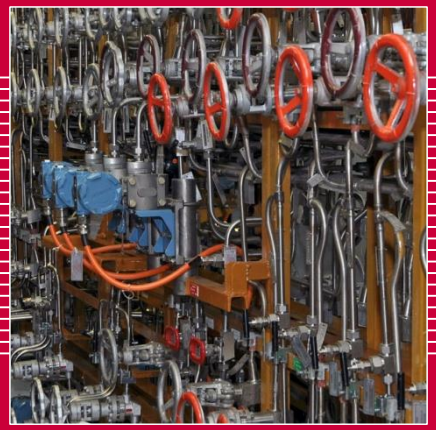
I&C Energo a.s.

reliable partnership since 1993



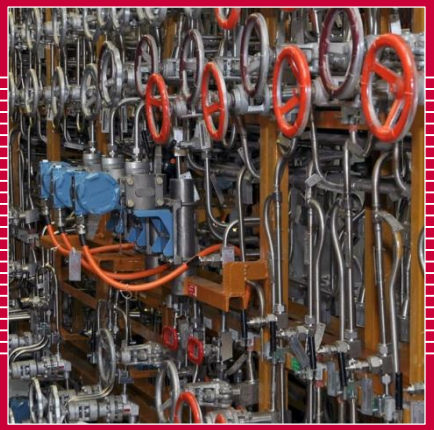
I&C Energo a.s.

The current situation and development of securing ICS, SCADA systems

Lukáš Obořil, Head of Software for Control and Safety Systems Department

4.11.2019



THE CURRENT SITUATION AND DEVELOPMENT OF SECURING ICS, SCADA SYSTEMS

- THE CURRENT SITUATION OF SECURING ICS, SCADA
- NEW CHALLENGES AND VISIONS FOR ICS, SCADA

THE CURRENT SITUATION AND DEVELOPMENT OF SECURING ICS, SCADA SYSTEMS

OT – OPERATIONAL TECHNOLOGY

- ICS – INDUSTRIAL CONTROL SYSTEM
  - PLC – Programmable Logic Controller
  - RTU – Remote Terminal/Telemetry Unit
  - HMI – Human Machine Interface
- SCADA/DCS
  - Distributed Control System
  - Supervisory Control And Data Acquisition System
- SIS – SAFETY INSTRUMENTATION SYSTEM

WE HAVE BEEN DOING SOFTWARE MODIFICATIONS SINCE 2005 FOR THESE SYSTEMS

CURRENT SITUATION OF SECURING ICS, SCADA

HOW THE UTILITIES REFLECT HIGHER NEED FOR CYBERSECURITY AND HOW THEY DEAL WITH IT ?

- **PROS**
  - **Legislation – 181/2014 Sb., ISO 27001 (27019), IEC 62443, IE 61226, IEC 60880, various NIST guidelines.**
  - **Cybersecurity requirements are included in tender documentation for new systems and for upgrades as well.**
  - **Higher demand for cybersecurity documentation.**
  - **Cybersecurity tests are integral part of supply.**
  - **Higher requirements for network architecture and network safety.**
  - **Some utilities have cybersecurity guidelines and have setup for scanners according to those guidelines.**
  - **Periodic scans**
  - **Awareness about ICS, SCADA, SIS monitoring**
  - **Crypto, VPN, Firewall**

CURRENT SITUATION OF SECURING ICS, SCADA

- **CONS**
  - **Utilities must be made more greatly aware of the need for ongoing further cybersecurity training.**
  - **ICS, SCADA, SIS monitoring is still very weak or missing completely.**
  - **No SIEM.**
  - **Not enough human resources for cybersecurity.**
  - **Lots of ancient communications channels in/out ICS, SCADA.**
  - **Firewall mantra.**
  - **Air-gap mantra.**
  - **Buying “Cybersecurity solution out of the box” mantra.**
  - **Do NOT touch if it is working mantra - > missing updates and patches.**
  - **Really old systems (hardware, software) – long lifecycle.**
  - **Testing environment**

NEW CHALLENGES AND VISIONS FOR ICS, SCADA, SIS

- **SYSTEM ARCHITECTURE AND NETWORK DESIGN**
  - Cybersecurity by design.
  - Advanced system architecture – Clusters, redundancy, thin clients.
  - Use well known suppliers and vendors. Don't trust blindly. *(ICE case)*
  - Advanced network devices as DATA DIODS, ADVANCED PERIMETER FIREWALLS, specific firewalls.
  - Monitoring must be integral part of new systems + SIEM.
- **PATCH AND UPDATES MANAGEMENT**
  - Test environment
  - Every box has software inside ! Keep in mind, they need to be monitored and patched properly, even firewalls ! *(VxWorks case)*
- **REMOTE ACCESS**
  - Use state of the art crypto and assign access carefully. Don't forget revoke access ! *(Avast case)*
  - Monitor everything

NEW CHALLENGES AND VISIONS FOR ICS, SCADA, SIS

- **OPERATING SYSTEM OR WITHOUT ?**
  - Traditional Windows, Linux, Unix (BSD, Solaris, Aix).
  - No OS inside.
  - RTOS (QNX, VxWorks, PikeOS, atd …).
- **CPU OR NOT ?**
  - Traditional CPU like Intel, AMD or commercially available.
  - ARM - specific design based.
  - FPGA - future for SIS!
- **HUMAN FACTOR**
  - Strongest and weakest part of our portfolio.
  - Lazy human nature. *(SIS - Triconex – Trisis case)*
  - Monitor everything.

Thank you for your attention !

Lukáš Obořil, Head of Software for Control and Safety Systems Department

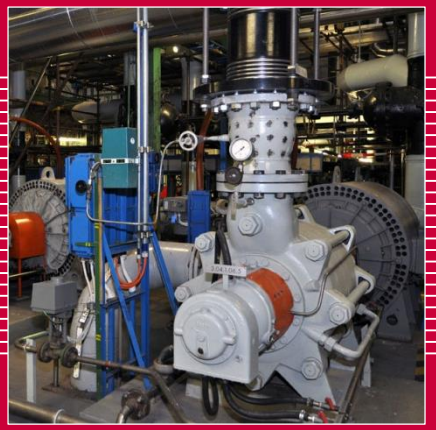
Power Production Optimization Division, I&C Energo, a.s.

E loboril@ic-energo.eu M +420 725 007 048

I&C Energo a.s., Nuclear Power Plant Temelín,

Czech Republic

REFERENCES



SELECTED REFERENCES OF POWER PRODUCTION OPTIMIZATION DIVISION 1/7

Information systems: (Note: reference title, end customer/investor, implementation from – to)

Asset management/Equipment ageing management (Plant Life Management - PLIM):

- **LTO Suite data support (services);** CEZ, a. s., Production Division (2014 - present)
- **LTO Suite upgrade;** CEZ, a. s., Production Division (2013 - present)
- **Equipment reliability evaluation - consultations, methodical and analytical services;** CEZ, a. s., Production Division (1995 - present)
- **Materials database ;** CEZ, a. s., Production Division (2014)
- **Valves diagnostic system ;** CEZ, a. s., Production Division (2014)
- **Central measuring equipment register - "CEM";** Teplarny Brno, a.s. (Brno Heating Company) (2010 - 2011)
- **Central SW system for LTO Project (Long Term Operation) - SW product name "LTO Suite";** CEZ, a. s., Production Division (2009 - 2011)
- **TRAMON - TRAnsformer MONitoring system;** CEZ, a. s., Dukovany NPP (2008 - present), Temelin NPP (2009 - 2010)
- **I&C equipment reliability monitoring system - "SSS";** CEZ, a. s., Production Division (2007 - 2009)
- **Power plant equipment monitoring information system - "TechMon";** CEZ, a. s., Production Division (2002 - 2008)
- **Reliability information system - "SIS";** CEZ, a. s., Production Division (1999 - 2004)

Asset management/Maintenance management 1/2:

- **Asset Suite release 6 to release 8 upgrade and integration;** CEZ, a. s., Production Division (2015 - present)
- **Consolidation of power plant SW solutions - "Power Plant Communication System - KSE";** CEZ, a. s., Production Division (2010 - 2014)
- **Asset Suite release 8 translation;** CEZ, a. s., Production Division (2013)
- **Upgrade of Asset Suite x FileNet integration;** CEZ, a. s., Production Division (2013)
- **Asset Suite release 6 EAM system implementation and integration;** CEZ, a. s., Production Division (2007 - 2010)
- **PassPort x SAP integration;** CEZ, a. s., Production Division (2007 - 2008)
- **PassPort x Primavera x PlantSchema/AXSYS Engine integration - "Communication System of Coordination - KSK";** CEZ, a. s., Temelin NPP (2006 - 2008)
- **PassPort x FileNet integration;** CEZ, a. s., Production Division (2005 - 2006)
- **PassPort EAM system implementation;** CEZ, a. s., Production Division (1995 - 2001)

SELECTED REFERENCES OF POWER PRODUCTION OPTIMIZATION DIVISION 2/7

Asset management/Maintenance management 2/2:

- **KKS code, creation and digitalization of technological schemas;** Prazska teplarenska, a.s. (Prague District Heating Company) (1996 - 2009)
- **KKS code, creation and digitalization of technological schemas;** CEZ, a. s., Production Division (1995 - 2002)

Document management:

- **Operational documentation management system - "PREV-DOK";** Slovenske elektrarne, a.s. (2012 - 2014)
- **Analysis and optimization of document management process and SW support;** CEZ, a. s., Production Division (2013)
- **Facility drawing documentation and related SW tools migration from PlantSchema to AXSYS.Engine;** CEZ, a. s., Dukovany NPP (2012), Temelin NPP (2012)
- **Consultations and target concept of cPLM (capital Project Lifecycle Management);** SKODA PRAHA Invest s.r.o. (2011)
- **Electronic drawings browser - "CRD";** CEZ, a. s., Dukovany NPP (2010)
- **Design Analysis Re-engineering Tool - "DART";** CEZ, a. s., Dukovany NPP (2009), Temelin NPP (2009)
- **Operational documentation management system - "ISSPD";** CEZ, a. s., Dukovany NPP (2004 - 2005), Temelin NPP (2007 - 2009)

Data warehouses & Technological information systems 1/2:

- **DIAG communication and calculation server within the Dukovany NPP M3,4,5 I&C system modernization project;** CEZ, a. s., Dukovany NPP (2008 - present)
- **Upgrade of NLAN (Wonderware platform);** CEZ, a. s., Dukovany NPP (2014 - 2016)
- **Company process (technological) data warehouse (OSIsoft/PI System platform);** ArcelorMittal Ostrava, a.s. (2015)
- **Central process (technological) data warehouse - "CUTD" (OSIsoft/PI System platform);** CEZ, a. s., Production Division (2011 - 2014)
- **NLAN extension of the data from selected substations;** CEZ, a. s., Dukovany NPP (2013)
- **Central data warehouse - CDS (Oracle platform);** CEZ, a. s., Production Division (2010 - 2011)
- **Process (technological) data warehouse - "STD" (Oracle platform);** CEZ, a. s., Production Division (2001 - 2009)
- **Process (technological) data repository and process information system - "NLAN" (Wonderware platform);** CEZ, a. s., Dukovany NPP (2002 - 2009)

SELECTED REFERENCES OF POWER PRODUCTION OPTIMIZATION DIVISION 3/7

Data warehouses & Technological information systems 2/2:

- **PCS (Process Computer System) communication and calculation server within the Dukovany NPP M1,2 I&C system modernization project;** CEZ, a. s., Dukovany NPP (2001 - 2009)
- **Communication and calculation server within the Technological Computer System - "TPS";** Slovenske elektrarne, a.s., Jaslovske Bohunice NPP (2005 - 2008)
- **Central diagnostic system (Wonderware platform);** CEZ, a. s., Dukovany NPP (2005 - 2007)
- **Emission monitoring system - "EMON";** CEZ, a. s., Production Division (2005 - 2007)
- **Process (technological) data acquisition and archival system for NPP units physical and power start-up - "STDAS" (Wonderware platform);** CEZ, a. s., Temelin NPP (2000 - 2001)

Development of „tailor-made“ software solutions:

- **Upgrade of Chemis;** CEZ, a. s., Dukovany NPP, Temelin NPP (2015 - present)
- **TTChange – Information system for I&C change management in Westinghouse Technology Transfer process;** CEZ, a. s., Temelin NPP (2014)
- **TTMagic – Software tools for I&C change implementation in Westinghouse Technology Transfer process;** CEZ, a. s., Temelin NPP (2013 - 2014)

Control systems:

Technological process automation 1/2:

- **Modernization of the I&C system - auxiliary systems;** CEZ, a. s., Dukovany NPP (2015 - present)
- **Modernization of the I&C system - modules M3,4,5 (ZAT platform);** CEZ, a. s., Dukovany NPP(2009 - present)
- **SW modifications of the PRPS, PAMS, RCLS safety systems - Westinghouse Technology Transfer (EAGLE 21 platform);** CEZ, a. s., Temelin NPP (2006 - present)
- **UIS (Unit Information System) Integration and UIS display modifications - Westinghouse Technology Transfer;** CEZ, a. s., Temelin NPP (2004 - present)
- **SW solution for planning and recording of power plant units output regulation;** CEZ, a. s., Dukovany NPP (2004 - present)

SELECTED REFERENCES OF POWER PRODUCTION OPTIMIZATION DIVISION 4/7

Technological process automation 2/2:

- **SW solution for transmission network ancillary services;** CEZ, a. s., Dukovany NPP (2004 - present)
- **Design and modifications of the PCS, TCS, TPS systems application SW - Westinghouse Technology Transfer (WDPF 9.0 platform);** CEZ, a. s., Temelin NPP (2002 - present)
- **Independent verification and validation of safety and safety related systems;** CEZ, a. s., Temelin NPP (1999 - present)
- **Upgrade of HSR (Historical Storage and Retrieval) servers (platform Oracle ZFS Storage 7120, IBM TS3200, IBM Power platform);** CEZ, a. s., Temelin NPP (stage 1: 2013 – 2014, stage 2: 2015 - 2016)
- **Complex modernization of classical power plant units (Siemens SPPA T3000 platform);** CEZ, a. s., Tusimice Power Plants, Prunerov Power Plants (2007 - 2016)
- **Construction of the new classical power plant unit (Siemens SPPA T3000 platform);** CEZ, a. s., Pocerady Power Plant (gas-steam) (2007 - 2014)
- **RSBT (turbine control system) to TELEDU (power plant terminal) data transmission for the provision of transmission network ancillary services;** CEZ, a. s., Dukovany NPP (2010 - 2012)
- **Construction of the new classical power plant unit (EMERSON Process Management OVATION platform);** CEZ, a. s., Ledvice Power Plant (2007 - 2011)
- **Collector level control logic with feed water tank level correction;** CEZ, a. s., Dukovany NPP (2008 - 2010)
- **Organizer of power plant unit output regulation for remote control of transmission network ancillary services;** CEZ, a. s., Dukovany NPP (2001 - 2005)

Engineering simulators 1/2:

- **Turbine control system (RSBT) validation using simulator;** CEZ, a. s., Dukovany NPP(2009 - present)
- **Process analyses using the simulator;** CEZ, a. s., Dukovany NPP, Temelin NPP (2000 - present)
- **Dukovany NPP simulator development and support - "SIMED/EDUS";** CEZ, a. s., Dukovany NPP (2000 - present)
- **Temelin NPP simulator development and support - "DYTE";** CEZ, a. s., Temelin NPP (2000 - present)
- **Pocerady gas-steam power plant simulator development - "EPOS";** CEZ, a. s., Pocerady Power Plant (2011 - 2014)
- **Control circuit logic validation using simulator;** CEZ, a. s., Dukovany NPP (2006 - 2007)

SELECTED REFERENCES OF POWER PRODUCTION OPTIMIZATION DIVISION 5/7

Engineering simulators 2/2:

- **Reactor control system (RCS), incl. reactor rod control system (RRRS), validation using simulator**; CEZ, a. s., Dukovany NPP (2003 - 2004)

Transmission network ancillary services certification:

- **Transmission network ancillary services certification (PC, SC, TC, CIO);** CEZ, a. s., Dukovany NPP, Temelin NPP (2001 - present)

Optimization:

Thermal cycle optimization (PowerOpti):

- **Support of PowerOPTI system;** CEZ, a. s., Porici Power Plant (2015 - present)
- **Support of PowerOPTI system;** Teplarna Strakonice, a.s. (Heating Plant) (2015 - present)
- **Power plant performance evaluation - consultations, methodical and analytical services;** CEZ, a. s., Dukovany NPP (2010 - present)
- **Analysis of potential for cooling circuit optimization;** ČEZ, a.s., Temelin NPP (2016)
- **Upgrade of NC3 (software system for the power plant units thermal performance evaluation; equivalent of PowerOPTI system);** CEZ, a. s., Dukovany NPP (2014 - 2015)
- **PowerOPTI implementation;** Teplarna Strakonice, a.s. (Heating Plant) (2014 - 2015)
- **Prediction of the power plant unit electrical output;** CEZ, a. s., Dukovany NPP (2014)
- **PowerOPTI implementation;** CEZ, a. s., Porici Power Plant (2013)
- **Training in the area of power plant thermal cycle performance optimization** (2013 - present)
- **Refined determination of the nuclear reactor thermal output;** CEZ, a. s., Dukovany NPP(2011)
- **Power plant units cooling circuit optimization;** CEZ, a. s., Dukovany NPP (2011)
- **Data validation using the data reconciliation method;** CEZ, a. s., Tisova Power Plant (2011), CEZ, a. s., Porici Power Plant (2011)
- **Data validation using the data reconciliation method;** Teplarna Strakonice, a.s. (Heating Plant) (2010 - 2011)
- **Data validation using the data reconciliation method;** United energy, a.s., Teplarna Komorany (Heating Plant) (2009)
- **SW system for the power plant units thermal performance evaluation (data reconciliation, process simulation; equivalent of PowerOPTI system) - "NC3";** CEZ, a. s., Dukovany NPP (2004 - 2009)

SELECTED REFERENCES OF POWER PRODUCTION OPTIMIZATION DIVISION 6/7

Combustion optimization (CombustionOpti):

- **Optimization of the solid fuel boilers combustion (DeNOx of K1-K6 EMĚ_I);** ALSTOM s.r.o./Energotrans, a.s. (2014 - 2016)
- **Pyrometer system for SNCR control (supply, delivery and commissioning);** Veolia Teplárna Karviná (Heating Plant) (2015 - 2016)
- **Camera system for surveillance of combustion in combustion chamber of the heating plant (supply, delivery and commissioning);** Veolia Energie Mariánské Lázně, s.r.o. (Heating Plant) (2014)
- **Optimization of the solid fuel boiler combustion;** CEZ, a. s., Tisova Power Plant (2011 - 2013)
- **Optimization of the solid fuel boiler combustion;** CEZ, a. s., Porici Power Plant (2011)

Methodological and software support of energy balances calculation:

- **Central SW system for the power plant units operation economy (energy balances) evaluation;** CEZ, a. s., Production Division (2012 - 2014)
- **Energy balance methodology;** Teplarny Brno, a.s. (Brno Heating Company) (2011); CEZ, a. s., Production Division (2013)
- **SW solution for the power plant units consumption characteristics creation - "VYNAP";** CEZ, a. s., Production Division (2010)

Other References:

- **Complex support of the supplied (mostly aforementioned) SW solutions;** various customers (2002 - present)
- **PassPort / Asset Suite EAM system support;** Indus International / Ventyx Software / ABB (2006 - present)

SELECTED REFERENCES OF POWER PRODUCTION OPTIMIZATION DIVISION 7/7

Special Instrumentation:

Equipment for Measuring of the Boron Concentration (AMKB) = „BORON METER“

- **Supply, delivery and commissioning of 10 pcs AMKB;** Slovenske elektrarne, a.s., Mochovce NPP (2015 - 2017)
- **Supply, delivery and commissioning of 1 pcs AMKB;** Slovenske elektrarne, a.s., Jaslovske Bohunice NPP (2014)
- **Supply, delivery and commissioning of 2 pcs AMKB;** Loviisa NPP (Finland) (2012)
- **Supply, delivery and commissioning of 2 pcs AMKB;** Slovenske elektrarne, a.s., Mochovce NPP (2012)
- **Supply, delivery and commissioning of 8 pcs AMKB;** Zaporizhia NPP (Ukraine) (2011 - 2012)
- **Supply, delivery and commissioning of 1 pcs AMKB;** Slovenske elektrarne, a.s., Mochovce NPP (2008)
- **Supply, delivery and commissioning of 13 pcs AMKB;** Rivenska NPP (Ukraine) (2005 - 2007)
- **Supply, delivery and commissioning of 7 pcs AMKB;** South Ukraine NPP (Ukraine) (2006)
- **Supply, delivery and commissioning of 1 pcs AMKB;** Paks NPP (Hungary) (2006)
- **Supply, delivery and commissioning of 3 pcs AMKB;** Chmelnitska NPP (Ukraine) (2005 - 2006)
- **Supply, delivery and commissioning of 15 pcs AMKB;** CEZ, a. s., Dukovany NPP (2002)
- **Supply, delivery and commissioning of 8 pcs AMKB;** Slovenske elektrarne, a.s., Mochovce NPP (1999)
- **Maintenance of AMKB;** Slovenske elektrarne, a.s. (2014 - present)

PARTNERS & MAJOR CUSTOMERS

- **PARTNERS**

- **MAJOR CUSTOMERS**