SCADA Maintenance and Refurbishment with Security Issue in Modern IT and OT Environment

Igor Ivanković
Croatian transmission system operator
HOPS
Zagreb, Croatia
igor.ivankovic@hops.hr

Ana Kekelj
Croatian transmission system operator
HOPS
Zagreb, Croatia
ana.kekelj@hops.hr

Renata Rubeša
Croatian transmission system operator
HOPS
Zagreb, Croatia
renata.rubesa@hops.hr

Igor Kuzle
University of Zagreb
Faculty of Electrical Engineering and Computing
Zagreb, Croatia
igor.kuzle@fer.hr

***Abstract*—When working with SCADA systems transmission system operator faces with challenges which arose from several issues that appeared over the last 10 years. SCADA system is crucial application for power system control. Refurbishment of those systems are planned usually once in a decade or even rarer. This strategy is now compromised because of intertwinement of SCADA systems with IT industries. HW platform for SCADA originates in IT world, which has different rate of technology change. With new IT landscapes, cyber security issues strongly influence the whole SCADA environment. Those facts will be presented in detail, with examples from real TSO with in depth analyses for issues with which TSO must deal in everyday business.**

Keywords—SCADA for transmission network; SCADA maintenace; SCADA refurbishment; SCADA cyber security

I. INTRODUCTION

TSO Company has crucial and strategical project of SCADA (Supervisory Control And Data Acquisition) maintenance and refurbishment, which lasts continuously, almost never-ending [1]. The reason for that is technology used in SCADA solutions from previous decade. Changes and development of IT (Information Technologies) are powerful driving momentum on market in general, strongly influencing SCADA solutions and all SCADA processes.

Cyber security issues are primary factor in those processes. New solutions have to be implemented for common IT sectors in company as for OT (Operational Technologies) sector including SCADA with all surroundings systems, subsystems and devices [2]. Such security business process inevitably influences SCADA maintenance and refurbishment.

Ultimate characteristic for SCADA system is high rate of reliability, achieving that it is a relatively long process which as a consequence means that SCADA, which is dependent on IT market environment, quickly becomes outdated in terms of operational systems and hardware. So at the beginning of new SCADA cycle in TSO Company, already "old" operational system and HW platform is installed. From this fact many challenges to daily business in TSOs arise.

This work has been supported by INEA (Innovation and Networks Executive Agency) by Grant Agreement, Connecting Europe Facility - Energy Sector Agreement No. INEA/CEF/ENER/M2016/1289177 and Croatian Transmission System Operator (HOPS).

II. ARHICTETURE OF REMOTE CONTROL IN TRANSMISSION NETWORK

Control systems in TSOs Company and also in DSOs Company today are remote based. These complex control systems have many components, systems and subsystems containing different vendors, technologies, communication solutions [3], [4] and architecture, with many of them having different year of production. Components in substations can have systems older than 20 or 25 years.

System and equipment in substations in general have very different technical solutions with some old fashioned solutions for remote control in operation, some devices and systems being even older than 30 years; For example having old RTU and AD convertors, and modern and powerfully IEDs (Intelligent Electronic Devices) in one substation.

All systems must be commissioned and put in operation in perfect order, so that the transmission network can be operated remotely from control room.

All those components can be categorized in 7 layers, bottom up, components in switchyards to visualization in control room, Fig. 1.

TSOs business process is constantly under influence from outside factors, such as electricity market, regulatory bodies, ENTSO-E (European TSO for Electricity) and others [5]. Consequence of that is constant increase in the number of SCADA measurements and indications in control room [6]. Those increases can be even 10% of total number of measurement and indications per year. Those processes are done continuously through years on existing SCADA system,

before total upgrade of the system. In time SCADA reaches the limit and total upgrade is inevitable.

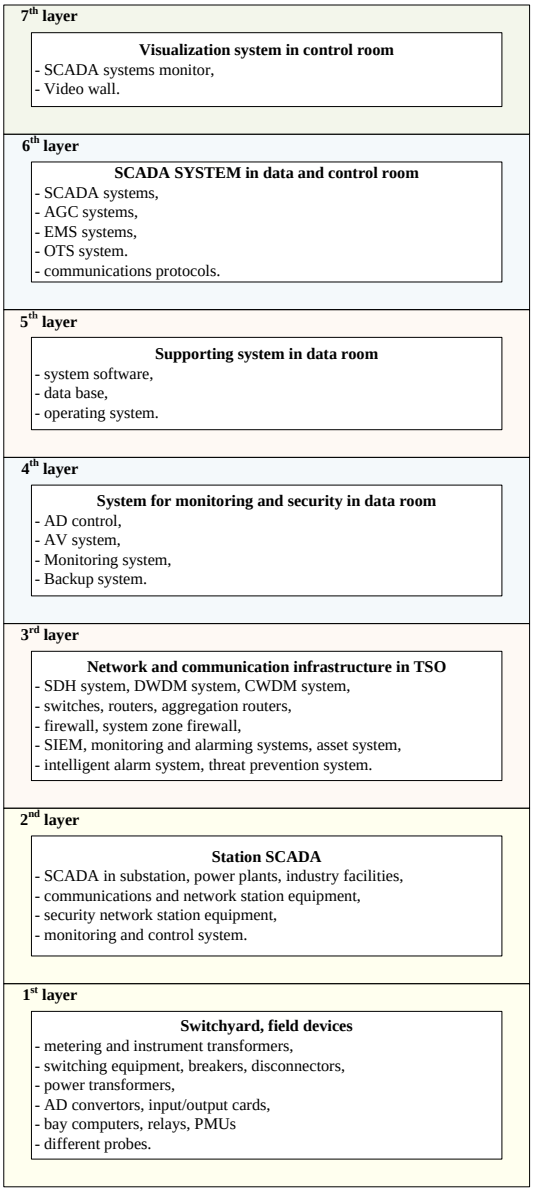

Fig. 1. Layers for complet SCADA systems, subsystem and components.

Those layers have much interference between each other and most effort should be placed for layers 4, 5 and 6 in control room for daily routine processes and some upgrades.

III. MAINTENANCE AND REFURBISHMENT

Processes for maintenance and system administrations for all layers have the following categories.

1) Preventive maintenace.

a) Periodical system check for the purpose of getting the status of the system and trying the prevent some failures.

b) Continously supervising and monitoring the system in order to find some potential failures or breakdowns in system.

2) Corective maintenace.

a) Solving and fixing the failures and others mistakes.

3) System extension.

a) Changes in transmission network (adding the new object/substations, extension of existing substation, refurbishment of primary equipment (brakers, etc.)).

b) Changes and extension of the secondary equipment (bay computer, station computer, RTUs).

4) Improving the system.

a) Developing new functionalities and improving the existing one.

b) Improving the cyber security.

5) System upgrading.

a) End of life or end of support for HW and/or SW.

b) Maintenance is too expensive

c) Extension of the system isn't possible.

Those maintenance steps are regulated in Company Rules of Maintenance. All maintenance processes are strictly enforced from SCADA personnel. Lot of commitment and time is needed in order to do maintenance on all 7 layers.

B. Upgrading the station SCADA

Activities regarding the station SCADA are not so complex in comparison to Big SCADA. On the other hand number of substations is high and standardized process has to be implemented so that the whole system runs smoothly. The fact is that the number of stations with its separate SCADA system is significant meaning there are a lot of variations of operating systems, SW and HW. In Table I. example of maintenance process complexity and necessity for compatibility of SCADA system version with Windows operating system is given. Vendor releases station SCADA in accordance to availability of Windows OS, Table I. In Table I, are presented only characteristic release for station SCADA.

TABLE I. WINDOWS OPERATION SYSTEM PER YEARS

No.	Date	Windows operation system
1.	1996/12	NT 4.0 Workstation Server
2.	2002/04	2000 Professional Server
3.	2003/06	XP Professional
4.	2010/04	Server 2003
5.	2010/04	Server 2008 Standard
6.	2010/04	Server 2008 Enterprise
7.	2112/11	Server 2008 R2
8.	2014/07	Server 2012 R2
9.	2017/09	Server 2016

It can be seen that in two decades on market at least 9 versions for station SCADA from only one vendor are released. In reality for more than 40 versions and subversions of station SCADA were released. This case present the complexity for

maintenance processes for SCADA personnel. Here must be presented also the fact that HW for station SCADA can be in operation in solid conditions (air-conditions room, etc.) for more than 15 years if you choose industrial PC.

C. Maintenance of data model in Big SCADA

TSO Company puts a lot of attention on data base in Big SCADA for two reasons. First one you need to have unified and strictly defined signals from transmission system, with which TSO accomplished total surveillance of the network and all system and subsystem [7], [8]. A second reason is that the TSO used those signal in data base for further maintenance processes of equipment [9], [10]. To add new station or group of signals the following procedure should be done, Fig. 2.

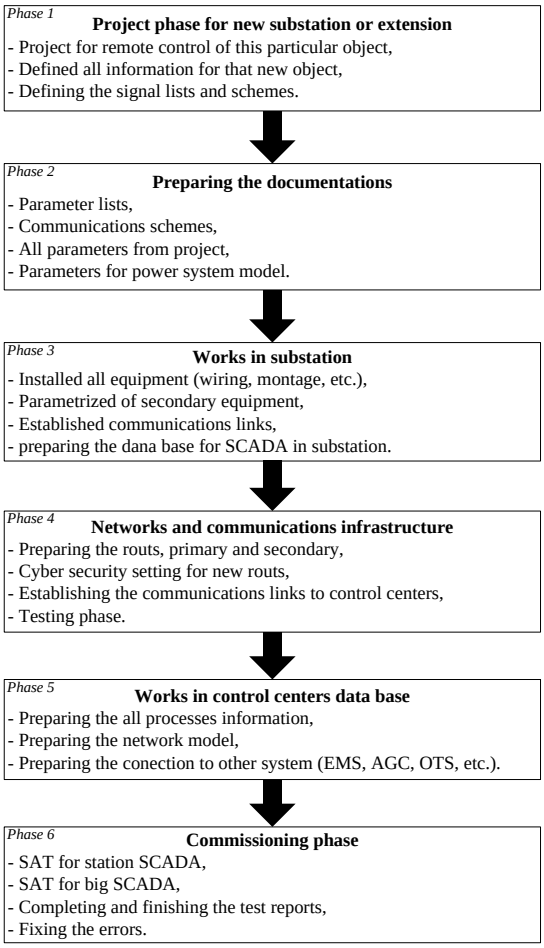

Fig. 2. Phases in all SCADA system for extension or adding the new substration object.

To add "small substation" (110 kV substation with 5 bays, 2 line bays, 2 transformer bays and coupler bay) SCADA personnel need almost 2 engineer/week of intensive work. It is very important to have finely tuned data base for Big SCADA, also because SCADA system is data source for other systems in control center.

Life time for Big SCADA system can be more than 10 years, maybe 15 years. But this life time strongly depends on life time of HW and SW platform which come from IT world. In that world, life cycle is 5 years or less. So Big SCADA personnel have great challenges to do their daily business (maintenance, upgrading and extension) under those circumstances. It is impossible to change Big SCADA every 5 years, even every 10 years that is a huge and challenging project. From experience of TSO, only in commissioning phase to do tests on all commands and signals for more than 100 substations, lasts two years.

For Big SCADA gap between releasing SCADA system and operations system is bigger than for station SCADA. In Table II., is presented situation for one SCADA vendor and vendors for operation system.

TABLE II. SCADA VENDOR AND OPERATIONS SYSTEM

No.	Operation system	SCADA version commissioning 2014	Actual SCADA version on market	New release of SCADA version
1.	Linux	Red Hat Linux 5.2	Red Hat Linux 7	Red Hat Linux 7.5
2.	Windows server	Windows Server 2003	Windows Server 2012 R2	Windows Server 2016
3.	Oracle	Oracle 10g	Oracle 12	Oracle 18
4.	Windows work station	XP Professional	Windows 10	Windows 10
5.	Office	Office 2003	Office 2016	Office 2016

Taking into account that the preparation of Big SCADA refurbishment and execution takes at least 3-4 years it is obviously that very soon the newest SCADA release will be "old" from a market perspective. Taking into account that support may be at the end of life very soon puts the whole project in risk situation. Because of that SCADA personnel are on constant pressure in maintenance phase because it is impossible to change SCADA system under market influence changes.

Daily routine testing and population of SCADA system today is strongly interfered with cyber security issues.

IV. IT AND OT SECURITY OBJECTIVES

Those two worlds of technologies in same company need to be put under one umbrella, despite of them being of very different nature, priorities, needs and business processes.

A. Different Priorities

Information technology (IT) and Operation technology (OT) differ greatly in their requirements and objectives regarding operations. IT is business critical oriented as high priority and OT have only one crucial goal, operations is mission critical. In Table III., are listed priorities for IT.

TABLE III. PRIORITIES FOR IT – BUSINESS CRITICAL

No.	IT Priorities
1.	Security focus on Data Confidentially
2.	Maximum attack impact on humans: Annoyance
3.	Security priorities: Confidentially before Availability
4.	Interruption due to security measure: Accepted.

5.	Communication behavior: Complex and often unpredictable
6.	Change Management: anytime, whenever needed
7.	Penetration tests: Active Backbox and whitebox types
8.	Equipment life cycle: 3-5 years
9.	Usual investments: 50k – 20M
10.	Processing requirements: minutes to days
11.	High throughput required
12.	Standardized architecture

List of priorities for OT is in Table IV.

TABLE IV. PRIORITIES FOR OT – MISSION CRITICAL

No.	**IT Priorities**
1.	Security focus on Process Availability & Safety
2.	Maximum attack impact on humans: Life threatening
3.	Security priorities: Availability before Confidentially
4.	Interruption due to security measures: Not accepted
5.	Communication behavior: Defined and predictable
6.	Change management: If possible only at maintenance
7.	Penetration tests: Only passive whitebox
8.	Equipment life cycle: > 15 years
9.	Usual investments: > 100M
10.	Processing requirements: miliseconds to seconds
11.	Low response time requirement
12.	Individual architecture (changing)

Priorities between those two worlds are interfering with each other. Somehow IT world can be much more easily adapted to new security requirements. In OT world there are serious limitations for upgrading to new requirements of cyber security.

B. *OT strategic objectives and principles*

One of security principles, which should be implemented for SCADA system, is a concept of perimeter, Fig. 3.

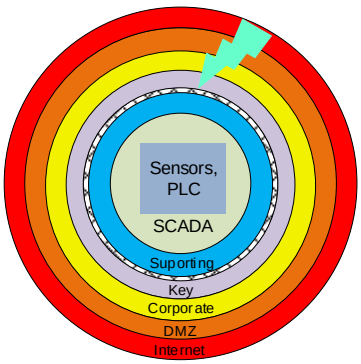

Fig. 3. Concept of perimeter.

Good perimeter protection is the surest way to secure systems and data. "Onion strategy" with more protective layers, gives better solutions for protecting SCADA system. Following that philosophy, the number of most protected systems in Company (SCADA system) should be limited.

That approach is used in many different ways through Company. It strongly influences physical and logical architecture, flow of commands and data, detecting and responding to incidents.

OT cyber security combines and targets different areas that are a part of Company's strategy. Security anomaly detection is a key component for strengthening incident detection and response capabilities. OT's strategic objectives in principle have five crucial parts.

1) Broadening the Cyber Security perimeter in the Digital Grid and Mission critical Systems.

a) Coverage of all Digital Grid assets from a cyber and physical security perspective (priority for substations systems, subsystems andg devices).

b) End-to-end control and monitoring of assets and related events.

2) Strengthening incident detection, response and recovery capabilities.

a) Reducing organization risk by reducing the potential impact of cyberattacks.

b) Improving procedures to reduce detection and recovery time after cyberattacks.

3) Ensuring Cyber Security Standardization and compliance with company policy.

a) ISO27001 standard adoption and continued risk management.

b) Compliance with applicable regulations under the scope of Cybersecurity and Privacy.

4) Enabling employees as the 1st line of Defense (training and awareness).

a) Developing Cybersecurity awareness culture on all employees.

b) Advanced training of cybersecurity teams.

5) Strengthening national and international partnership for info-sharing & best practices.

a) Improved ability to detect and respond to incidents with inter-organizational impact.

b) Continuous updating of cybersecurity benchmarking and collaboration.

C. *IT and OT connections*

IT and OT systems in Company are two different ones that are organized and run independently but there are connected through some predefined paths for data exchange, Fig. 4. Data from OT part should be transfer to IT part for further processing in other business applications (security N-1 planning, scheduling, Data warehouse (DWH), transparency platform, etc.).

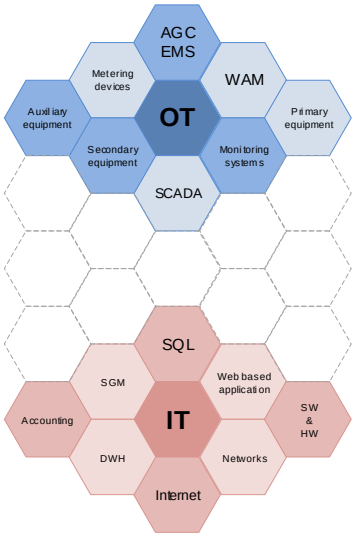

Fig. 4. Present light interweaving between OT and IT

Pressure from integration between many IT levels and applications so that company users will have data available from all IT devices may arise in future. Also some kind unidirectional data flow may be changed and moderated to bidirectional flow to all company IT devices, Fig. 5.

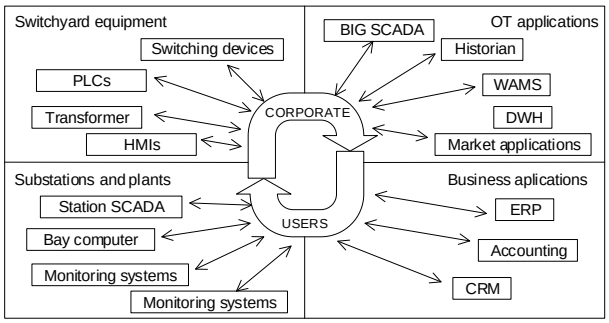

Fig. 5. Possible future strong interweaving between OT and IT

Data from multiple devices and locations will be instantly accessible to entire enterprise.

D. Evolutions of needs and influencers

Company IT and OT technology constantly progresses and evolves. Those changes are driven from outside world and also from company's inside needs and developments.

Evolution of needs can be summarized in the following:

- OT staff needs to have access to both networks.
- Office applications for flow predictions.
- Office tools incorporated to SCADA systems.
- Remote support for OT through internet.
- Near real-time reporting of flow data, transparency regulations.
- Flow demands of data to OT engineers for flow scheduling.
- Metering data to commercial applications.
- HW setup becomes complex. Only IT & network engineers can support it.

Second driving factor is evolutions of influencers, with the following main aspect.

1) More technology in OT.

a) New types of increased intelligence in traditional devices.

b) More in everything.

2) More technology in IT.

a) Incrrease in quality & quantity.

b) Pervasive IT in daily routine.

c) Virtul machines and cloud.

3) More technology in communications.

a) Easy implementations.

b) Inexpensive solutions.

c) Huge capacities.

Today company culture for an OT and IT are actually based on needs and wishes from three different groups of employees. Those groups have at the end same goal, they want to control, develop and improve business processes based on platform and data from OT and IT world. OT group have focus on the following, Table V.

TABLE V. FOCUS IN A WORLD OF OT

No.	Features
1.	Designed for controlling things
2.	Focus in process control
3.	Scope is providing detailed instructions to machines
4.	Communicate plans to automation
5.	Accommodate multiple protocols & equipment interfaces
6.	Diverse asset specific policies, risk includes loss of data & life

IT group are focused on following, Table VI.

TABLE VI. FOCUS IN A WORLD OF IT

No.	Features
1.	System design assumes human as the endpoint
2.	Focus in making money
3.	Scope is cross-functional orchestration of supply chain
4.	Consolidate view across multisite network
5.	Enforce standard interface in an ERP
6.	Homogeneous policies, primary risk is loss of data

And at the end, the third group, company managers have their own goals, but also based on data from OT and IT company world, Table VII.

TABLE VII. FOCUS IN A WORLD OF MANAGEMENT

No.	Features
1.	Manage vs control brings value
2.	Measure productivity/product
3.	Aggregate & disaggregate
4.	Centralize & distribute consistency
5.	Integrate & interoperate
6.	Cybersecurity

All three groups are highly dependent on IT and OT technology and they must manage it.

E. IT-OT common ground

Besides the many difference in technology, technical solutions and business process they have common ground, which should be paid attention to in the future. That common ground is very important and IT and OT world should implement them in nearest future or in new solutions.

1) Encryption.

a) For all communications between devices to ensure privacy of data transmitted.

2) Authentication.

a) Identifying and authenticating all devices and machine within the system to ensure only approved devices and systems are communicating with each other.

b) Mitigate the risk of a hacker inserting untrusted devices into the network and taking control of any systems or machines.

3) Integrity.

a) Ensuring integrity of the data generated from these systems.

4) Upgrades.

a) Perform remote upgrades to software and ensure integrity of those updates.

V. CONCLUSION

Ownership of technologies and management of people for those OT and IT world should be adopted or reorganized or redesigned. In those processes budgets should be redistributed and supervision will be improved.

IT department supports client business units within enterprise staffed only during primary or extended business hours. OT is a core business. Staffing is 24x7 reflecting the nature of critical infrastructure.

Different emphases are put on avoiding failures, because of different impact of IT and OT.

IT serves the needs of the many: sharing/storing/analyzing/manipulating data. OT brings reliability, predictability & resilience above all.

OT is too skeptical about changes that IT considers part of daily routine. Network scanning, patching operating systems & installing AV software, are considered low risk/daily routines activities by IT, so as to minimize risk, data leakage & close vulnerabilities. OT views the same processes as potential causes of downtime.

Both IT and OT are vulnerable to attacks. It should be brought under consideration to deploy multilayer cybersecurity defense measures under universal cybersecurity policy.

In future SCADA personnel will face with aspect driven by market of IT world and vendors, and cyber security issues. When will be established equilibrium for OT requirements and IT technology it is hard to predict; before that moment some solutions in Big SCADA maintenance and refurbishment should be proposed.

REFERENCES

[1] P. A. Graullera, "Architecture Design and Interoperability Analysis of a SCADA System for the Power Network Control and Management," Degree Project in Mechatronics, KTH Royal Institute of Technology, Stockholm, June 2017

[2] R. C. Borges, H. Goseva-Popstojnova, K. Goseva-Popstojnova, "Characterization of Cyberattacks aimed at Integrated Industrial Control and Enterprise Systems: A case study," 2016 IEEE 17th International Symposium on High Assurance Systems Engineering, pp. 1-9, IEEE Computer Society, 2016

[3] Y. Yan, Y. Qian, H. Sharif, D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," IEEE Communications surveys & Tutorials, January 2013, DOI: 10.1109/SURV.2012.021312.00034

[4] S. Mohagheghi, J. Stoupis, Z. Wang, "Communication Protocols and Networks for Power Systems-Current Status and Future Trends," 2009 IEEE/PES Power Systems Conference and Exposition, April 2009, pp. 1-10

[5] S. Dević, I. Luković, "Development of a Database for the Common Information Model of Power Grids," ITC 3/46, Journal of Information Technology and Control, Vol. 46, No. 3, 2017, pp. 319-332, DOI 10.5755/j01.itc.46.3.14340

[6] O. Pohl, F. Rewald, S. Dalhues, P. Jöke, C. Rehtanz, C. Wietfeld, A. Kubis, R. K. Tamgue, D. Kirsten, "Advancements in Distributed Power Flow Control," IEEE, pp. 1-6, 2018

[7] N. Baranović, P. Andersson, I. Ivanković, K. Žubrinić-Kostović, D. Peharda, J.E. Larsson, "Experiences from Intelligent Alarm Processing and Decision Support Tools in Smart Grid Transmission Control Centers", CIGRE Session 46, 21-26 August 2016, Paris, France, paper D2-112

[8] M. Perkov, N. Baranović, I. Ivanković, I. Višić, "Implementation strategies for migration towards smart grid", Powergrid Europe 2010, Conference & Exhibition, 8-10 June 2010, RAI, Amsterdam, Netherlands, Session 3, Grid evolution I

[9] Z. Gajić, I. Ivanković, B. Filipović-Grčić, R. Rubeša, "New General Method for Differential Protection of Phase Shifting Transformers", 2nd International Conference on Advanced Power System Automation and Protection, Jeju-South Korea, 24-27 April 2007

[10] I. Ivanković, D. Peharda, D. Novosel, K. Žubrinić-Kostović, A. Kekelj, "Smart grid substation equipment maintenance management functionality based on control center SCADA data", CIGRÉ Session 47, 26-31 August 2018, Paris, France, paper B3-211, pp 1-10