



SOUTH EASTERN EUROPEAN REGION OF CIGRÉ

SEERC

AUT - BIH - GRC - HRV - HUN - ITA - MKD - MNE - ROU - SRB - SVN - TUR - UKR - CZE

Technical Advisory Committee Meeting

Problems of Information Security in Energy Objects Control Systems

Y.Bondarenko, A.Denysenko
S&T Company ENPASELECTRO, Ukraine

Prague, 15-16 March, 2017

New challenges for energy objects control systems:

- **Open standards – open and easy of access specifications**
- **Off-the-shelf hardware and software**
 - => results of convergence of IT and OT**
- **More IEDs – more telemetry information from the field – more communication links**
- **Decentralization, distributed generation, Smart Grid, microGrids - more risk of unintentional impact on power equipment**
- **Decentralization and de-corporatization – more participants with its own understanding of information security**



СЕВЕРНАЯ 330 КВ/ 110 КВ/ 10 КВ ПРИМЕЧАНИЯ

ТЗН-6 НОВО-ХИВСКАЯ ЧАСОВ

ОСШ

ОПУ 110 КВ

КАЗАРОВИЧИ ГАЗС ВЫШГОРОД-1 ВЫШГОРОД-2 ОБОЛОНЬ-2 ОБОЛОНЬ-1 ИРПЕНЬ-3 БЕЛИЧИ ОКТЯБРЬСКАЯ МИНСКАЯ

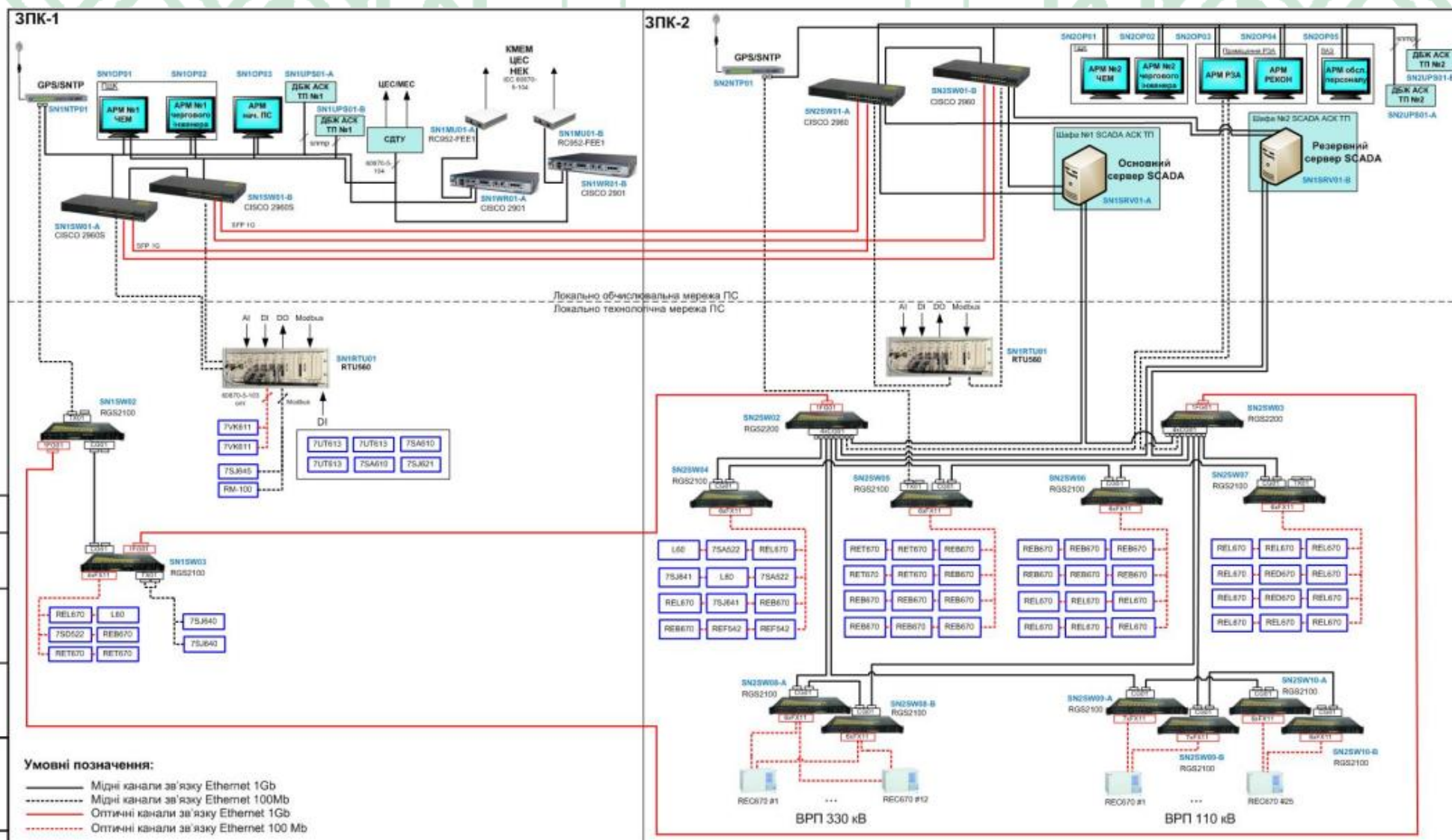
II СЕК. 330 КВ

III СЕК. 330 КВ

АТ-1 АТ-2

ОТПАЙКА ОТ ВЛ-10 ЛЮТЕЖ-Н, ПЕТРОВИЦЫ

ПРИМЕЧАНИЯ:



Cyber attack 17.12.2016:

- Infection of "TKS Energia" and SAS servers
- Spoofing of IEC 61850 (MMS) data exchange*)
- Malicious operation of CBs
- => de-energization of 145 MW in Kiev city and 48 MW in Kiev district
- Simultaneous attacks on other state and governmental organizations

*) "Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Inverter Installations", Queen's University Belfast, 2015

Cyber attack Dec.2015 (3 Oblenergo):

- **Infection of Oblenergo's information LANs via malicious emails**
- **Access to structure of information networks, SW, remote access accounts, passwords, ...**
- **Malicious operation via remote access to substation**
- **Mass calls from Russian Federation telephone numbers to numbers of oblenergo's call-centers**
- **=> short term shutdown of 227.500 consumers**

Cause of accident (2016):

- Each private distribution Company make its own control system
- Absence of general and mandatory requirements to energy utilities for IT security of automated facilities
- Lack of awareness of technological staff in cyber attacks
- No interconnection with CERT-UA (computer emergency response team)
- Insufficient hardware and IT facilities to assure protection against cyber attacks

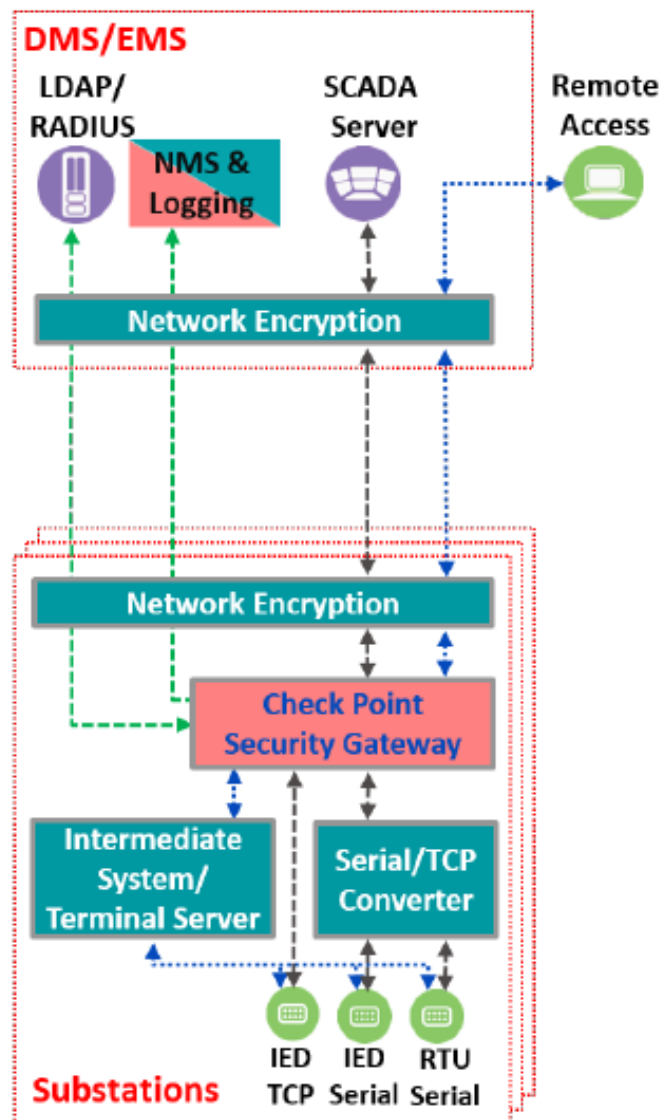
Cause of accident (2017):

- IEC 60870-5-104 and IEC 61850 vulnerability
 - Insufficient authentication of data exchange participants
 - No end-to-end data traffic protection
 - No authorizing of data access to critical resources
 - GOOSE messages are not protected
 - Insufficient logging
 - Insufficient user management access rights

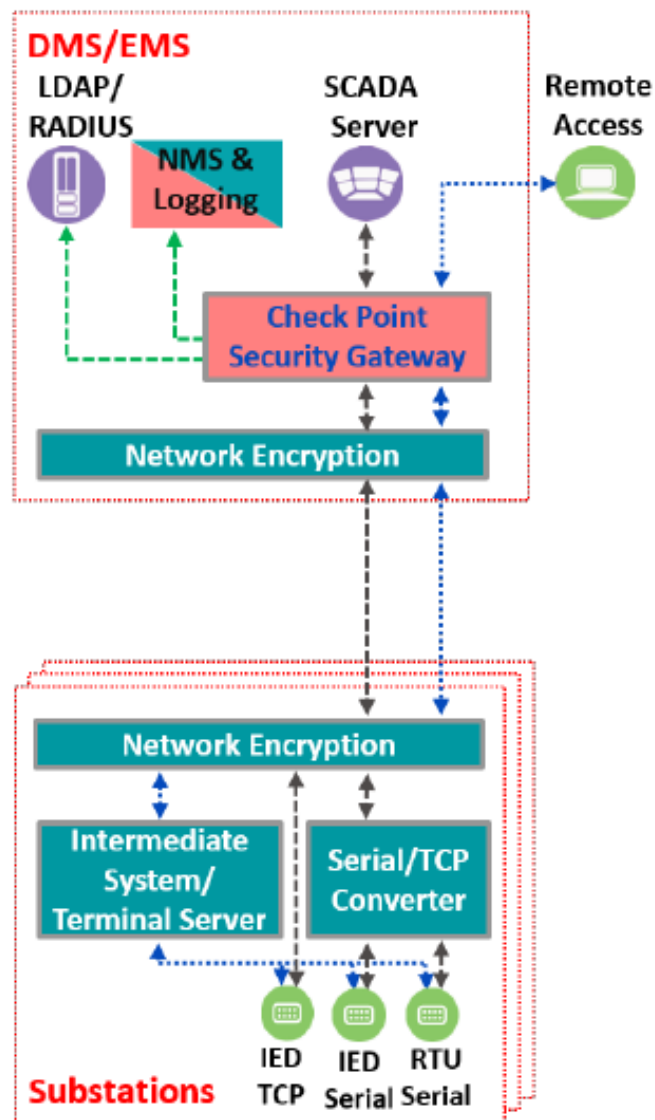
Cause of accident (2017):

- IEC 60870-5-104 and IEC 61850 vulnerability
 - Insufficient authentication of data exchange participants
 <- **IEC 62351-3 X.509 certificates**
 - No end-to-end data traffic protection
 <- **IEC 62351-3 TLS encryption**
 - MMS and GOOSE messages are not protected
 <- **IEC 62351-4 (TLS), IEC 62351-6 (VLAN)**
 - No authorizing of data access to critical resources
 <- **IEC 62351-5**
 - Insufficient logging
 <- **IEC 62351-7**
 - Insufficient user management access rights

Distributed Firewall



Centralized Firewall (Overlay Solution)



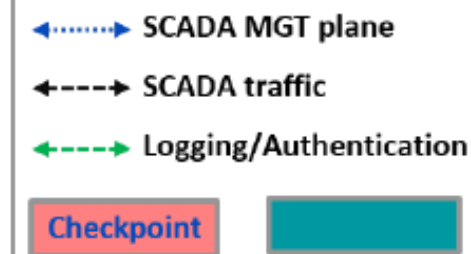
Cyber Security Networking Equipment



SecFlow
Cyber Security
Innovation of the
Year Award 2014



Megaplex
Cyber Security
Innovation of the
Year Award 2015



Centralized protection solution:

- "end-to-end" protection of telecommunications infrastructure
- Distributed (or centralized) firewall on the network perimeter

All firewalls provide:

- cryptography for standard SCADA protocols (serial and Ethernet based)
- authentication of users and software processes
 - => creating an additional layer of cyber security
- ICS Security Gateway component:
 - application management module to prevent penetration into a secure network
 - deep analysis of network packets
 - logging of ingoing and outgoing traffic

Thank you!