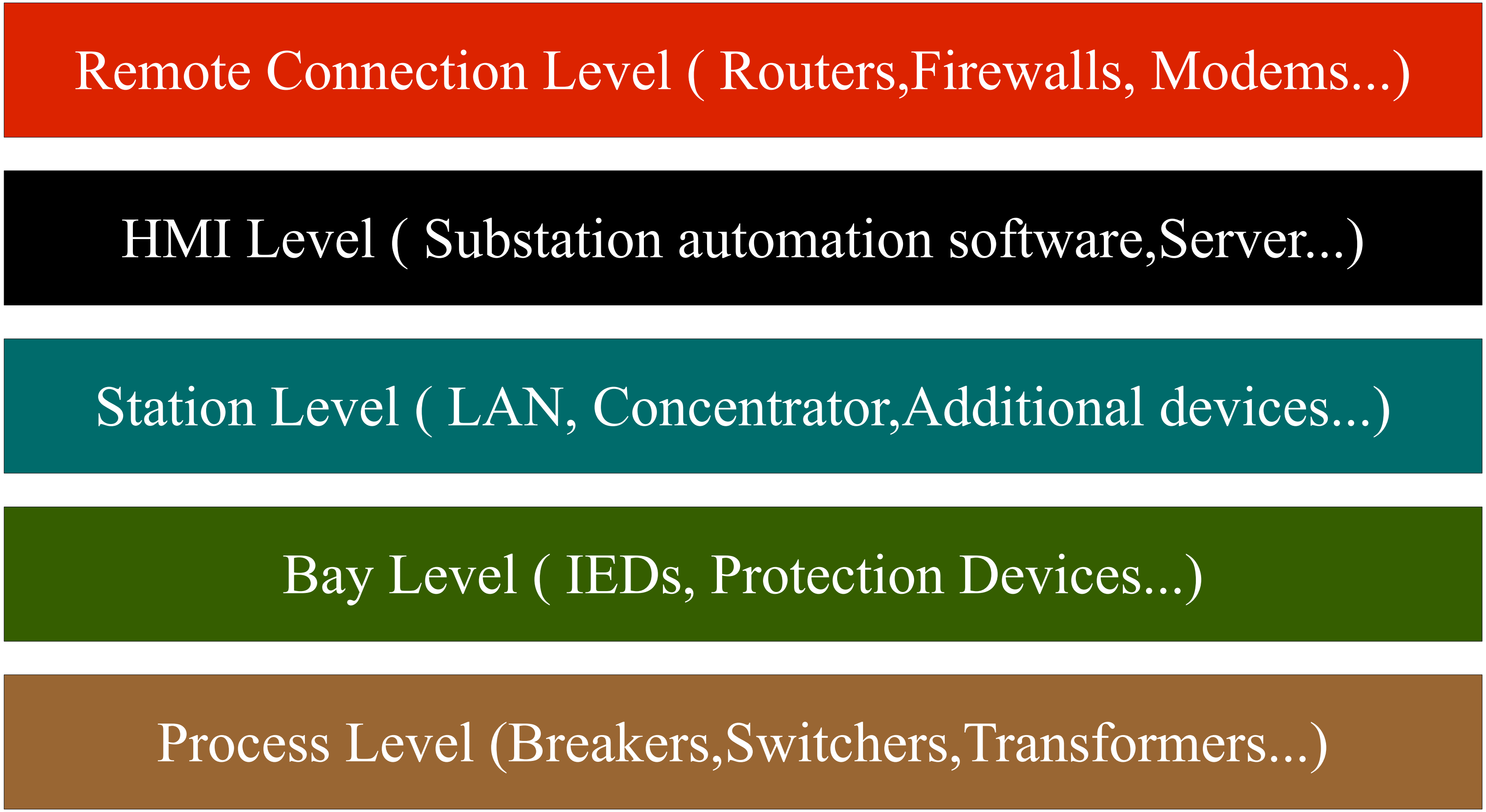
- Interconnection buses for lines
- Step down transformers
- Measurement, protection, interruption and dispatch equipment
  - Disconnect Switches
  - Load Break Switches
  - Circuit Switchers
  - Power Fuses
  - Circuit Breakers

Types of Substations

→ Transmission → Distribution → Collector → Switching

2.Electrical Energy System V

Transmission – Substation Automation I



Remote Connection Level (Routers,Firewalls, Modems...)

HMI Level (Substation automation software,Server...)

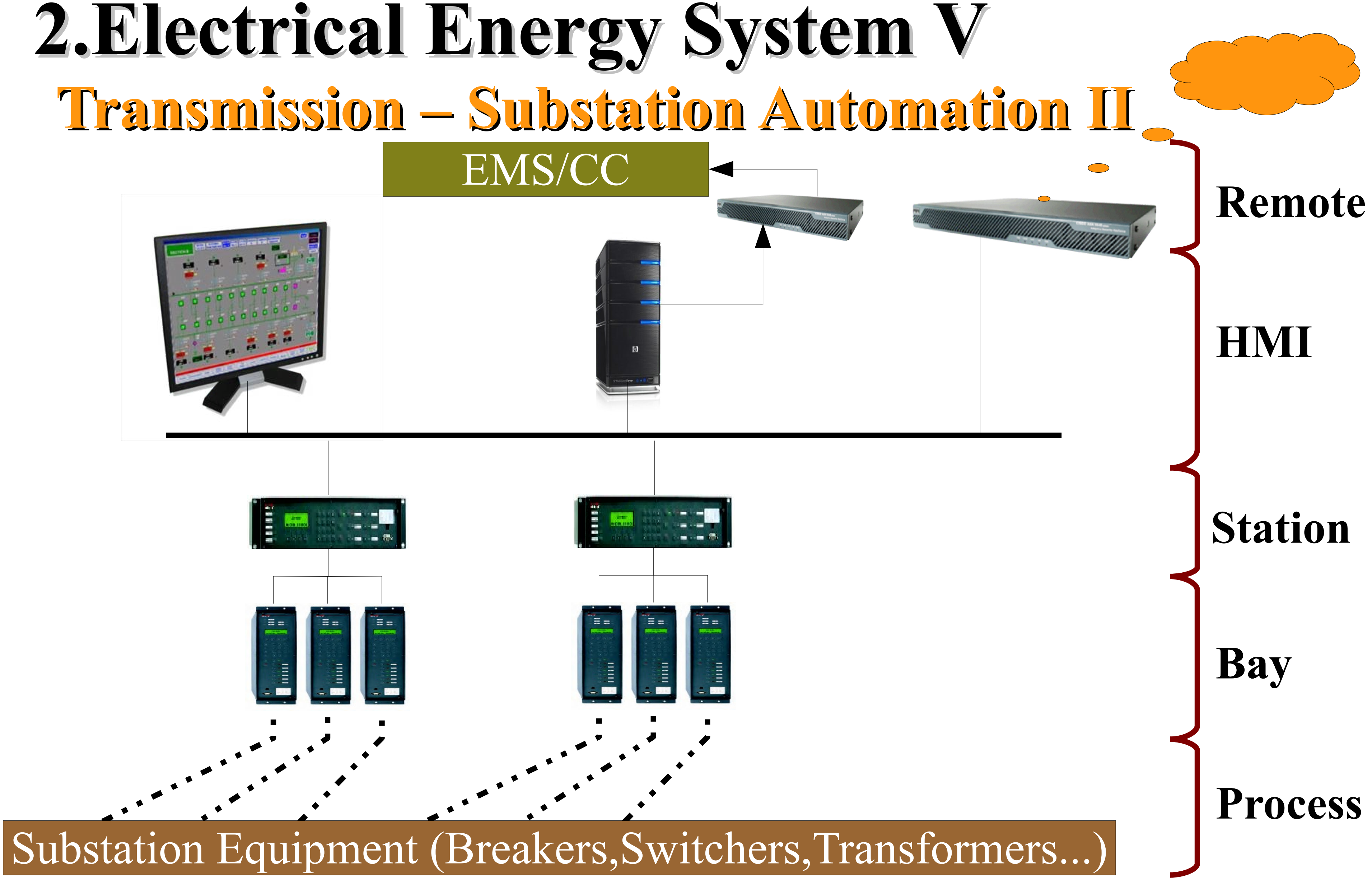
Station Level (LAN, Concentrator,Additional devices...)

Bay Level (IEDs, Protection Devices...)

Process Level (Breakers,Switchers,Transformers...)

2.Electrical Energy System V

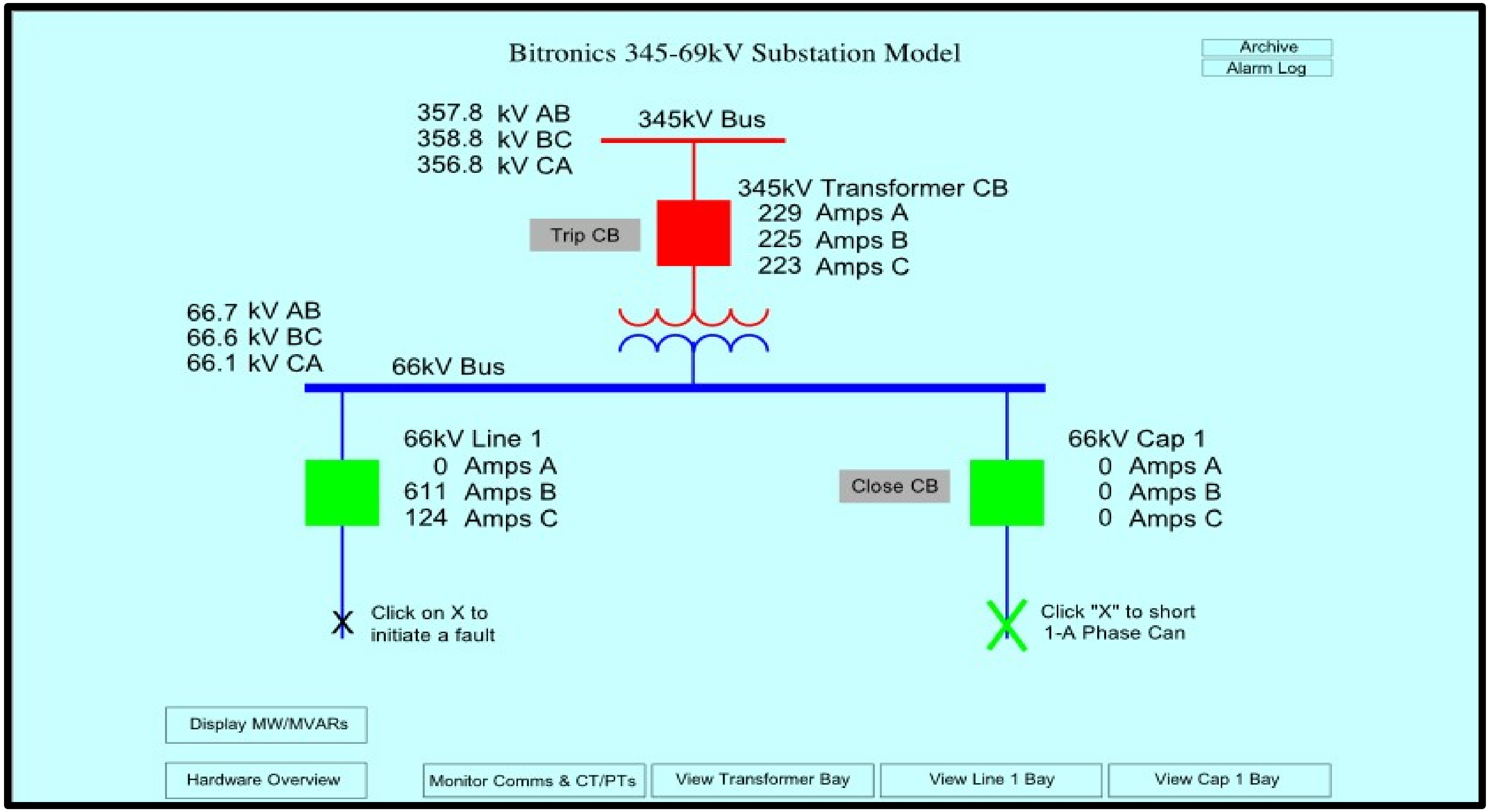
Transmission – Substation Automation II



2.Electrical Energy System V

Transmission – Substation Automation III

- HMI
- One-line diagrams



Bitronics 345-69kV Substation Model

357.8 kV AB
358.8 kV BC
356.8 kV CA

345kV Transformer CB
229 Amps A
225 Amps B
223 Amps C

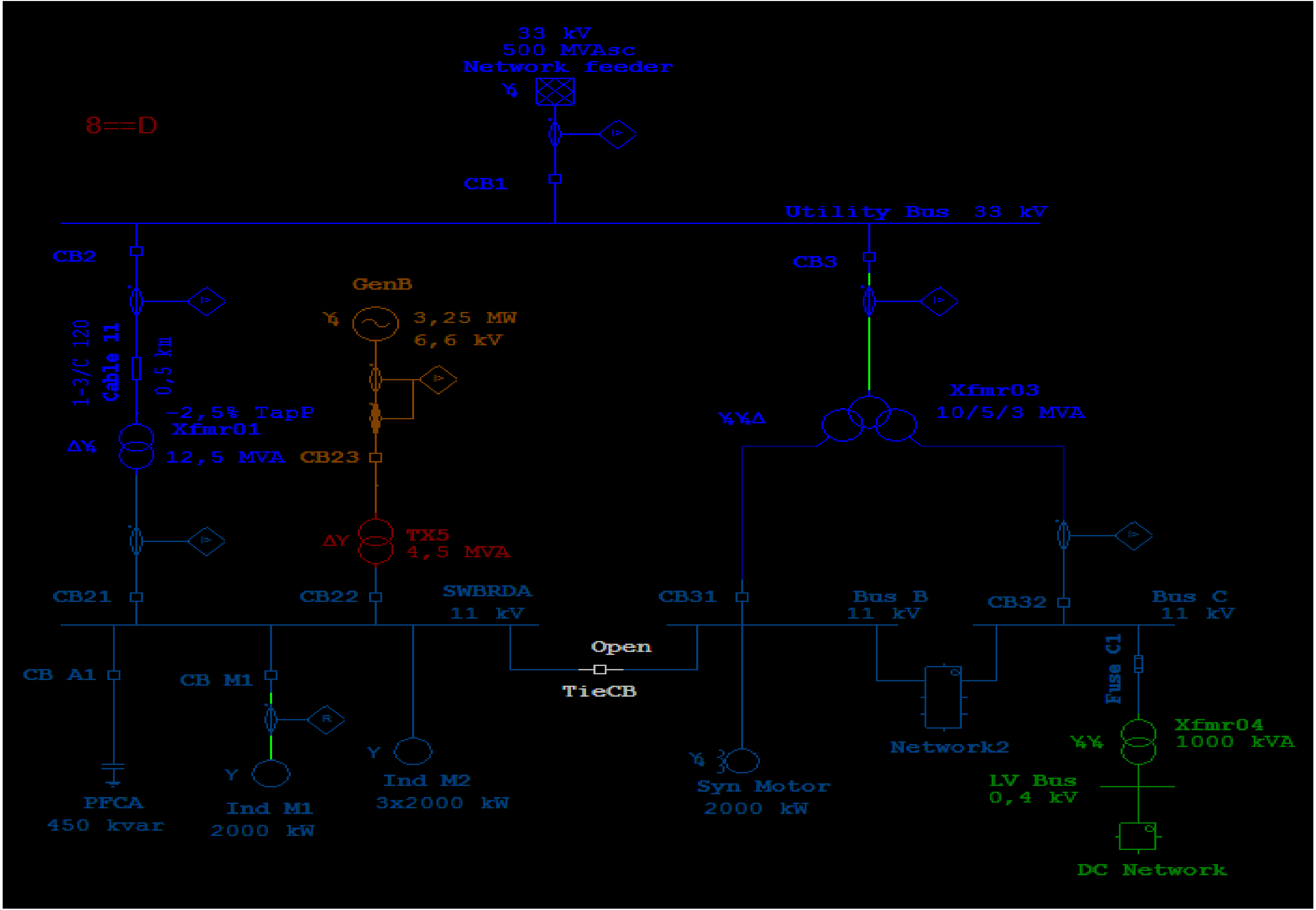
66.7 kV AB
66.6 kV BC
66.1 kV CA

66kV Line 1
0 Amps A
611 Amps B
124 Amps C

66kV Cap 1
0 Amps A
0 Amps B
0 Amps C

Click on X to initiate a fault

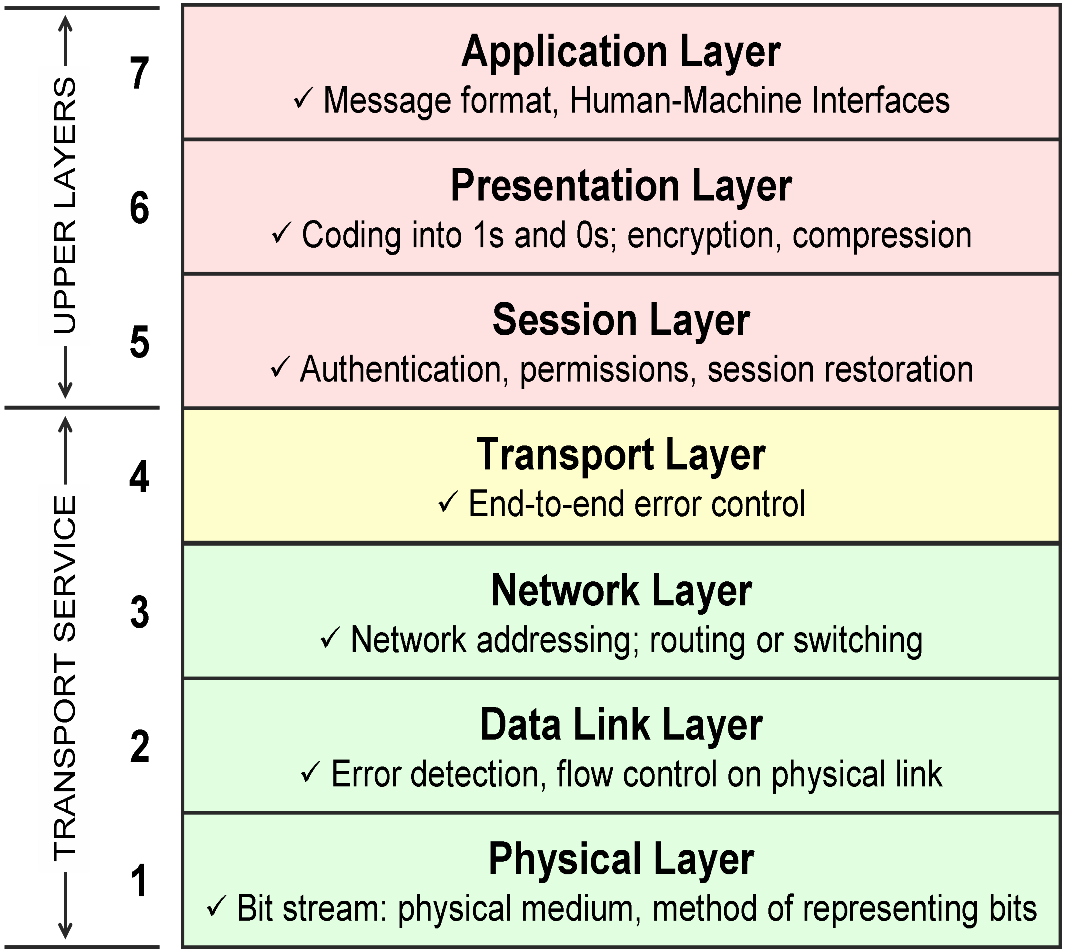
Click "X" to short 1-A Phase Can


33 kV
500 MVAsc
Network feeder
8==D
CB1
Utility Bus 33 kV
CB2
1-3/C 120
Cable 11
0,5 km
-2,5% TapP
Xfmr01
ΔY
12,5 MVA
GenB
3,25 MW
6,6 kV
CB23
ΔY
TX5
4,5 MVA
CB3
Xfmr03
10/5/3 MVA
YYΔ
CB21
CB22
SWBRDA
11 kV
CB31
Bus B
11 kV
CB32
Bus C
11 kV
Open
TieCB
CB A1
CB M1
Y
Y
Ind M2
3x2000 kW
PFCA
450 kvar
Ind M1
2000 kW
Syn Motor
2000 kW
Network2
Fuse C1
Xfmr04
1000 kVA
YY
LV Bus
0,4 kV
DC Network

2.Electrical Energy System V

Transmission – Substation Automation IV

- Protocols
  - DNP3
  - Modbus
  - IEC 60870-5-10(1,3,4)
  - IEC 61850
  - ICCP
  - OPC
  - RS-232/485
  - UCA2 MMS
  - Vendor specific
    - Harris
    - Westinhouse
    - ABB
    - ...



UPPER LAYERS

7 Application Layer
✓ Message format, Human-Machine Interfaces

6 Presentation Layer
✓ Coding into 1s and 0s; encryption, compression

5 Session Layer
✓ Authentication, permissions, session restoration

TRANSPORT SERVICE

4 Transport Layer
✓ End-to-end error control

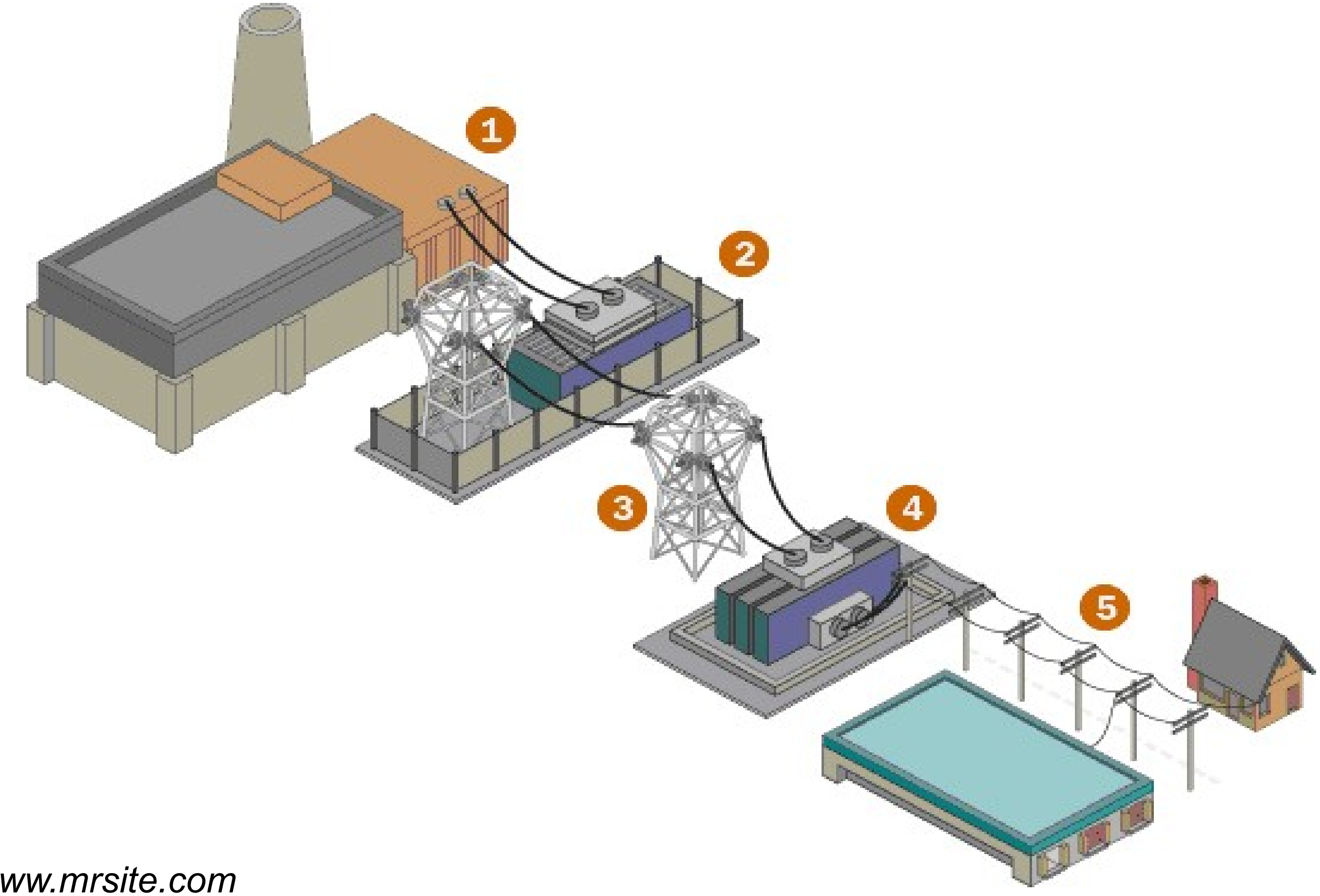
3 Network Layer
✓ Network addressing; routing or switching

2 Data Link Layer
✓ Error detection, flow control on physical link

1 Physical Layer
✓ Bit stream: physical medium, method of representing bits

2.Electrical Energy System V

Distribution

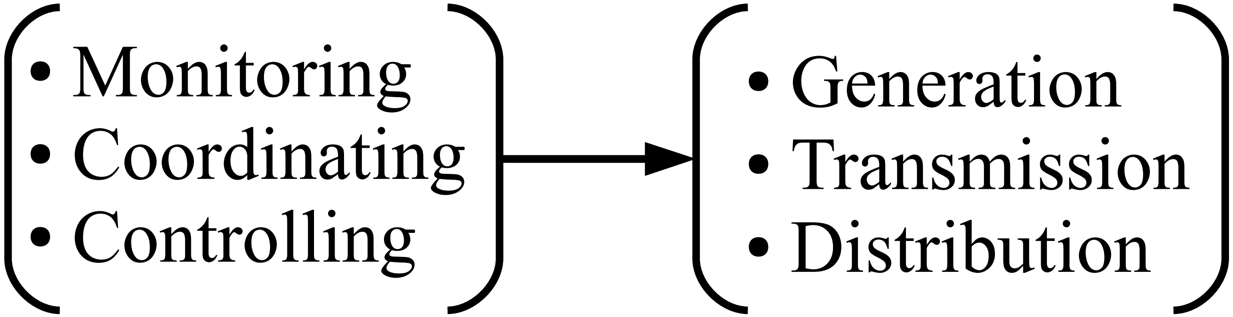


www.mrsite.com

3. EMS / SCADA

ENERGY MANAGEMENT SYSTEMS I

Computer based tools for...



- Monitoring
- Coordinating
- Controlling

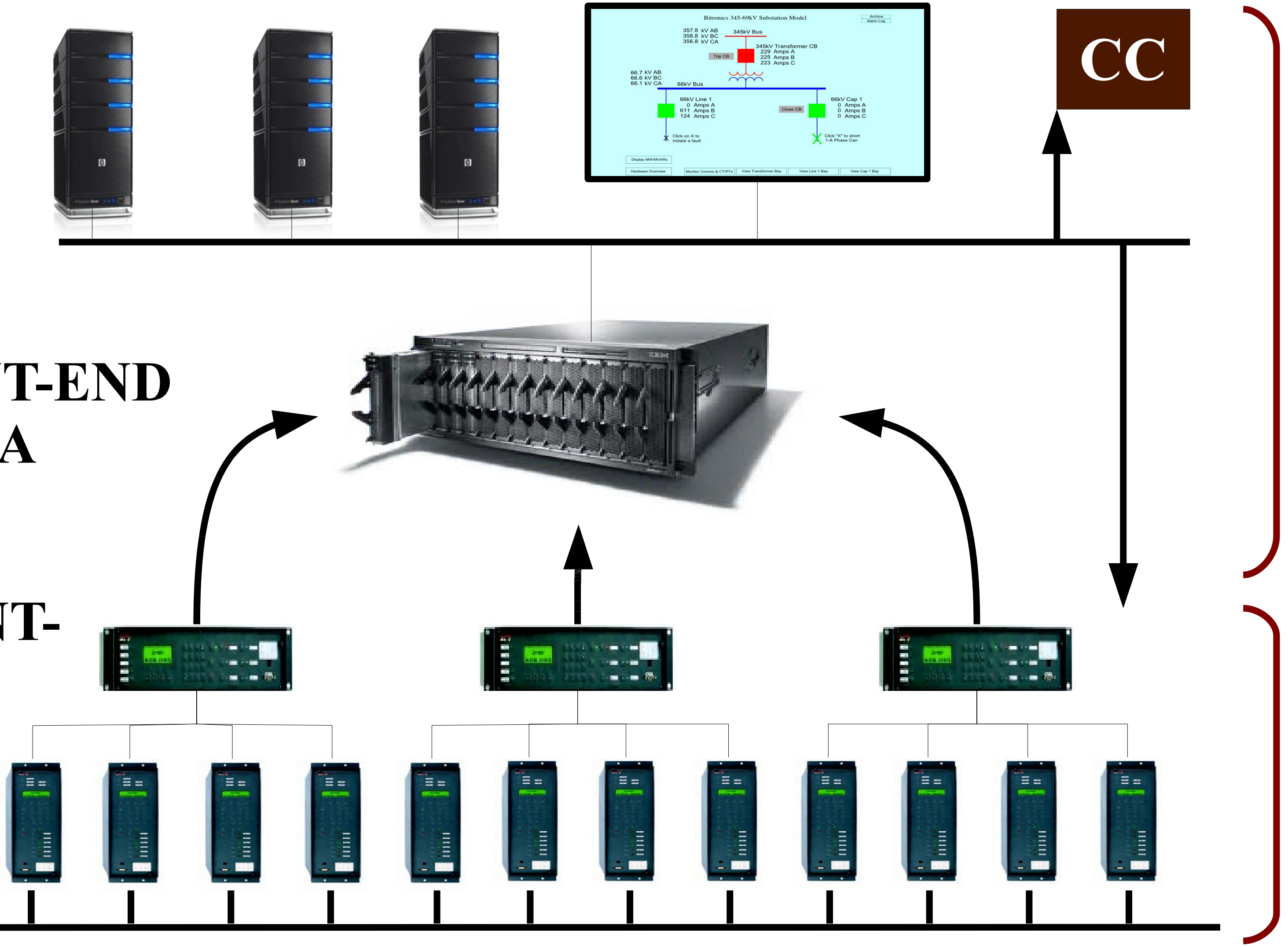
- Generation
- Transmission
- Distribution

KEY CONCEPT:

DECISSION SUPPORT TO OPERATORS

2. EMS / SCADA I

ENERGY MANAGEMENT SYSTEMS II



CONTROL CENTER

FRONT-END SCADA

FRONT-ENDs

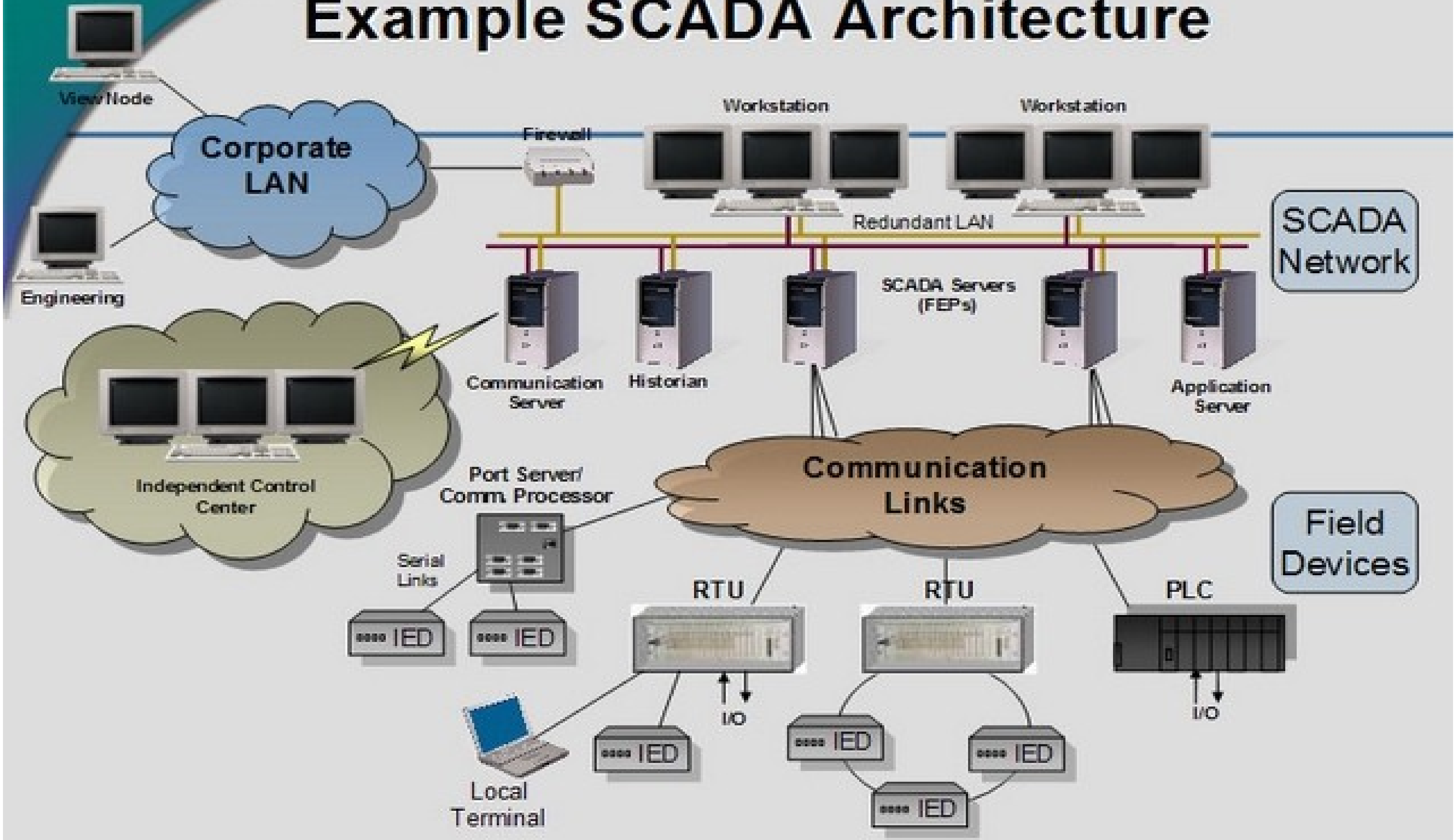
IEDs RTUs

Substation

. . .

PowerPlant

Example SCADA Architecture

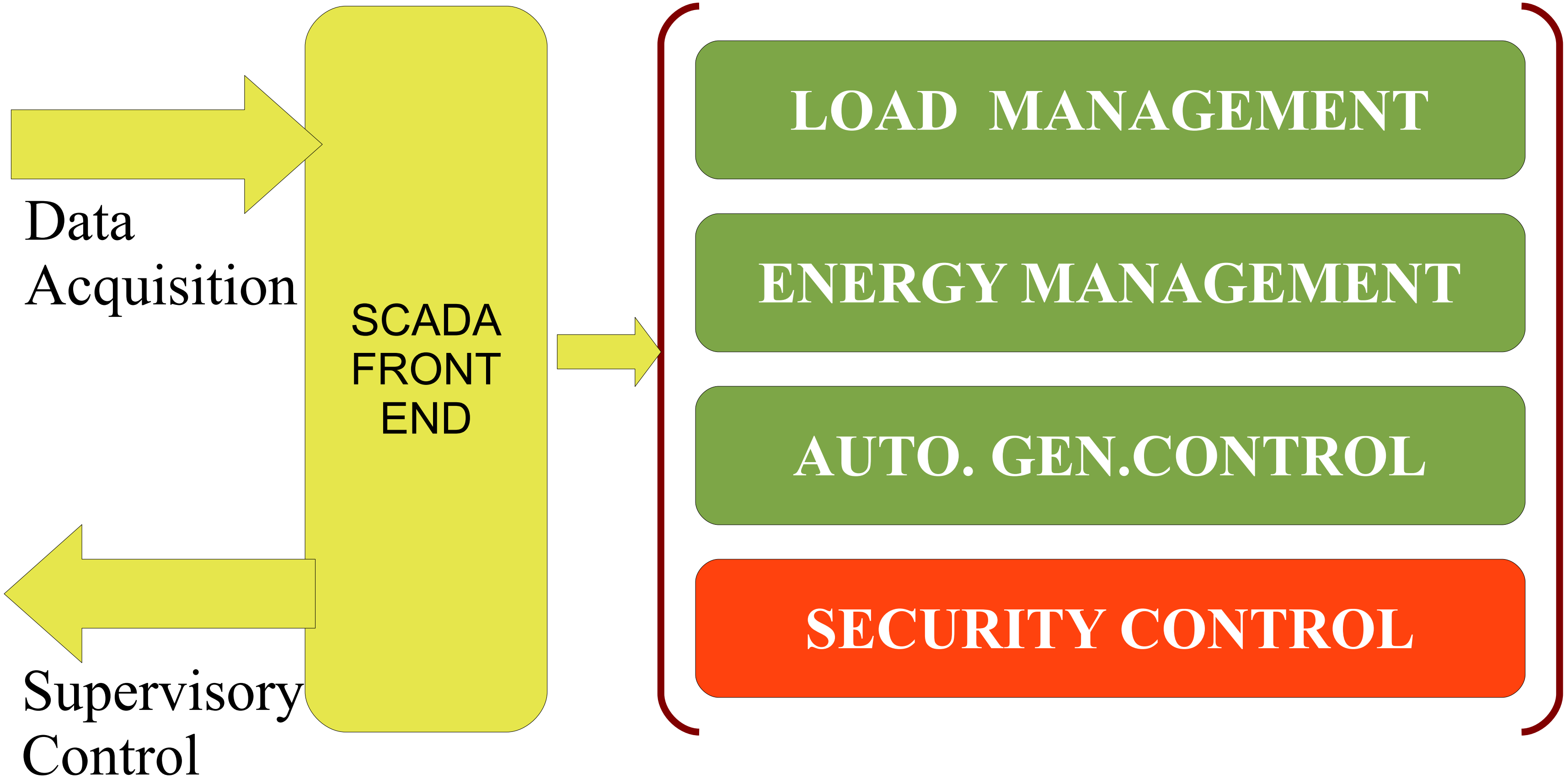


Battelle

Pacific Northwest National Laboratory
U.S. Department of Energy 5

3. EMS / SCADA

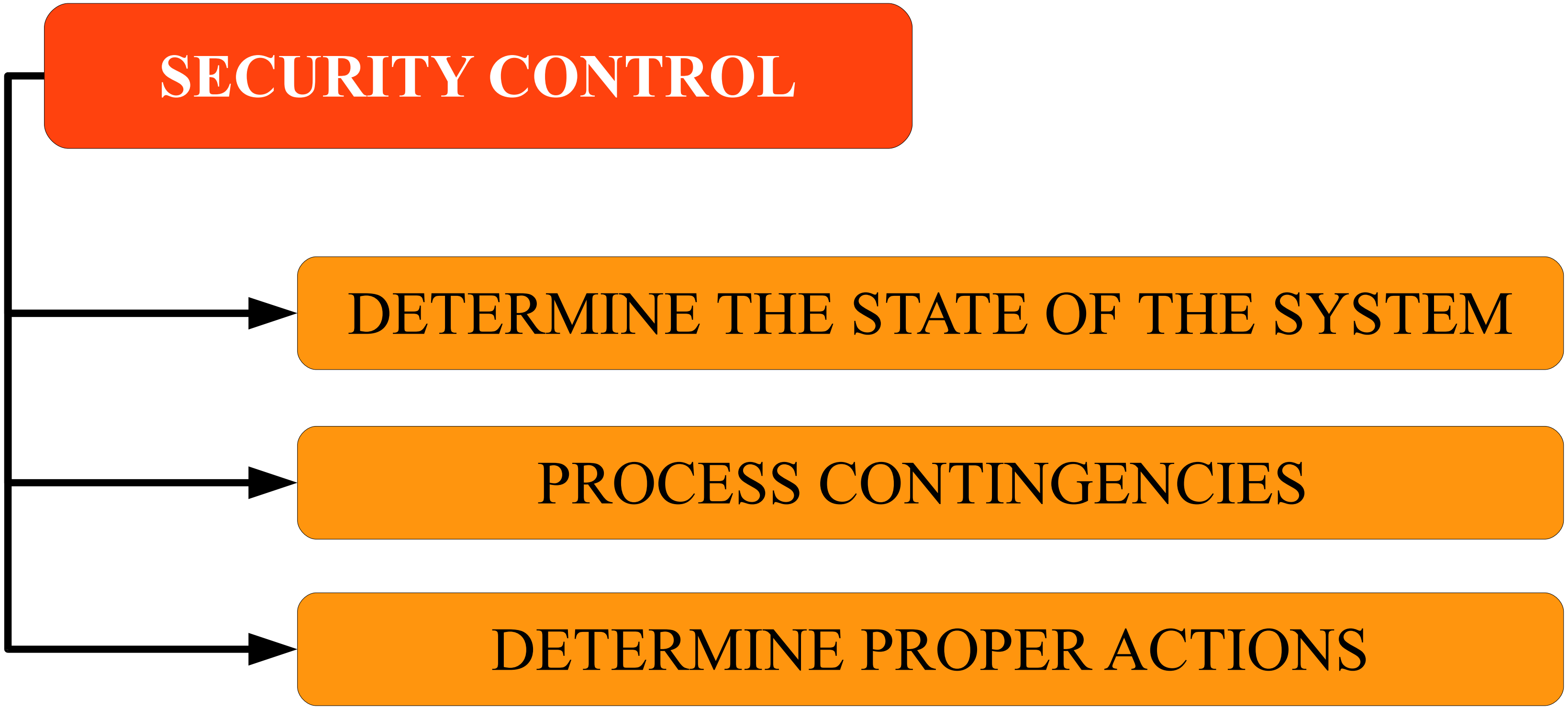
ENERGY MANAGEMENT SYSTEMS III



3. EMS / SCADA

ENERGY MANAGEMENT SYSTEMS III

THE SYSTEM MUST SURVIVE IN ANY CASE



SECURITY CONTROL

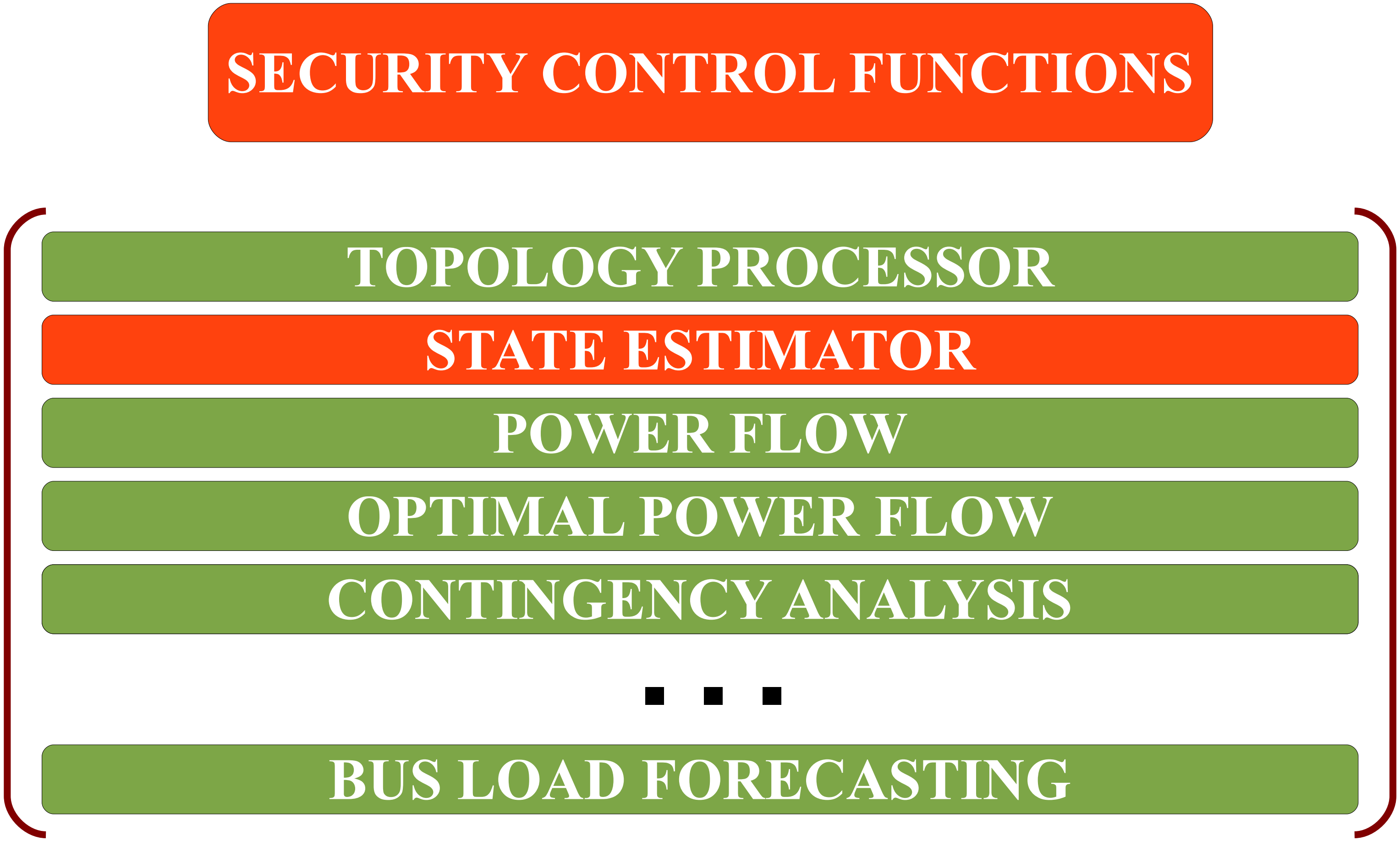
DETERMINE THE STATE OF THE SYSTEM

PROCESS CONTINGENCIES

DETERMINE PROPER ACTIONS

3. EMS / SCADA

ENERGY MANAGEMENT SYSTEMS IV



PRACTICE

4.SCADA TROJANS I

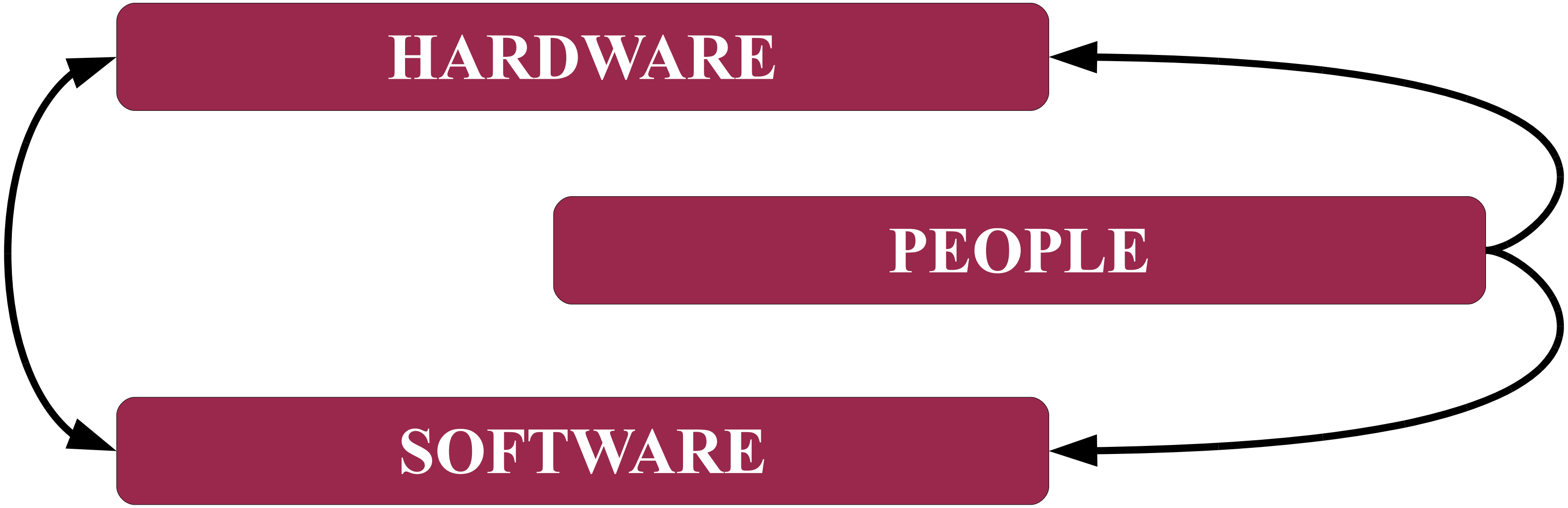
- YOU'RE NOT A TARGET
- SPONSORED BY STATES, LARGE CORPORATIONS AND/OR 4CHAN
- TWO-STAGE TROJANS
- AUTONOMOUS AGENTS
- INTELLIGENCE INSIDE... AND OUTSIDE

4.SCADA TROJANS II

- YOU NEED TO P0WN THE RIGHT PEOPLE
- OBTAIN NEEDED INFO
- REPLICATE THE TARGET
- DEPLOYMENT
- YOU CAN USE MONEY,TECHNOLOGY OR BOTH
- SOME DAY, SOMEWHERE THE 2nd STAGE WILL BE TRIGGERED

4.SCADA TROJANS III

ATTACK VECTORS



4.SCADA TROJANS IV

CONTEXT

TWO LITTLE COUNTRIES IN CONFLICT

RUBENHISTAN
REGGAETONIA
Tiramisú
Gasolinia

- **REGGAETONIA PLANS TO HOLD THE BIGGEST REGGAETON FESTIVAL EVER.**
- **RUBENHISTAN IS DETERMINED TO STOP IT.**

4.SCADA TROJANS V

OPERATION SNOW-HAMS

- RUBENHISTAN's Secret Service maintains a list of companies that operate Reguetonia's facilities.
- RUBENHISTAN's Secret Service also consults public open source intelligence sources as a city's urban planning to determine substations coverage.
- RUBENHISTAN's Secret Service launches a Targeted attack against the operators who control a key substation and even the Reguetonia's EMS

LET'S SEE HOW TO PROCEED

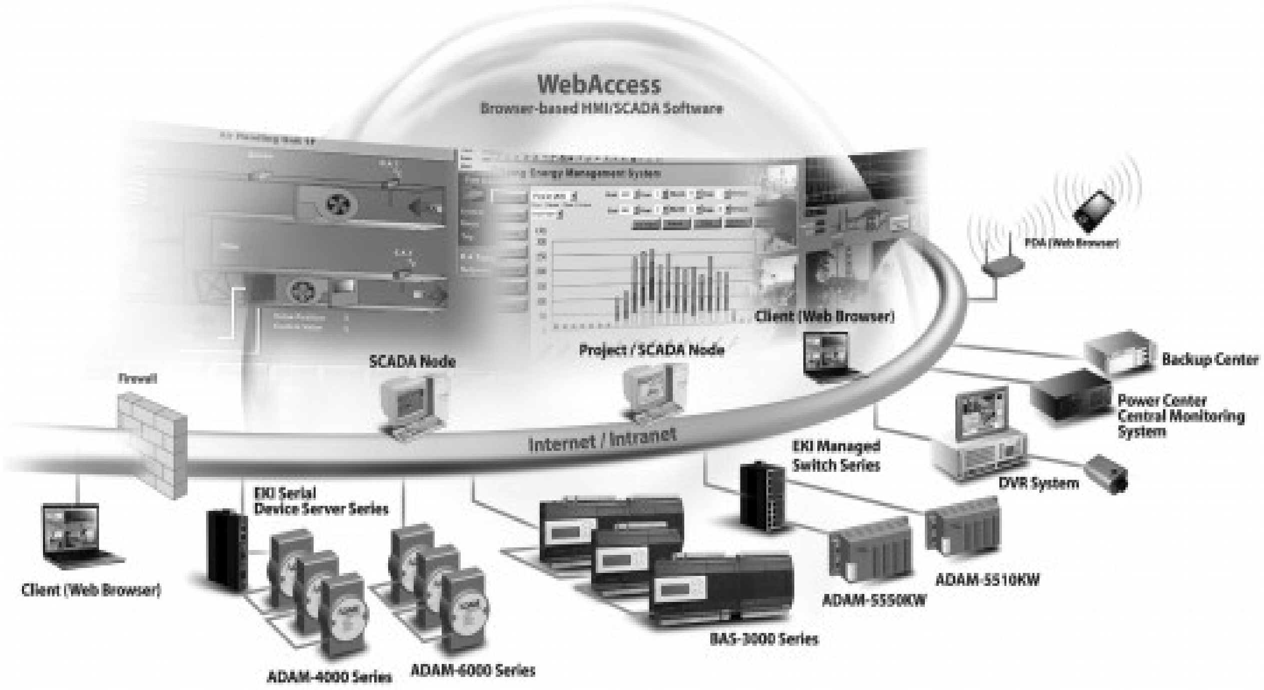
4.SCADA TROJANS VI

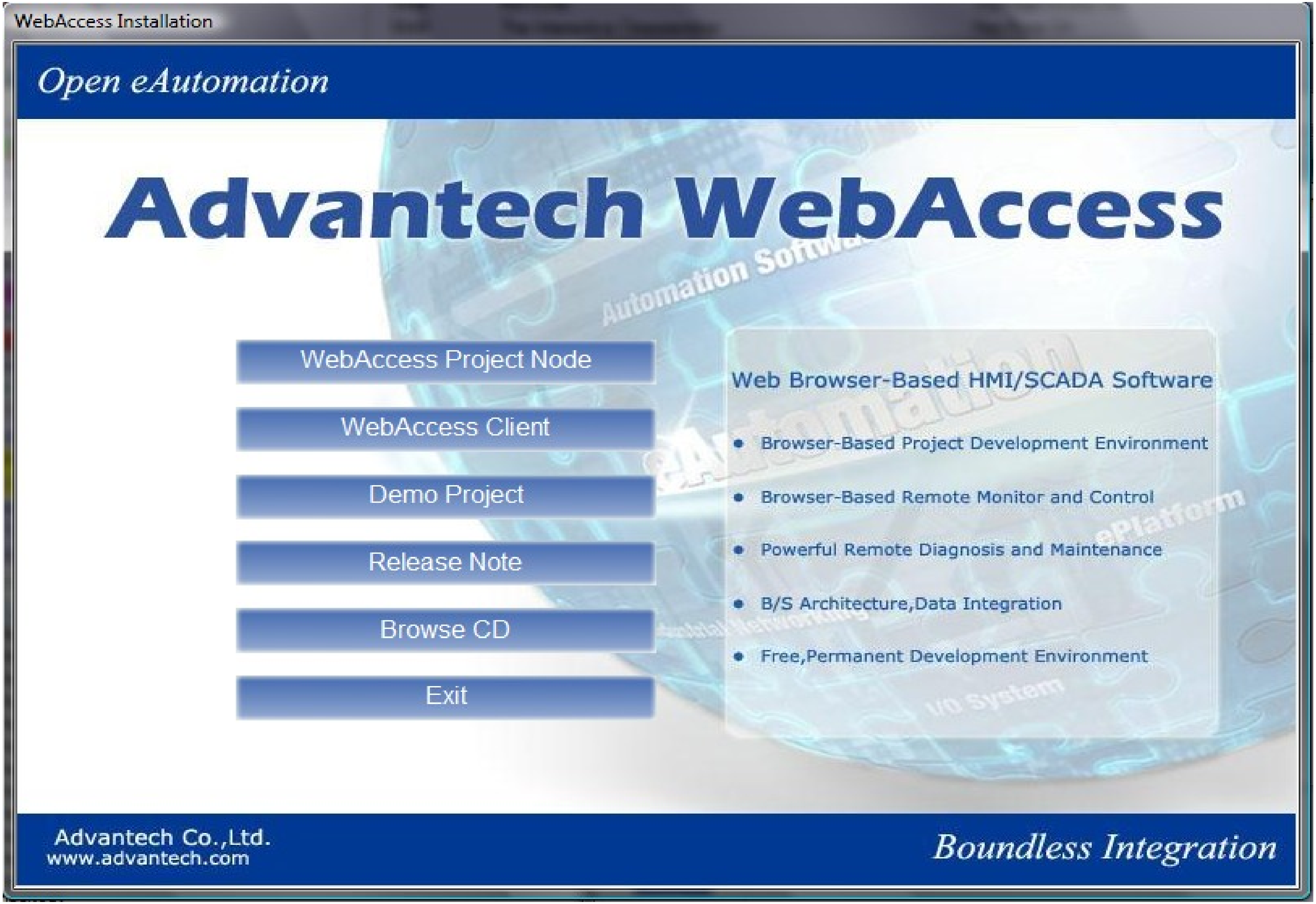
P0WNING THE SUBSTATION I

PURE FICTION

It's known the company who operates the SubStation implements a HMI client/server software from Advantech.

Advantech WebAccess





Open eAutomation

Advantech WebAccess

Web Browser-Based HMI/SCADA Software

- Browser-Based Project Development Environment
- Browser-Based Remote Monitor and Control
- Powerful Remote Diagnosis and Maintenance
- B/S Architecture,Data Integration
- Free,Permanent Development Environment

Advantech Co.,Ltd.
www.advantech.com

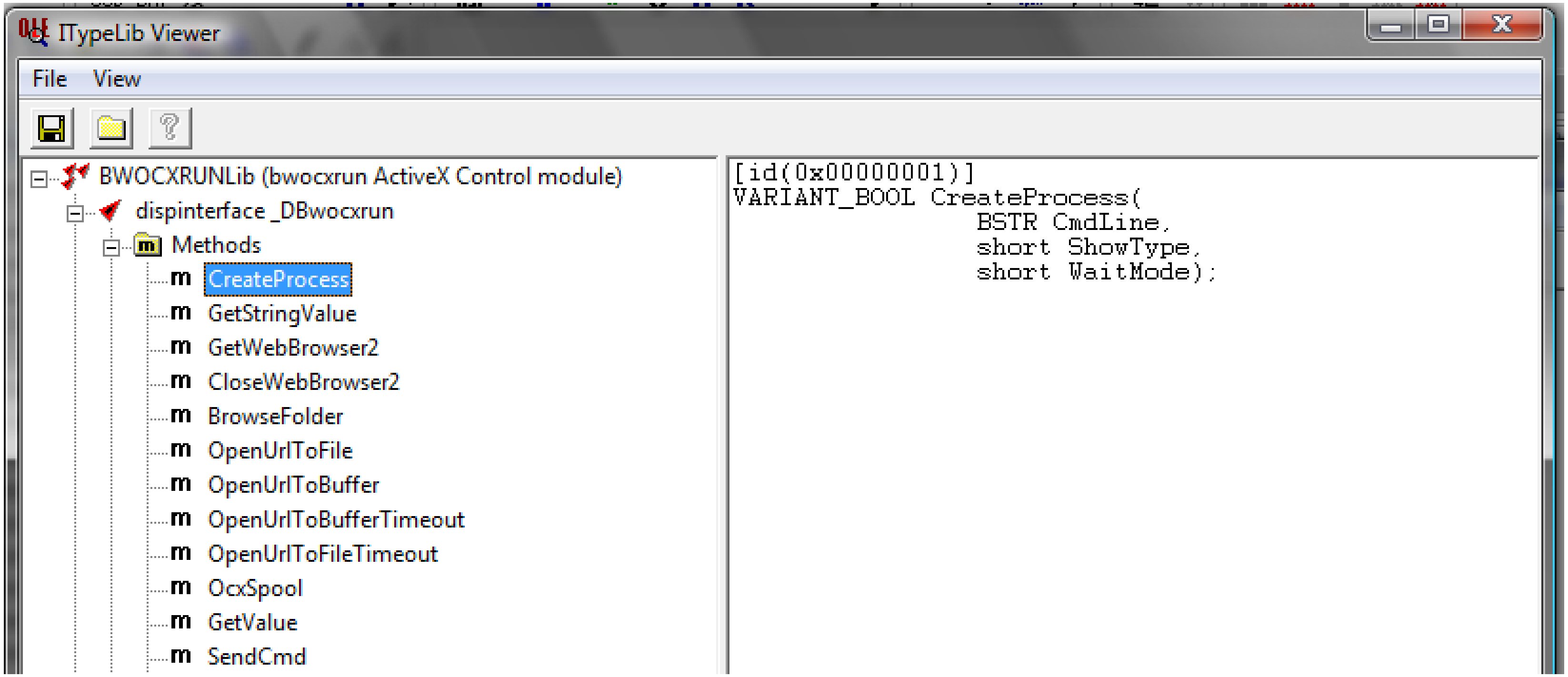
Boundless Integration

4.SCADA TROJANS VI

P0WNING THE SUBSTATION II

c:\windows\system32\bwocxrun.ocx [WebAccess Client]

Implements IObjectSafety: True
IDisp Safe: Safe for untrusted: caller,data
IPersist Safe: Safe for untrusted: caller,data
IPStorage Safe: Safe for untrusted: caller,data



```
[id(0x00000001)]
VARIANT_BOOL CreateProcess(
                BSTR CmdLine,
                short ShowType,
                short WaitMode);
```

4.SCADA TROJANS VI

P0WNING THE SUBSTATION III

- After enticing one of the operators into visiting a specially crafted web, our bwocxrun.ocx exploit worked. We landed.
- Time to map the Substation network.
- At Bay level we find CSE-Semaphore RTUs/IEDs

http://www.cse-semaphore.com/

TBOX LITE 200 - Ethernet

2 counters (I) 6 Analog (I) 4/20mA

8 digital (I/O) 2 Temperature (I) 4 relays 230 V ac 3A(O)

EMBEDDED HTTP Server, FTP, SNMP, EMAIL ...

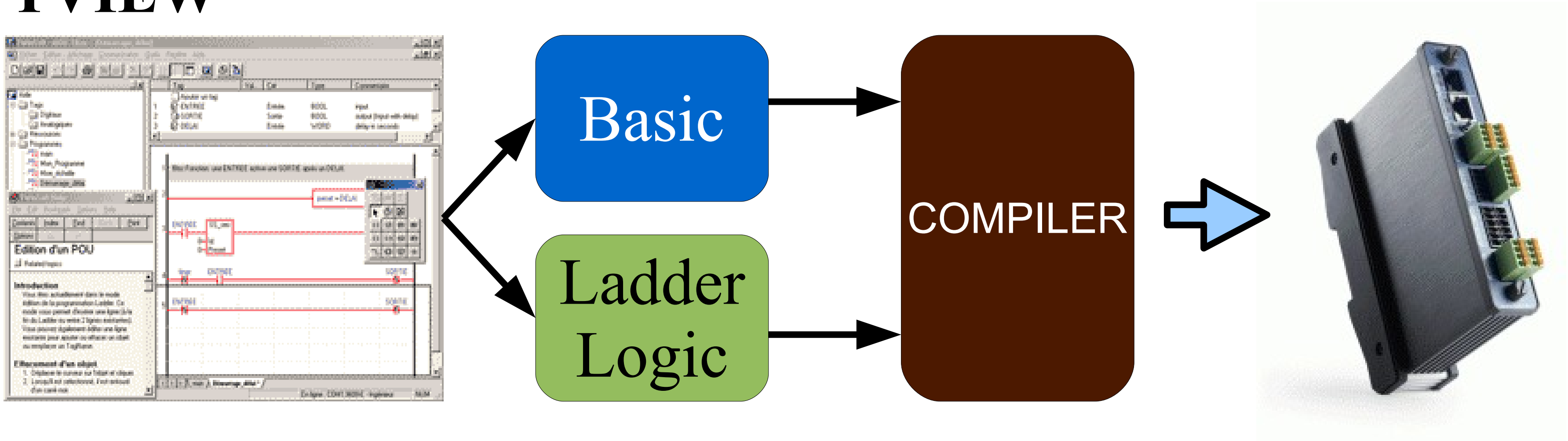
DNP3,
IEC 60870-5
MODBUS
...
+40 Drivers

http://www.cse-semaphore.com/pdf/brochure_T-BOX-Lite.pdf

4.SCADA TROJANS VI

P0WNING THE SUBSTATION IV

TVIEW

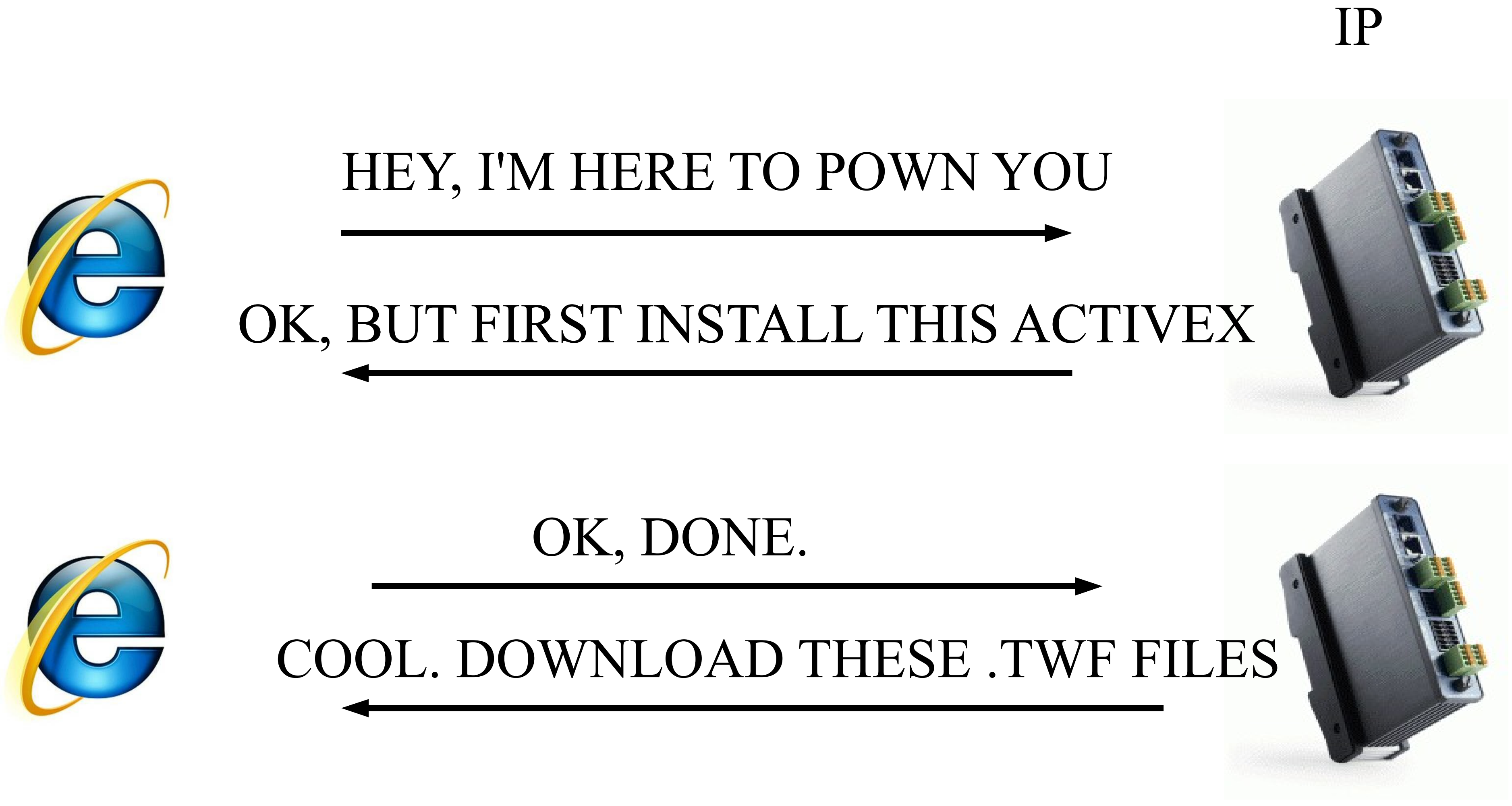


SECURITY

- MODBUS: (Optional)
  ACCESS CODE- 4 Hexa Chars.
- HTTP AUTH (Optional)
- CUSTOM PASSWORD PROTECTION VIA SOURCE CODE

4.SCADA TROJANS VI

P0WNING THE SUBSTATION V



IP

HEY, I'M HERE TO POWN YOU

OK, BUT FIRST INSTALL THIS ACTIVEX

OK, DONE.

COOL. DOWNLOAD THESE .TWF FILES

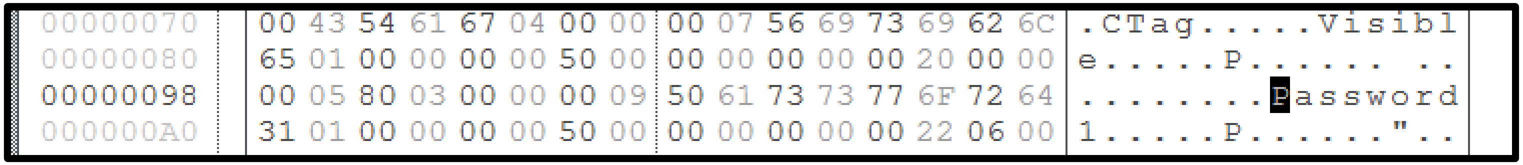
4.SCADA TROJANS VI

P0WNING THE SUBSTATION VI

TWF FILES

- Compressed
- Contains code compiled by the original programmer
- VBasic Script code → executed by vbscript.dll
- Propietary Format. Parsed by WebFormParser.dll
- Contains fixed "classes"
  - CStationList
  - CTagList
  - CTag...

Inside the TWF, each CTag entry contains its name, MODBUS address and length.



```
00000070   00 43 54 61 67 04 00 00 00 07 56 69 73 69 62 6C  .CTag.....Visibl
00000080   65 01 00 00 00 00 50 00 00 00 00 00 00 20 00 00  e.....P.......  ..
00000098   00 05 80 03 00 00 00 09 50 61 73 73 77 6F 72 64  .........Password
000000A0   31 01 00 00 00 00 50 00 00 00 00 00 00 22 06 00  1.....P......."..
```

4.SCADA TROJANS VI

P0WNING THE SUBSTATION VII

HEY, TCOMM.DLL USES MODBUS AGAINST YOU

THAT'S RIGHT. IT'S HOW YOU CAN INTERACT WITH ME

MMM, BASIC CODE IS COMPILED AND EXECUTED AT CLIENT-SIDE, EVEN AUTH ROUTINES!

WHAT IS CLIENT-SIDE?

4.SCADA TROJANS VI

P0WNING THE SUBSTATION VIII

Break on **vbscript!COleScript::Compile** to modify TWF's basic code before being compiled.

REAL EXAMPLE

```
If txt_Password.Text <> Dlb_SMSPassword.Value Or
txt_password.text = "" Then
    msgbox "The Password is incorrect!!" & vbCrlf &  "A
passord is ...." & vbCrlf & "Contact your local distributor to
get the password.",Vbexclamation,"Password"
    Exit Sub
End If
```

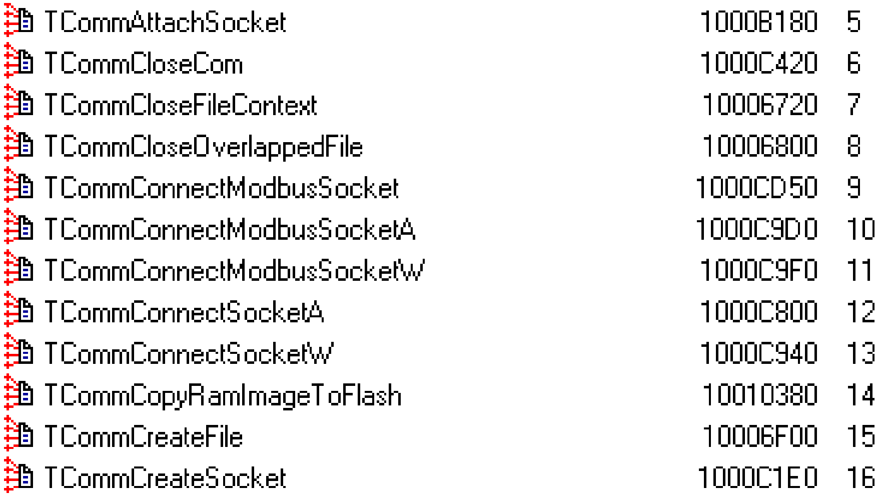
CHANGE “<>” BY “=” ... WE ARE IN!

4.SCADA TROJANS VI

P0WNING THE SUBSTATION IX

YOU REALIZE EVERYONE CAN SEND YOU RAW MODBUS REQUESTS?

DON'T BE EVIL!



TCommAttachSocket	1000B180	5
TCommCloseCom	1000C420	6
TCommCloseFileContext	10006720	7
TCommCloseOverlappedFile	10006800	8
TCommConnectModbusSocket	1000CD50	9
TCommConnectModbusSocketA	1000C9D0	10
TCommConnectModbusSocketW	1000C9F0	11
TCommConnectSocketA	1000C800	12
TCommConnectSocketW	1000C940	13
TCommCopyRamImageToFlash	10010380	14
TCommCreateFile	10006F00	15
TCommCreateSocket	1000C1E0	16

Tcomm.dll

4.SCADA TROJANS VI

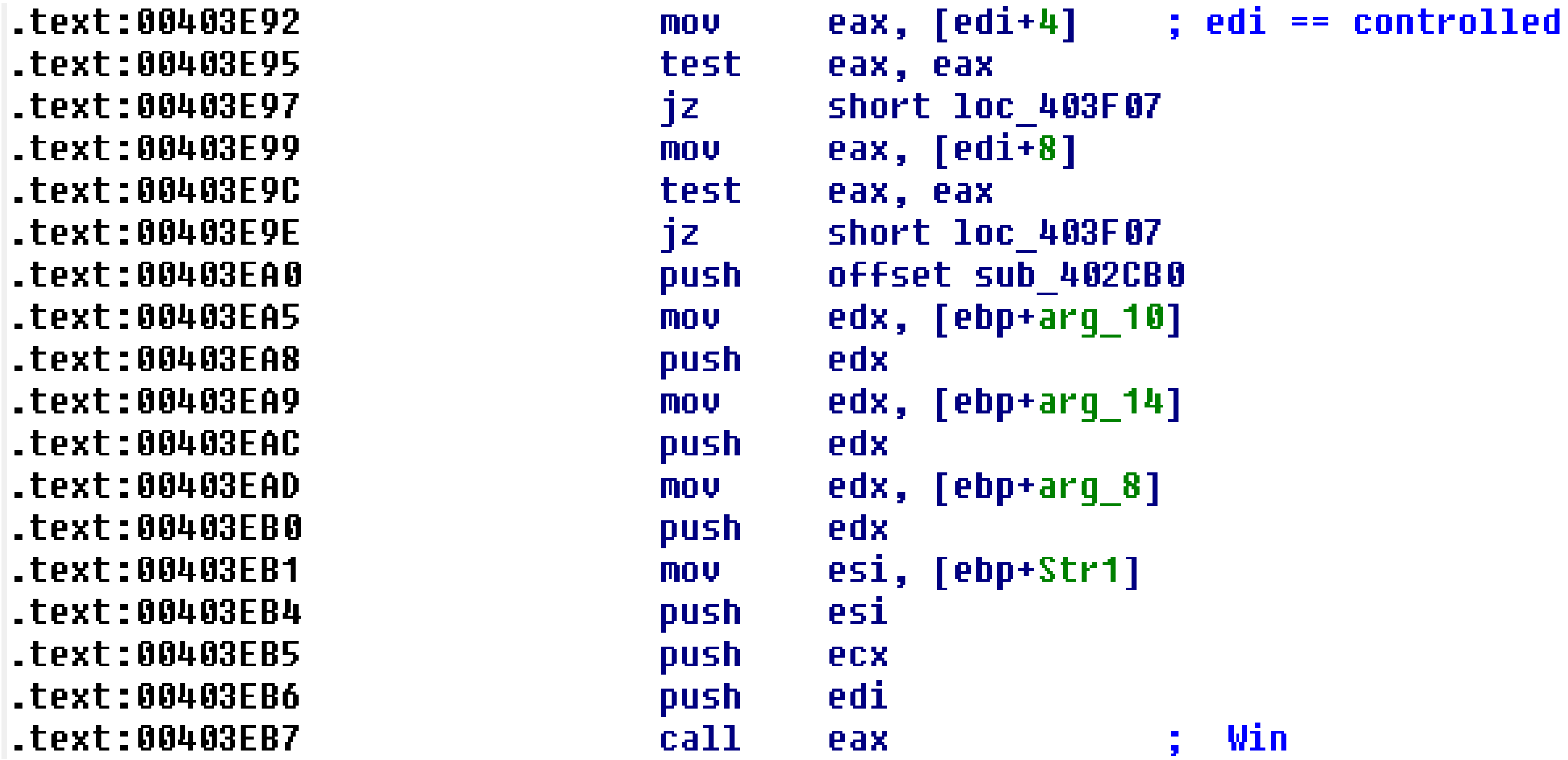
P0WNING THE SUBSTATION X

- We are already controlling Bay Level and Station Level However, still needed a vector to the EMS
- SCADA Front-End + Network Service (webvrpcs.exe)
- MIDA.plw + MIDL.exe + Opcode 0x00 + others...

```
void sub_401000(     /* [in] */ handle_t arg_1,
                     /* [in] */ long arg_2,
                     /* [in] */ long arg_3,
                     /* [in] */ long arg_4,
                     /* [size_is][ref][in] */ unsigned char *arg_5,
                     /* [in] */ long arg_6,
                     /* [size_is][ref][out] */ unsigned char *arg_7,
                     /* [ref][out] */ long *arg_8)
```

4.SCADA TROJANS VI

P0WNING THE SUBSTATION XI



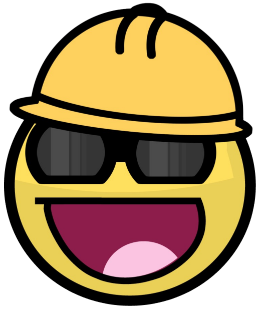
```
.text:00403E92                 mov     eax, [edi+4]    ; edi == controlled
.text:00403E95                 test    eax, eax
.text:00403E97                 jz      short loc_403F07
.text:00403E99                 mov     eax, [edi+8]
.text:00403E9C                 test    eax, eax
.text:00403E9E                 jz      short loc_403F07
.text:00403EA0                 push    offset sub_402CB0
.text:00403EA5                 mov     edx, [ebp+arg_10]
.text:00403EA8                 push    edx
.text:00403EA9                 mov     edx, [ebp+arg_14]
.text:00403EAC                 push    edx
.text:00403EAD                 mov     edx, [ebp+arg_8]
.text:00403EB0                 push    edx
.text:00403EB1                 mov     esi, [ebp+Str1]
.text:00403EB4                 push    esi
.text:00403EB5                 push    ecx
.text:00403EB6                 push    edi
.text:00403EB7                 call    eax             ;  Win
```

webvrpcs.exe port 4592

LANDED!

4.SCADA TROJANS VII

Recalling



Station/Operator p0wned via bwocxrun.ocx 0day

Bay Level p0wned via TBOX flawed logic 0day

SCADA Front-End p0wned via webvrpcs.exe RPC 0day

3 0days! Almost Stuxnet! ;)

ALL AT ONCE

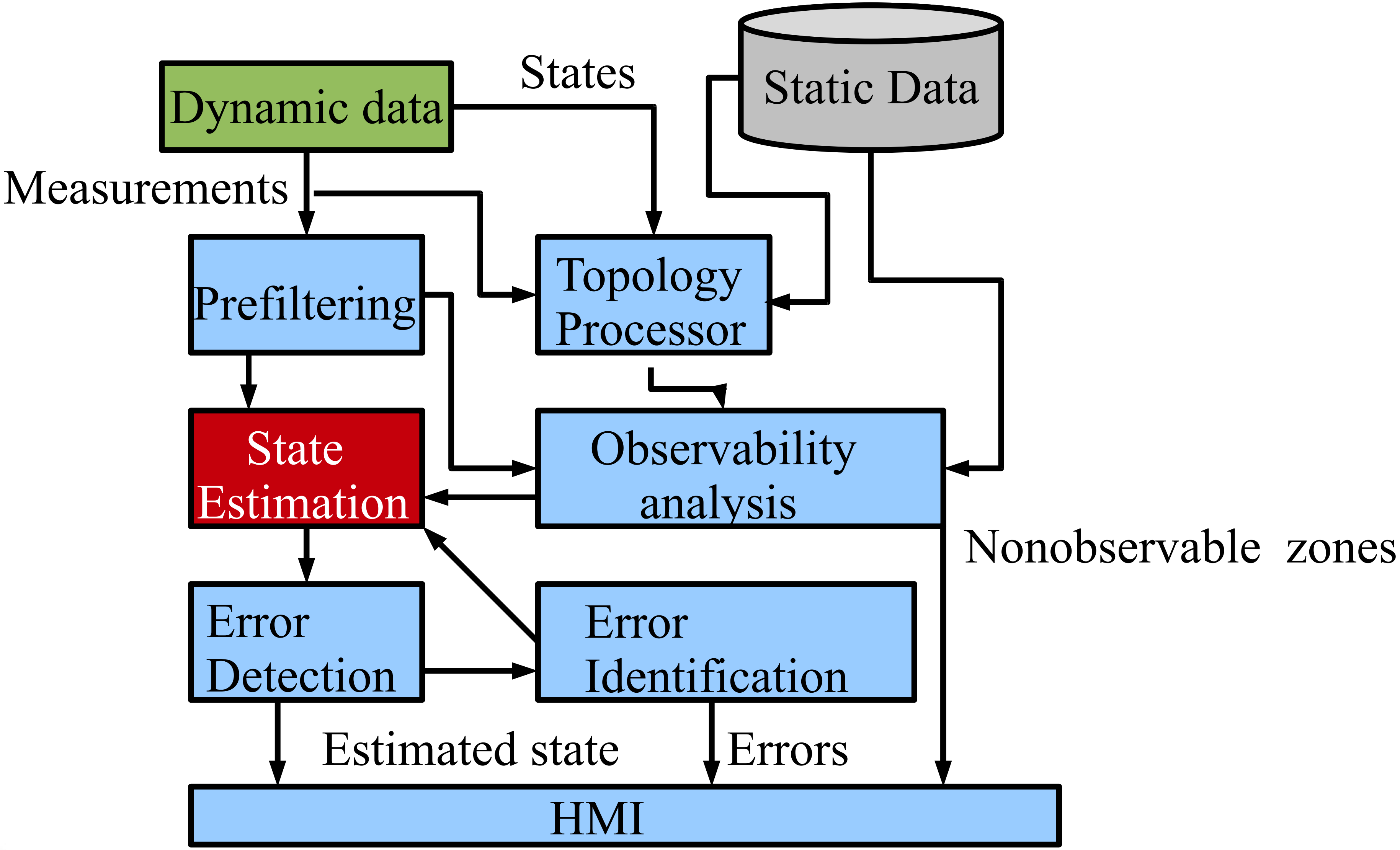
4.SCADA TROJANS VIII

THE 2nd STAGE I

- We deploy an autonomous agent to attack the State Estimator.
- Its goal is generating unexpected contingencies, which may end up causing a blackout.
- Operators will deal with fake results. Only "in memory". Everything else is correct.
- The entire EMS is no longer operating within a secure state.

4.SCADA TROJANS VIII

THE 2nd STAGE II



4.SCADA TROJANS VIII

THE 2nd STAGE III

- Why an State Estimator?

Flows → real + reactive
Injections → real + reactive
Voltage
Current
Virtual Measurements
Pseudomeasurements

4.SCADA TROJANS VIII

THE 2^{nd} STAGE IV

We can describe previous measurements as a function of the system states. h_i are nonlinear.

$$z = \begin{bmatrix} z_1 \\ z_2 \\ . \\ . \\ . \\ z_m \end{bmatrix} = \begin{bmatrix} h_1(x_1, x_2, \dots, x_n) \\ h_2(x_1, x_2, \dots, x_n) \\ . \\ . \\ . \\ h_m(x_1, x_2, \dots, x_n) \end{bmatrix} + \begin{bmatrix} e_1 \\ e_2 \\ . \\ . \\ . \\ e_m \end{bmatrix} = h(x) + e$$

4.SCADA TROJANS VIII

THE 2nd STAGE V

Given the state vector

$$x^T = [\theta_2 \theta_3 \ldots \theta_N \; V_1 V_2 \ldots V_N]$$

$$\begin{pmatrix} V_i \, , \, V_j \\ \theta_{ij} = \theta_i - \theta_j \\ G_{ij} + B_{ij} \\ b_{ij}^p \end{pmatrix}$$

The following $h_i(x)$ are used

$$\left.\begin{aligned} P_i &= \sum_{j=1}^{N} V_i V_j \left(G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij} \right) \\ Q_i &= \sum_{j=1}^{N} V_i V_j \left(G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij} \right) \end{aligned}\right\} \textbf{Injections}$$

$$\left.\begin{aligned} P_{ij} &= V_i V_j \left(G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij} \right) - G_{ij} V_i^2 \\ Q_{ij} &= V_i V_j \left(G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij} \right) + V_i^2 \left(B_{ij} - b_{ij}^p \right) \end{aligned}\right\} \textbf{Flows}$$

4.SCADA TROJANS VIII

THE 2nd STAGE VI

$\hat{z} = h(\hat{x})$ and $\hat{r} = z - \hat{z}$

$$\begin{tikzcd}
J(x) = \sum_{j=1}^{m} w_j r_j^2 \arrow[r] & J(x) = \sum_{j=1}^{m} \frac{r_j^2}{\sigma_j^2} = \sum_{j=1}^{m} \frac{(z_j - h_j(x))^2}{\sigma_j^2} \arrow[r] & J(x) = [z - h(x)]^T W [z - h(x)] \arrow[dll] \\
\cdots \arrow[d] & & \\
\Delta x^k = [G(x^k)]^{-1} H^T(x^k) W [z - h(x^k)] \arrow[r] & x^{k+1} = x^k + \Delta x^k \arrow[r] & x^{k+1} = \begin{bmatrix} \hat{x}_1 \\ . \\ . \\ . \\ . \\ . \\ \hat{x}_n \end{bmatrix}
\end{tikzcd}$$

WLS ALGORITHM

4.SCADA TROJANS VIII

THE 2nd STAGE VII

WLS BASED S.E ALGORITHM (Weighted Least Squares)

1. Initialize the state vector $x = x^0$ with the flat voltage profile ($V_i = 1$ pu, $\theta_i = 0$) and the iteration counter ($k = 0$).

2. Compute the measurement residuals $r = z - h(x^k)$.

3. Obtain H and $G = H^T W H$.

4. Solve the linear system: $\Delta x^k = G^{-1} H^T W r$

5. Update the state vector ($x^{k+1} = x^k + \Delta x^k$) and the iteration counter ($k = k + 1$).

6. If any of the elements of x exceeds the specified convergence threshold then return to step 2. Otherwise, stop.

4.SCADA TROJANS VIII

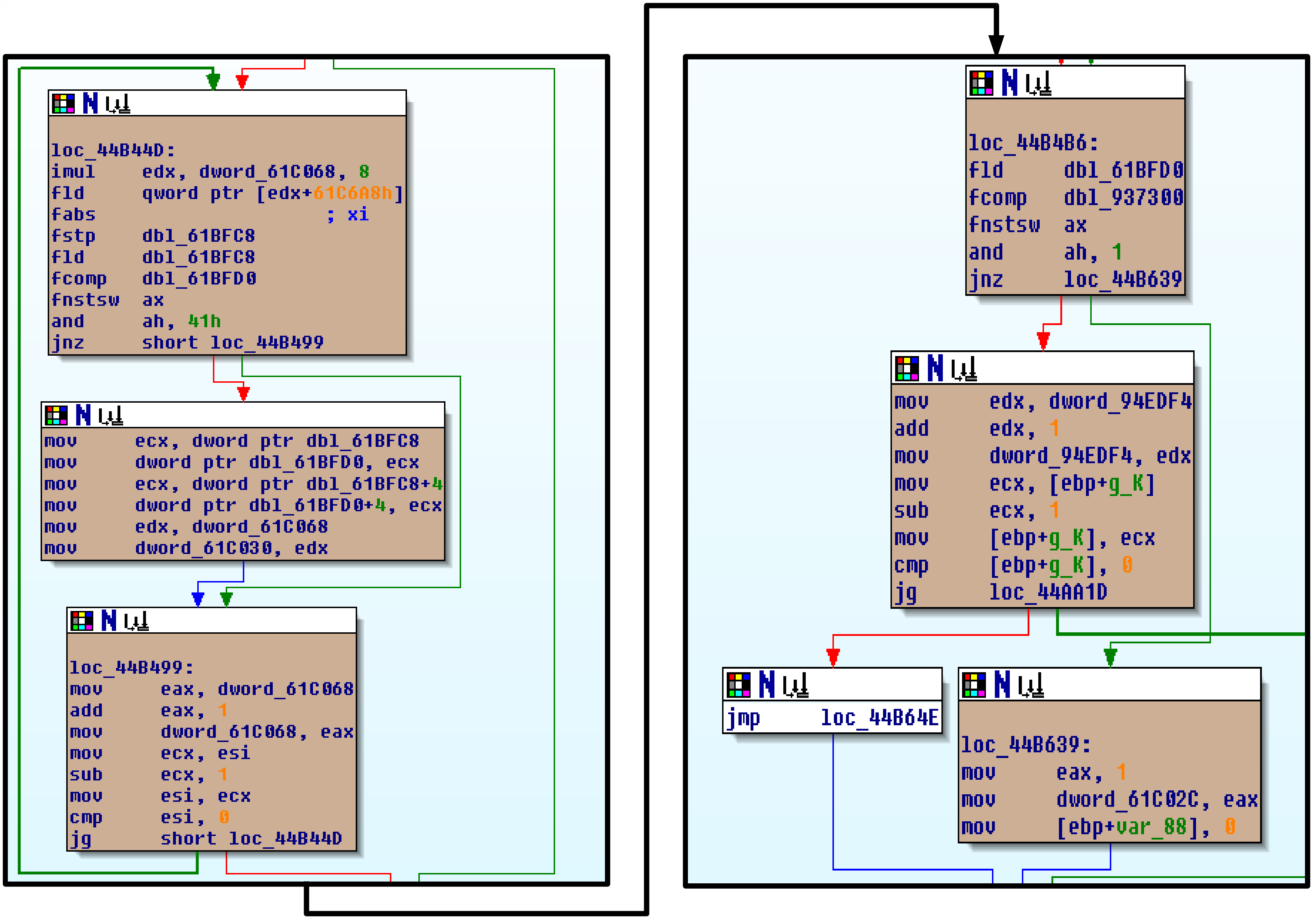
THE 2nd STAGE VIII

- Our trojan must be triggered during the WLS algorithm. So we have to reverse engineering the target EMS Software to find out where it performs the operations we have been seeing.

- Due to the complexity of EMS products, we should use tools for "differential debugging". A great/free tool is "myNav", implemented as an IDA plugin developed by Joxean Koret.

http://code.google.com/p/mynav/

```
// Step 6 - WLS Algorithm - Obtain max value from $\Delta x^k$
for ( dword_61C068[0] = 1; v9 > 0; --v9 )
  {
   dbl_61BFC8 = fabs(*(double *)&dword_61C6A8[2 * dword_61C068[0]]);
   if ( dbl_61BFC8 > dbl_61BFD0 )
   {
    dbl_61BFD0 = dbl_61BFC8;
    dword_61C030 = dword_61C068[0];
   }
   ++dword_61C068[0];
  }
  v3 = dbl_61BFD0;
  if ( dbl_61BFD0 < dbl_937300[0] )  //Max val from $\Delta x^k$  < Tolerance
  {
   dword_61C02C = 1;
   v43 = 0;
   goto No_More_iters;
  }
  ++dword_94EDF4;
  --g_K; // iterations
  if ( g_K <= 0 )
   goto No_More_iters;  // It didn't converge
```



```
loc_44B44D:
imul    edx, dword_61C068, 8
fld     qword ptr [edx+61C6A8h]
fabs                            ; xi
fstp    dbl_61BFC8
fld     dbl_61BFC8
fcomp   dbl_61BFD0
fnstsw  ax
and     ah, 41h
jnz     short loc_44B499
```

```
mov     ecx, dword ptr dbl_61BFC8
mov     dword ptr dbl_61BFD0, ecx
mov     ecx, dword ptr dbl_61BFC8+4
mov     dword ptr dbl_61BFD0+4, ecx
mov     edx, dword_61C068
mov     dword_61C030, edx
```

```
loc_44B499:
mov     eax, dword_61C068
add     eax, 1
mov     dword_61C068, eax
mov     ecx, esi
sub     ecx, 1
mov     esi, ecx
cmp     esi, 0
jg      short loc_44B44D
```

```
loc_44B4B6:
fld     dbl_61BFD0
fcomp   dbl_937300
fnstsw  ax
and     ah, 1
jnz     loc_44B639
```

```
mov     edx, dword_94EDF4
add     edx, 1
mov     dword_94EDF4, edx
mov     ecx, [ebp+g_K]
sub     ecx, 1
mov     [ebp+g_K], ecx
cmp     [ebp+g_K], 0
jg      loc_44AA1D
```

```
jmp     loc_44B64E
```

```
loc_44B639:
mov     eax, 1
mov     dword_61C02C, eax
mov     [ebp+var_88], 0
```

TRY IT YOURSELF. PET http://www.ece.neu.edu/~abur/pet.htm

5.SCADA TROJANS IX

MISSION COMPLETED

- After the successful attack, Reggaetonia suffered random blackouts for months till its own people ,tired of the situation, assaulted the institutions.

- Every attempt to contract a considerable amount of MW for reggaeton festivals, ended up in an partial blackout.

RUBENHISTAN WINS.

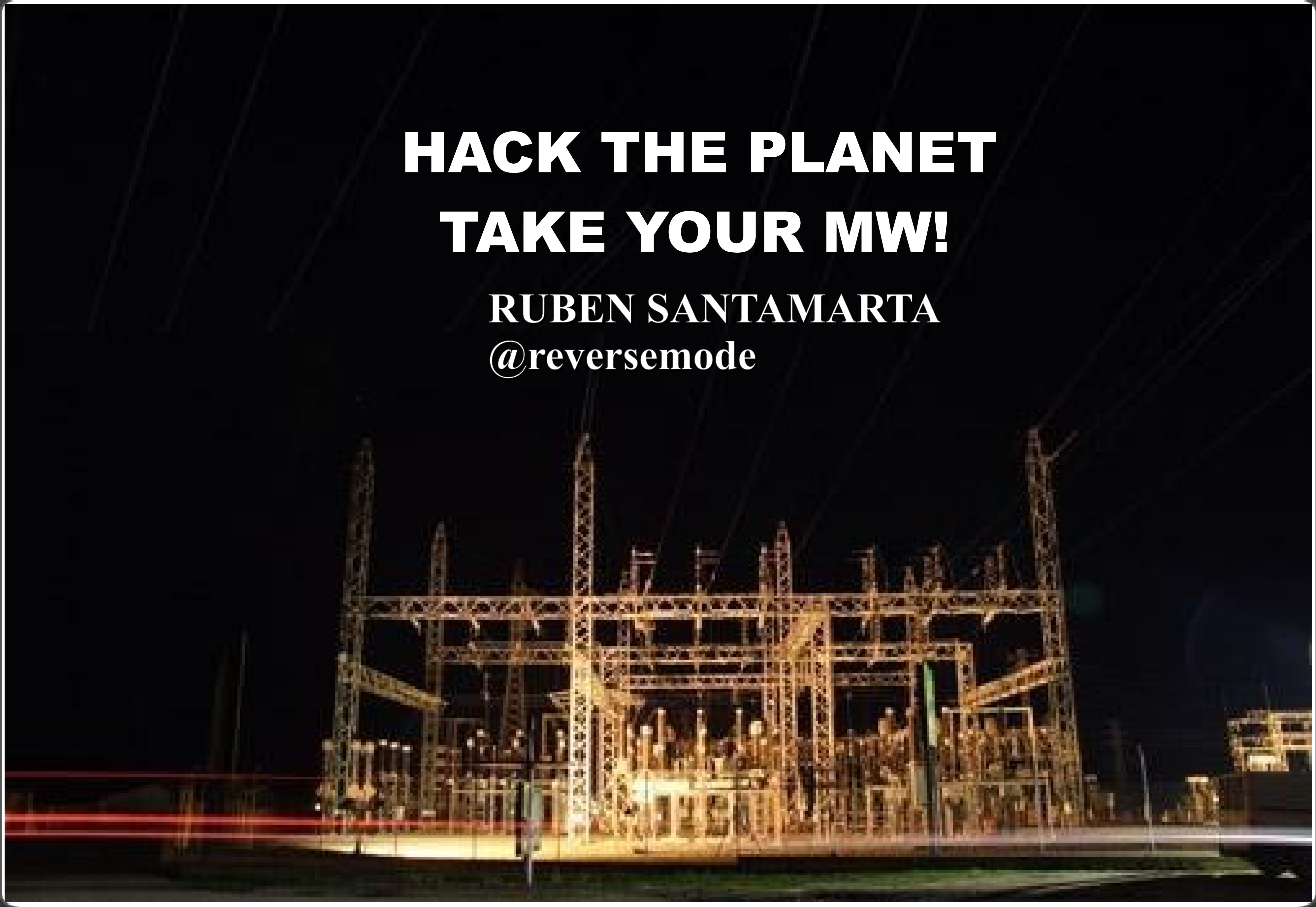
6.CONCLUSIONS

- Trojans designed for SCADA environments, should do their job stealthly,quietly... letting operators think still can trust their HMI/equipment.

- Combined attacks against State Estimators give you 100% success guaranteed. In the near future, a massive adoption of PMU could set a point of inflection.

- False data injection, nowadays, is more an academic attack than a real world attack IMHO.

- We have presented a general attack against SE.



HACK THE PLANET
TAKE YOUR MW!

RUBEN SANTAMARTA
@reversemode