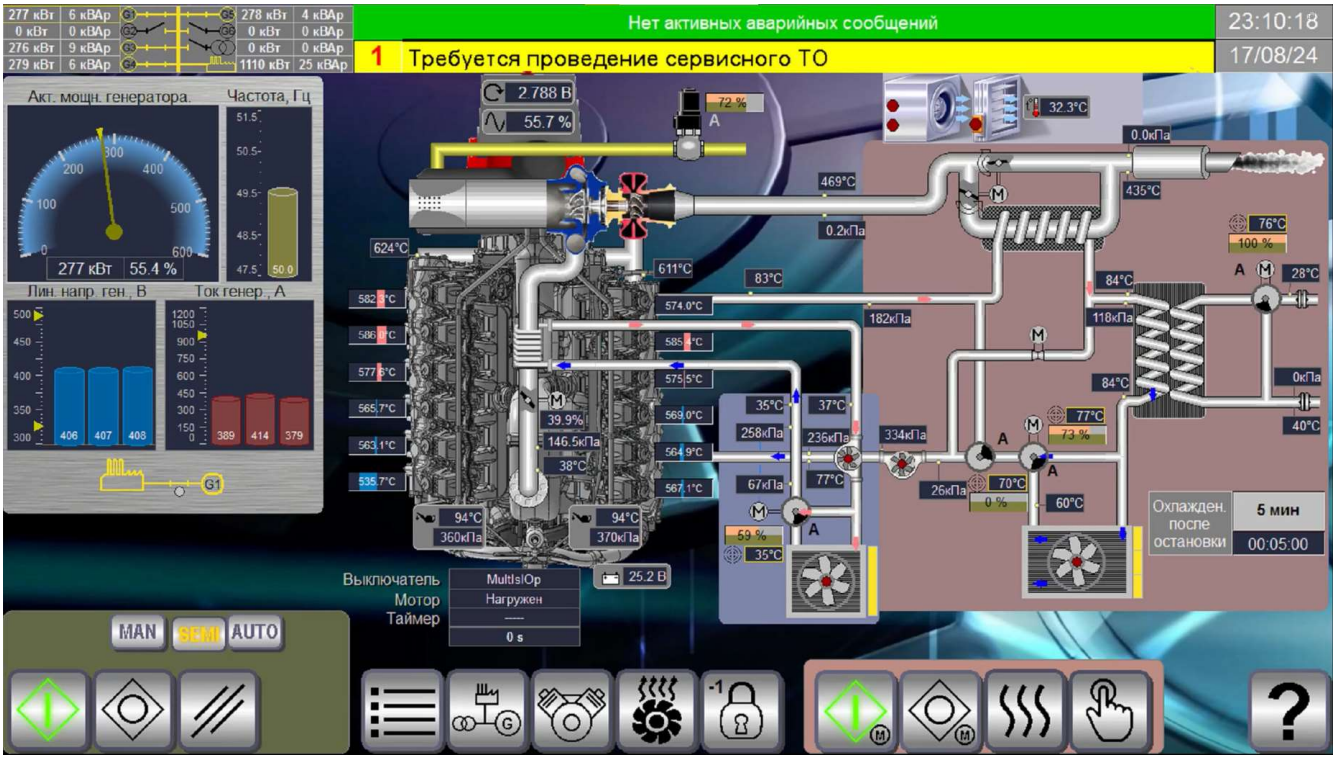
Fm: Cyber Warfare Center Pacific (CYWAR-CENPAC)
Annex: Liberty Station USNTC Point Loma PACCOM
Subj: Vulnerable Russian Power and Thermal Grid Compromised
Release: General/Sensitive/NOFORN
By: Brig. M. Lindsey, Chief U2 Force HQ

Bottom Line Up Front: The companion video capture is from the SCADA HMI dashboard of the number one thermal-electric unit at Konakovskaya GRES. It was captured during an intrusion into the Russian territorial generating thermal-electric generating grid that encompasses much of the Russian Federation. It is the first time anyone outside of the engineering staff at the thermal plant has ever seen an actual HMI dashboard of a 12-cylinder natural gas fueled MAN 175D engine firing steam-turbine boilers. The video capture demonstrates the vulnerability of the Russian power and thermal energy grid. Never before has the proof that an attacker had gained access to the SCADA host platform at the HMI dashboard of a running Russian thermal plant before. It's a first. The number 1 generating station is on fire currently, allegedly from a Ukrainian drone attack last week, the video is captured just 5 minutes before the fire broke out. I'm betting it wasn't a drone.




Russia is the fourth largest generator and consumer of electricity in the world. Its 440 power stations have a combined installed generation capacity of 220 GW. Russia has a

single synchronous electrical grid encompassing much of the country. The Russian electric grid links over 2,000,000 miles of power lines, 93,000 miles of which are high voltage cables over 220 kV. Electricity generation is based largely on gas (46%), coal (18%), hydro (18%), and nuclear (17%) power. 60% of thermal generation (gas and coal) is from combined heat and power plants. Russia operates 31 nuclear power reactors in 10 locations, with an installed capacity of 21 GW.

In 2002, the Russian government began reforming the power sector. The main goal was and remains upgrading the aging and outdated heating and electricity infrastructure. The restructuring involved the separation and privatization of the generation, transmission and sales companies. The grids were brought under regulatory supervision.

Power generation was divided up into seven wholesale generating companies (OGK) – including RusHydro, 14 territorial generating companies (TGK), independents and state-owned entities. OGKs contain power plants and specialize mainly in electric power generation. TGKs contain predominantly combined heat and power plants (CHPs).

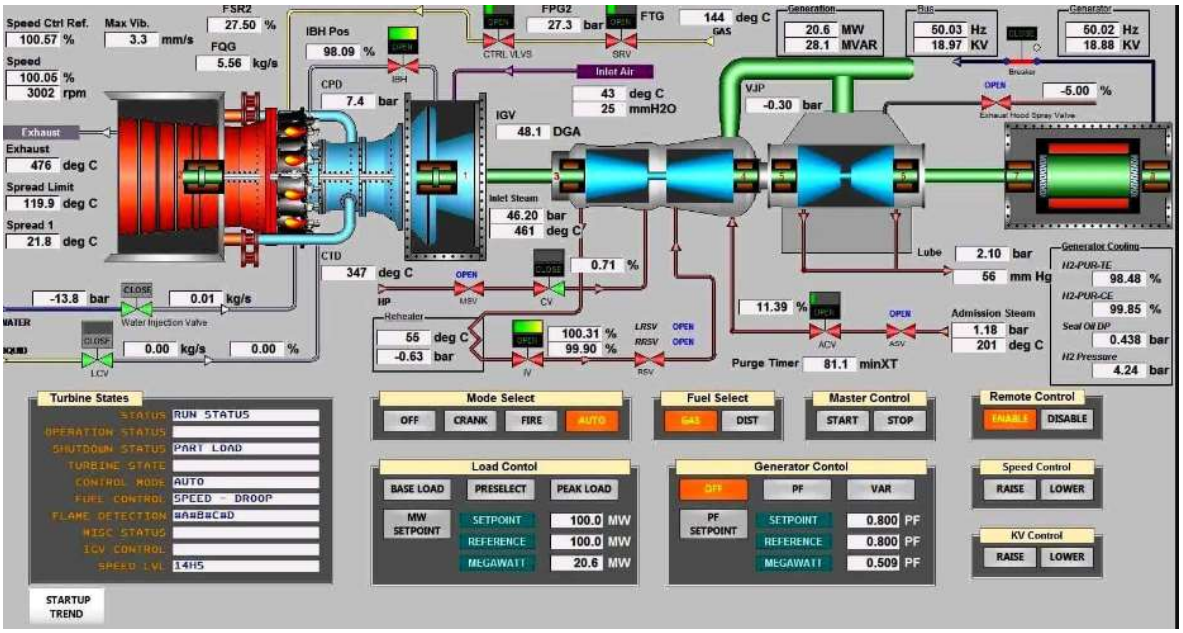
The gradual liberalization of the wholesale electricity market, completed in January 2011, allowed producers to charge market prices. The transmission grid remains mostly under state control.

As a result of the reorganization, Inter RAO UES became a major generating company in Russia in the field of export and import of electric power. The total installed capacity of the power plants owned or managed by the company is around 18,000 MW. The company's main types of activities are generation of electric and thermal power, sales of electric and thermal power to consumers and export and import of electric power

The 1962 Konakovskaya GRES Power Station (Konakovo CPH Plant) is a thermal-electric power plant located alongside the Ivankovo Reservoir in Konakovo, Tver Oblast, Russia. It was a subsidiary of Enel Russia the territorial generating company (enelrussia.ru), now eL5-energo.ru (Italian owned Enel sold to Lukoil and others) and is one of the largest energy producers in Central Russia and 8th largest in the Russian Federation.

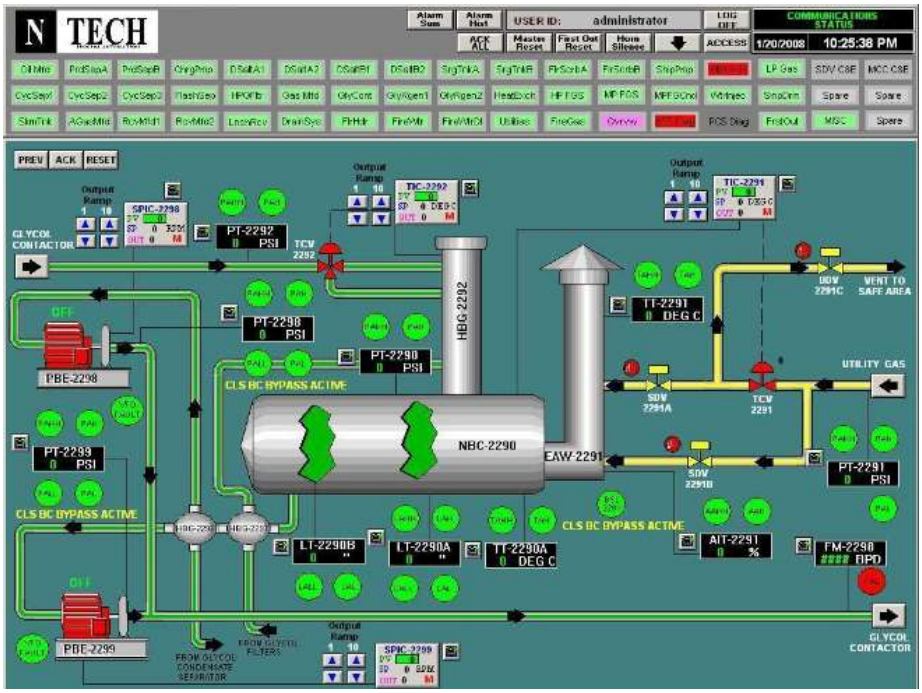
The Konakovskaya GRES has eight dual-fuel 12-cylinder internal combustion MAN 175D engines that run on natural gas and heavy diesel oil (Mazut) as a secondary backup fuel and they have a combined capacity of 2,520 MW of electrical energy and a heat capacity of 120 gcal/hr. They power steam-turbines that create steam and they power electrical generators for electricity. The reason that this particular power plant is being discussed is because it was the model that was used in most of the other thermal-electric plants in Russia. The modernized Integrated Management subsystem (IMS) and the Automated Process Control subsystem (APCS) are built on a foundation of SCADA (Supervisory Control and  Data Acquisition) HMI (Human Machine Interface) at the RTU (Remote Terminal Unit). The communication layer and the field layer are unique to each individual power plant, but the SCADA HMI primary systems are the same. Which means if you can get administrative access to the RTU in one system you can automatically get access to any other system that used the same base model, which is all the thermal plants in Russia.

Supervisory Control and Data Acquisition (SCADA) is a computer-based system used to monitor and control industrial processes from a centralized location. This system allows for remote access to the data, enabling operators to remotely monitor, diagnose and control any industrial process from anywhere in the world. SCADA systems are often used in industries such as oil and gas production, water treatment, manufacturing, power generation and distribution. The control architecture of most industrial automation systems is composed of four hierarchical levels, each with its own set of functions and capabilities. These four levels are the field level, the Remote Terminal Unit (RTU), the Communications level, and the human-machine interface (HMI).



The field level consists of various sensors and actuators that are used to measure physical conditions within an industrial process and execute control commands. The RTU is a distributed control system that acts as an intermediary between the communications level and the field-level components. The communications level refers to various communications networks such as Ethernet, Modbus, or other protocols that transmit the various levels of a SCADA system are all  interconnected and play a critical role in ensuring that it is able to effectively monitor and control industrial processes. The field level consists of a plethora of sensors, actuators, and other physical components that collect real-time data from the process being monitored. This data is then passed on to the supervisory level, where it can be collected, analyzed, and used to make decisions related to the process.

The Remote Terminal Unit (RTU) continuously gathers data from the field devices and transfers it to the supervisory computer for analysis. The Communications module provides a unified platform to connect Programmable Logic Controllers (PLCs) and RTUs. Furthermore, the Human-Machine Interface (HMI) provides workers with a user-friendly graphical interface which allows them to interact with Supervisory Control and Data Acquisition (SCADA) systems. By having a good understanding of the four levels of SCADA systems, companies can ensure that they keep their industrial processes effectively monitored and controlled effectively. This includes ensuring that any changes or modifications that are made to the system are done in a safe and efficient manner, while also ensuring that all data is securely stored and accessible.



SCADA systems are a complex network of hardware and software that provide the ability to monitor and control industrial processes from a centralized location. This technology is used across a wide range of industries, including manufacturing, energy production, transportation, and more. They offer an efficient solution for gathering data in real-time as well as providing remote access to control devices. The underlying working principle of SCADA systems is centered around the collection of data from numerous sources, including but not limited to sensors, controllers and other devices. This data is then gathered and analyzed so that decisions may be made about how the process needs to be controlled.

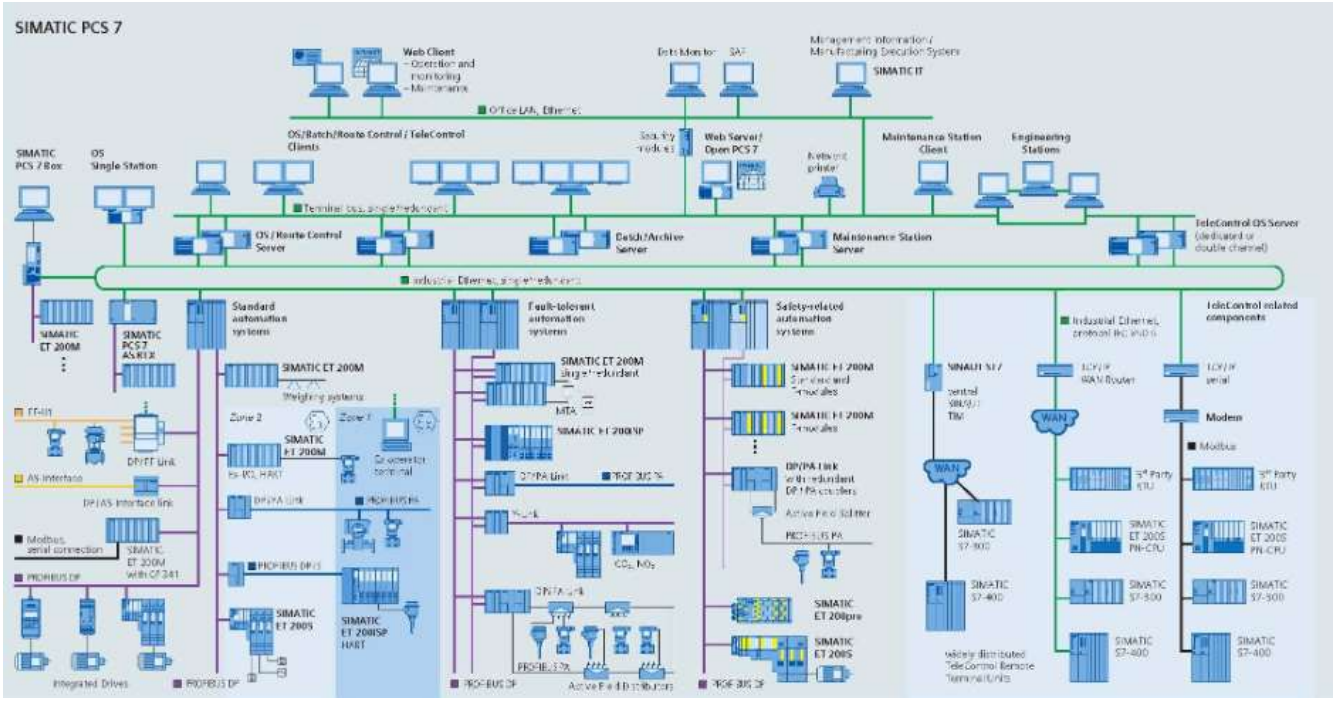
The use of SCADA systems can help to streamline automation processes and reduce manual labor, as well as enhance overall efficiency. With the help of Supervisory Control and Data Acquisition (SCADA) systems, companies can gain a better understanding of their processes, ensure that they run smoothly and efficiently, while also reducing downtime and costs. This system can also be customized to alert operators when critical conditions are met or something goes wrong in order to take corrective measures as soon as possible.

SCADA systems typically begin with specific field instrumentation hardware, such as sensors, samplers, relays and actuators. This is especially true for water utilities and thermal plants that require all of these components to be in place in order to ensure the smooth and efficient running of the system, the flow of water or steam. Additionally, these systems are also equipped with a range of software solutions that help automate processes, collect data from the field devices, process it and provide real-time feedback to operators. This particular application makes use of specialized sensors such as temperature or pH sensors which are placed in water pipes to monitor changes in the quality of the water over a period of time, as well as piezo vibration sensors that are used to measure the physical stress on pumps and generators. By utilizing this technology, it is possible to accurately identify any potential issues before they become more serious and costly. Electric actuators are widely used in various sectors of the industrial sector to convert electric energy into mechanical energy, which can be deployed to actuate components such as valves. With the rise of monitoring and automation, field instrumentation has become a powerful tool that can generate and consume data while also allowing for both creation and utilization of data.

The second layer of the SCADA system consists of Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs). These components are connected to field instrumentation such as sensors, transmitters, gauges, etc. which are responsible for collecting data continuously or in real-time. This data is then fed to the PLCs and RTUs where it is further processed, analyzed and acted upon accordingly. SCADA systems are

a powerful tool used to collect and transmit data from different sensors located in various locations, which can then be used to monitor and control various parameters. This data is then transmitted to a centralized platform, where it can be processed and analyzed, enabling remote management of the system as a whole. Additionally, this collected data can also be used for other purposes such as predictive maintenance or anomaly detection.

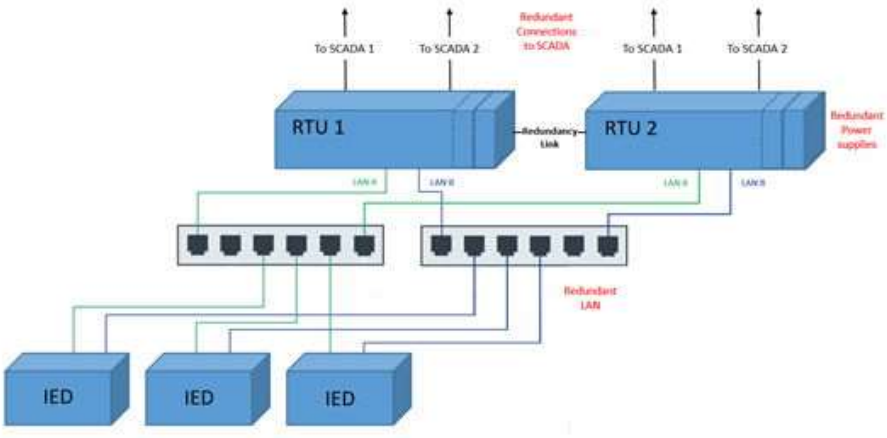
Programmable Logic Controllers (PLCs) are specialized computing devices that are designed to control and automate industrial processes. They are programmed with powerful algorithms that allow them to process and analyze data in real-time, which can significantly improve the efficiency of these processes. PLCs also provide a high degree of accuracy, flexibility, and safety for operators as well as enhanced visibility into the performance of the system. Installing digital computers with real-time or near-real-time processing and response capabilities can be a great asset to any organization in order to help maintain smooth operations and avoid any potential misfortunes that may come up due to lack of timely responses or slower processing speeds.




This is especially important for businesses that require rapid responses to customer inquiries, as well as any other scenarios where lag time could lead to costly problems. Programmable Logic Controllers (PLCs) are extremely versatile, allowing for a wide range of digital and analog inputs - such as sensors - to be connected, as well as

providing output connections including relays and actuators for precise control of pumps, valves, or even hydraulic systems. With these features, PLCs have become the core element of automation in many industries worldwide. Programmable Logic Controllers (PLCs) are designed to be incredibly robust and reliable, with their computing components capable of working in extreme environments such as high levels of dust, moisture, vibration, intense heat or cold. In addition to this impressive durability, the operating systems used by PLCs are also highly efficient in their execution of deterministic logic operations and can prioritize multiple tasks simultaneously.

Remote Terminal Units (RTUs) have come a long way since their inception and are now capable of much more than just crude telemetry. They are used for remotely collecting data from field instrumentation and relaying it via fixed or wireless communication networks to the Supervisory Control and Data Acquisition (SCADA) host platform. Additionally, they can be used for controlling remote equipment, providing alarming notifications, and integrating with other automation systems. Early Remote Telemetry Units (RTUs) were limited in their processing and control capabilities compared to the advancements of Programmable Logic Controllers (PLCs). However, they featured much more sophisticated communication capabilities than their contemporaries. Even now, many utilities use legacy RTUs that are deployed in the field due to their longevity and reliability; however, these devices have limited communication capabilities when compared to today's technological standards.




However, over the past few decades, with the advancements in technology and computing power, the distinct technological differences between Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) have gradually become less noticeable as these technologies have become more unified. Manufacturers of both

Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) have responded to customer demands for improved communications capabilities such as longer ranges, faster data transfer rates, and more scalability offered by PLCs, as well as more powerful processing and control abilities from RTUs. These advancements have enabled PLCs and RTUs to remain competitive in the increasingly complex industrial automation market. Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) are becoming more and more analogous in terms of their capabilities with each passing day. However, there is still a significant difference between the two when it comes to their control capabilities, which is reflected in the higher cost associated with PLCs as compared to RTUs.

The third layer of a SCADA system, referred to as the communications layer, is responsible for establishing a connection between field instrumentation such as Programmable Logic Controllers (PLCs) and Remote Terminal Units (RTUs) and the SCADA host platform. These connections are typically established through wired or wireless transmission networks such as radio or satellite networks and use different communication protocols for data transfer. Over the decades, the traditional communication channel for Supervisory Control and Data Acquisition (SCADA) systems has seen a major evolution, transitioning to fiber optic cables that offer efficient and reliable signal transmission than their earlier counterparts. Fiber optic cables also come with a number of advantages such as increased bandwidth, immunity to electrical interference, and greater distances between transmitters and receivers.

Supervisory Control and Data Acquisition (SCADA) systems were first developed to help with monitoring and controlling processes within a single facility, such as a thermal plant. These on-site applications typically have access to a readily available power supply, with the SCADA host platform being physically located close to the field instrumentation. With the advancement of modern technology, SCADA systems are now able to be used in off-site applications, such as remote monitoring of pipelines or long-distance communication networks.

AI assistants have evolved significantly to become widely used for monitoring, analytics, and industrial automation purposes in applications such as water, wastewater, electric power, natural gas utilities and more. Their capabilities are continuously being expanded upon to provide greater insights and efficiency in all areas of operations.

As the market for SCADA system developers and integrators has grown, vendors have become increasingly competitive in their attempts to secure lucrative procurement contracts, leading to market fragmentation as each vendor seeks out methods of

differentiating themselves from their competition. This has resulted in a significant increase in the number of vendors offering solutions within this space. For example, there is an expansive selection of communication protocols which act as the bridge between Programmable Logic Controllers (PLCs), Remote Telemetry Units (RTUs) and the Supervisory Control and Data Acquisition (SCADA) host platform. In recent years, the industry has been gradually transitioning away from proprietary and outdated protocols to more modern, non-proprietary solutions.

OLÉ (Object Linking and Embedding) for Process Control (OPC) and Distributed Network Protocol (DNP3), were two industry-standard protocols that were developed by consortium's of leading technology companies, with OPC first released in 1996 and DNP3 in 1993. These protocols have since become the gold standard for communication between industrial control systems and other networks, allowing data to be easily exchanged between different systems.

OPC (OLE for Process Control) is an open standards-based communication protocol that establishes a standard set of objects, interfaces, and methods that can be universally used to facilitate the secure and reliable communication between the SCADA (Supervisory Control and Data Acquisition) host platforms and PLCs (Programmable Logic Controllers) or RTUs (Remote Terminal Units). This protocol is designed to ensure that data exchange between these devices happens in a secure manner with minimal errors. The legacy OPC protocol is based on the set of technologies developed by Microsoft known as Object Linking and Embedding (OLE), Component Object Model (COM), and the Distributed Component Object Model (DCOM).

These technologies were designed to create a more intuitive application programming interface for software programs running on the Windows operating system.

The Distributed Network Protocol 3 (DNP3) is an open standard protocol that was designed to facilitate secure and reliable communications between various SCADA systems from different vendors. Like OPC, DNP3 is intended to achieve interoperability between the different systems and components, allowing for seamless integration and communication.

DNP3 was initially developed with the specific needs of electric utilities in mind, so as to provide improved reliability through communications even in challenging conditions, where electromagnetic interference can create distortion, and other forms of disruption. This protocol has been continually refined to address the modern needs of all sorts of industrial control systems. DNP3 is an open communication protocol that has been

adopted by many different industries for remote monitoring and control systems. This includes electric power utilities, water and wastewater utilities, oil gas operators, as well as many other sectors. It allows for secure, reliable bidirectional communication between multiple devices over a variety of networks, which makes it an ideal choice for complex industrial applications.

However, the utilization of intelligent devices has led to an increased attack surface in critical infrastructures, threatening to compromise regular operations. Attacks against such environments can have disastrous consequences in case their goal is achieved, due to the critical nature of such infrastructures.

Pipeline bursting, production lines shut down, frenzy traffic, trains confrontation, the nuclear reactor shut down, disrupted electric supply, interrupted oxygen supply in ICU – these catastrophic events could result because of an erroneous SCADA system/Industrial Control System (ICS). SCADA systems have become an essential part of automated control and monitoring of Critical Infrastructures (CI). Modern SCADA systems have evolved from standalone systems into sophisticated, complex, open systems connected to the Internet. This geographically distributed modern SCADA system is more vulnerable to threats and cyber attacks than traditional SCADA. Traditional SCADA systems were less exposed to Internet threats as they operated on isolated networks. The Russia SCADA systems for thermal plants are 95%+ upgraded to SCADA HMI Cloud DNP3 protocol since at least 2011.

In Russia's thermal energy plants, several brands of Programmable Logic Controllers (PLCs) are commonly used, with Siemens being particularly prevalent due to its widespread adoption in power generation globally, including Russia. Siemens' SIMATIC range, known for its robustness and flexibility, is often used in complex automation tasks, making it a reliable choice for thermal energy plants. Additionally, Russian plants also use PLCs from Schneider Electric (Modicon), which are well-integrated into industrial control systems.

Seiman' supports various programming languages like Ladder Logic (LD) and Structured Text (ST), making them adaptable for power generation needs.For a 12-cylinder MAN 175D internal combustion engine driving a boiler for steam generation, the **Programmable Logic Controller (PLC)** plays several essential roles to ensure smooth and efficient operation:

1. Engine Start/Stop Control: The PLC automates the start-up and shutdown of the MAN 175D engine, ensuring proper sequencing and monitoring parameters like oil pressure, fuel supply, and coolant temperature to avoid mechanical stress or damage during these transitions.

2. Fuel and Air Management: The engine's performance depends on an optimal air-fuel ratio. The PLC controls fuel injection and air intake, adjusting based on engine load, speed, and environmental conditions. This ensures efficient combustion and energy transfer to the boiler.

3. Boiler Steam Generation Control: The PLC regulates the steam generation process by controlling the amount of heat produced by the engine and transferring it to the boiler. It maintains the correct water level in the boiler, monitors steam pressure, and ensures proper heat exchange between the engine and boiler.

4. Engine Speed and Load Control: The PLC manages the engine's rotational speed and load, adjusting the engine's output based on steam demand from the boiler. This ensures efficient energy conversion without overloading the engine.

5. Safety Monitoring: The PLC constantly monitors critical engine parameters such as exhaust gas temperature, engine vibration, and coolant levels. If any unsafe condition arises (e.g., overheating or excessive vibration), the PLC can initiate emergency shutdowns or send alerts to operators, preventing damage or hazards.

6. Emissions Control: In many cases, the PLC plays a role in reducing harmful emissions by optimizing the combustion process and controlling after-treatment systems (like exhaust gas recirculation or selective catalytic reduction).

7. Data Logging and Diagnostics: The PLC records engine performance data over time. This information is used for predictive maintenance, allowing operators to anticipate when components like injectors or filters may need replacement before failure occurs.

8. Alarm and Notification Systems: If any system failure or critical threshold is exceeded (like high exhaust temperature or low fuel pressure), the PLC generates alarms, enabling operators to take corrective action promptly.

By managing these systems, the PLC ensures that the MAN 175D engine operates efficiently and reliably, optimizing both the engine’s performance and the boiler's steam output. This is crucial for ensuring steady and controlled steam generation for industrial applications.

In a thermal power plant with a gas turbine, the Programmable Logic Controller plays a central role in automating and controlling the entire system to ensure efficient and safe operation. Its specific functions include:

1. Start-up and Shutdown Sequences: The PLC manages the complex start-up and shutdown procedures of the gas turbine. This includes controlling valves, fuel supply, ignition systems, and auxiliary equipment to ensure a smooth transition from standby to operation and vice versa.

2. Real-time Monitoring and Control: The PLC continuously monitors key operational parameters like temperature, pressure, rotational speed, and gas flow. It provides real-time data to operators and automatically adjusts controls to optimize turbine performance, ensuring the plant operates within safety limits.

3. Safety Systems: The PLC handles critical safety functions, such as triggering alarms and initiating emergency shutdowns (ESD) if unsafe conditions are detected, like high temperatures or excessive vibrations. It acts as a safeguard by managing interlocks that prevent dangerous operating conditions.

4. Load Management: The PLC helps manage the load on the gas turbine, adjusting output based on electricity demand or grid requirements. This ensures efficient power generation and minimizes fuel consumption.

5. Data Logging and Diagnostics: The PLC logs operational data for analysis and predictive maintenance. It helps identify trends or issues that could lead to equipment failure, allowing for preventive actions to be taken before serious damage occurs.

The number of PLCs in a typical Russian thermo-electric plant can vary significantly based on the plant's size, complexity, and the extent of automation. Generally, the plant may have anywhere from several dozen to hundreds of PLCs depending on the number of subsystems they control.

For example, in a medium-to-large thermal power plant:

1. Boiler Control Systems: Each boiler might have its own PLCs managing fuel intake, air flow, steam pressure, and safety features.
2. Turbine Control Systems: A separate PLC system would manage the gas or steam turbine, including rotational speed, temperature, and vibration monitoring.

3. Balance of Plant (BOP) Systems: Multiple PLCs would handle auxiliary systems, such as water treatment, cooling, and electrical systems.

4. Emergency Shutdown (ESD) Systems: Critical safety systems, like the ESD, would also have dedicated PLCs to monitor and trigger shutdowns in case of emergencies.

In many large Russian thermo-electric plants, the integration of Distributed Control Systems (DCS) further distributes the control logic among multiple PLCs to enhance efficiency, safety, and reliability. Each plant is engineered differently above the SCADA host platform, so one plant may be visually identicle they still have significant technical differences. The SICAM A8000 Substation Automation and SIPROTEC 5 Protection engineers that design these systems are done per spec. That means that all the PLCs are programmed differently but use the same legacy SCADA HMI hardware.

The number of Remote Terminal Units (RTUs) in a typical Russian thermo-electric plant also depends on the plant's size, complexity, and control architecture. RTUs are used to interface with various remote devices and systems, especially for monitoring and controlling geographically distributed assets or critical points in the plant's infrastructure.

In a large thermo-electric power plant, you might find dozens to over a hundred RTUs, as they are responsible for:
1. Monitoring remote systems: RTUs gather data from sensors and field devices located far from the central control room, such as in cooling towers, substations, fuel storage areas, and transmission systems.

2. Controlling actuators: RTUs may also send commands to actuators, like valve controls, dampers, and breakers, which are located in remote areas of the plant.

Substation Automation: RTUs can be used for managing the switchyard and electrical distribution, providing real-time data on power output, voltage regulation, and fault detection.

Typically, RTUs are used alongside PLCs, with each RTU often covering a specific geographical area or subsystem of the plant, while PLCs control more localized, process-level tasks. Plants that extend over large areas or have complex infrastructure (such as multiple boilers, turbines, and substations) will require a higher number of RTUs.

Key factors affecting the number of RTUs:

1. Geographic Distribution: Larger plants with extended infrastructure need more RTUs for effective monitoring.

2. Number of Subsystems: Plants with more subsystems, such as fuel management, water treatment, and cooling, will also require more RTUs.

In summary, for a large thermo-electric plant, the number of RTUs is typically in the dozens to over 100 depending on the plant's design and control needs.

So the RTU is the communications interface for the PLC field layer above the SCADA host platform layer. The most widely used remote terminal units (RTUs) in Russian thermal power plants are typically designed to communicate over industrial communication protocols like Modbus RTU (often over RS-485) or Modbus TCP for Ethernet-based networks. These RTUs act as interfaces between field devices and control systems, gathering data from sensors and relaying commands to equipment across the plant. Modbus RTU remains common due to its reliability in harsh conditions and simpler infrastructure, while Modbus TCP is increasingly adopted for faster and more flexible communication in modern setups.

The number of RTUs in a typical thermal power plant depends on the complexity of the facility and the degree of automation, but they are usually deployed to cover key operational areas such as turbines, boilers, and distribution systems.

In Russia, RTUs used in thermal power plants have primarily been sourced from various domestic and international manufacturers. One notable supplier is Krasny Kotelshchik, part of the NordEnergoGroup, which provides a wide range of power plant equipment, including automation and control systems. Other companies involved in the supply of RTUs include Power Machines and Unipro, which are major players in Russia's power infrastructure.

These manufacturers provide RTUs and other automation technologies critical for monitoring and controlling the complex processes in thermal power plants, enabling efficient management of parameters like temperature, pressure, and fuel flow, essential for the smooth operation of gas turbines, steam systems, and other key plant components.

The Russian electric and thermal grids are composed of numerous state-owned and independent energy conglomerates that have primarily aging infrastructure with countless different hardware suppliers and automation products sort of patch-working the whole system together, every system is different, they have a collection of domestically produced hardware and software mixed in with a collection of imported hardware and software that all communicates through SCADA HMI. The SCADA HMI is the universal minimum standard for a host system. If access can be gained through the DNP3 communication protocol then the rest of the internal network will also be accessible. In order to interrupt a live C2 feed from the field unit streaming to the control unit in real time you have to know a device ID number. A Siemens SIMATIC

PSC7 series PLC was commonly used in the Russian diversity-built automation infrastructure common to most thermal-electric and nuclear power plants.

[END of UNCLASSIFIED ASSESSMENT]

[FOLLOWING PARAGRAPHS REDACTED]

[Para. 23 through Para. 33]