INCREASING RELIABILITY OF NUCLEAR REACTOR EMERGENCY DIESEL GENERATORS THROUGH THE USE OF INTELLIGENT DIGITAL CONTROL SYSTEMS

Sergei Aleksanin, Kirill Lopatsky, Edward Petit de Mange
Diakont
3821 Calle Fortunada, San Diego, CA 92123 USA

support@diakont.us.com

Copyright 2012 by the American Nuclear Society, La Grange Park, Illinois
INCREASING RELIABILITY OF NUCLEAR REACTOR
EMERGENCY DIESEL GENERATORS THROUGH THE USE OF
INTELLIGENT DIGITAL CONTROL SYSTEMS

Sergei Aleksanin, Kirill Lopatsky, Edward Petit de Mange
Diakont
3821 Calle Fortunada, San Diego, CA 92123 USA
support@diakont.us.com

ABSTRACT

Rosenergoatom contracted Diakont to complete a 9-year project to design and supply digital modernizations for nuclear power plant Emergency Diesel Generator control systems. The new systems leveraged the functionality of modern digital controls while mitigating risk through the use of innovative features, including a parallel analog logic train. This methodology substantially increased EDG reliability and uptime, and Diakont’s design has since been utilized at multiple nuclear power plants. The design parameters of this digital modernization represented First of a Kind (FOAK) engineering for EDG control system modernization.

Key Words: Emergency Diesel Generator, Digital I&C, Loss of Off-Site Power (LOOP)

1 INTRODUCTION

1.1 Nuclear Power Plant Emergency Diesel Generators

Nuclear power plant Emergency Diesel Generators (EDG) are large diesel engines coupled to electrical generators, which provide power to plant safety and control systems when required. EDGs are critical safety components of Generation II NPPs because they provide electrical power necessary to activate and control reactor cooling and safety systems in the event of a Loss of Off-site Power (LOOP) event, and to prevent a critical Station Blackout (SBO) scenario. Generally a reactor unit will be equipped with 2-5 EDGs, ideally physically-separated, whose control systems are isolated and do not rely on common interconnection. In some installations, multi-unit plants implement the capability to cross-connect EDGs between reactor units.

Each EDG includes both principal and auxiliary components. The principal components are the diesel engine, generator, and automated control system including the automatic voltage regulator. These principal EDG components are typically classified in the top safety category for plant equipment. The auxiliary components are sub-systems that are not directly-related to the operation of the EDG, such as ventilation and draining equipment.

1.2 Kola Pilot Project

Kola NPP is a 4-unit plant located in northwestern Russia near Murmansk, above the Arctic Circle. Units 1 and 2 are VVER-440/230 models, the original Russian pressurized light water design, while Units 3 and 4 are VVER-440/213 models, a design which incorporated added safety features. In 2002, Units 1 and 2 had been operational for close to 30 years and were nearing a scheduled shutdown. The operator, Rosenergoatom, made the decision to proceed with applying for 15-year life extensions on Units 1 and 2, and to utilize international funding available through the Swedish International Project (SIP) to improve plant safety equipment, including the backup power systems. Rosenergoatom awarded Diakont a Phase 1
contract to complete the development and installation of upgraded EDG base control systems at Kola. Follow-on Phase 2 and Phase 3 components would later add the automatic voltage regulator and generator protection sub-systems. The EDG control system modernization at Kola was to be a pilot project, which if successful would take the designs and lessons-learned and apply them to other older Russian reactors expected to receive 15-year life extensions, including those at Novovoronezh and Kursk NPPs.

1.3 Kola Legacy Emergency Diesel Generator Control Systems

All of the EDGs at Kola utilize model 15D100 diesel engines supplied by the Malyshev company in Ukraine, with model VS-34/26 regulators and model SGDS-15-74-8 and SGDS-15-54-8 synchronous generators, both with outputs of 6300 V at 50 Hz. The systems were initially installed with model SHES 9002-02B2 control systems supplied by the engine manufacturer, offering only minimal functionality for remote and automated EDG operation. The control systems utilized simple analog relays, and their running parameters were only displayed locally in the engine room on indicator lights or analog-type dial gauges.

Kola’s EDGs had a history of poor uptime rates, extensive maintenance requirements, and non-compliance with modern regulatory requirements. The root cause for the majority of these problems was attributed to the antiquated control systems [1]. At the start of the upgrade project, the plant operator cited the following specific deficiencies of the legacy EDG control systems which could be improved:

- The use of outdated, low-reliability electronic components with obsolescence problems
- No provision for diagnostics
- No resilience to any single failure
- Little running performance feedback during operation
- No provision for data logging from sensors, events, and personnel actions
- No provision for future expansion or iterative modernization
- Compounded support problems due to unregulated lifecycle modifications

The EDG control systems at Kola (as well as at other Russian nuclear plants) are designated as safety Class 2U equipment, under Russian nuclear safety regulatory code OPB-88/97. Class 2U is the highest level of safety for automation equipment.

<table>
<thead>
<tr>
<th>TABLE I. Parameters of Kola EDG engines and generators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Diesel Engine</strong></td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Number of cylinders</td>
</tr>
<tr>
<td>Displacement, cubic inches</td>
</tr>
<tr>
<td>Rated power output, hp</td>
</tr>
<tr>
<td>Rated speed, rpm</td>
</tr>
<tr>
<td>Charge air pressure, psi</td>
</tr>
<tr>
<td>Starting method</td>
</tr>
<tr>
<td>Cooling system</td>
</tr>
<tr>
<td><strong>Generator</strong></td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Power output at Cos $\varphi=0.8$, Watts</td>
</tr>
<tr>
<td>Voltage, V</td>
</tr>
<tr>
<td>Frequency, Hz</td>
</tr>
<tr>
<td>Rated speed, rpm</td>
</tr>
</tbody>
</table>
2 KOLA UPGRADES

2.1 Project Definition

In 2002, Diakont began developing digital system upgrades for the 13 EDGs at Kola, required to meet the following principal requirements:

- Replacement and new elements were to be integrated with the existing engine and generator, without significant mechanical modification
- New elements were to have a design lifetime of not less than 30 years
- The automatic voltage regulator was to be upgraded to a modern design
- A generator protection sub-system was to be included in the development
- Installation and commissioning were to be conducted within the period of a refueling outage (<20 days)
- Pre-commissioning was to be conducted within a short timeframe (8-12 days)
- Control system was to meet the requirements for equipment in top-tier safety class 2U, per OPB-88/97
- Control system was to meet Category 1 seismic requirements (unaffected operation during and after a seismic event, of approximate magnitude 7.0) per GOST 17516.1-90 Group M39 (analogous to IEC 721-3-3 and IEC 721-3-4 Class 3M1 and Class 4M1)
- Control system was to meet IEC 1000-4-1, 1000-4-8, 1000-4-9, 1000-4-11-IV-A, and GOST R 50746-2000 EMC/EMI standards
- EDG units with updated control systems were to have an uptime rate of not less than 99.5%

The new control system design was to provide the following functionality:

- Automatically maintain the EDG in a standby state, ready for an automated start
- Automatically start and synchronize to electrical bus
- Provide continuous loaded operation without operator intervention for no less than 300 hours
- Automatically start and stop upon signals from the plant I&C system, control room, or local operator panel (including pre-starting and post-stopping sequences)
- Automatically refill the fuel day tank, and oil, water, and compressed air service tanks
- Protect engine and generator from fluctuations in electrical load and bus condition
Perform continual diagnostics of engine, generator, regulator, and control system, and generate operator alarms and warnings
Perform data logging, and periodically transmit extended information packages to operators
Provide the ability to test system functionality, protection, and interlocks prior to installation, using a separate external simulator

2.2 Project Planning
The EDG control system upgrade at Kola was divided into 3 phases. Phase 1 (2002-2004) was the replacement of the base relays with intelligent digital control systems, Phase 2 (2007-2009) was the upgrade to digital automatic voltage regulators, and Phase 3 (2010-2011) was the incorporation of the generator protection systems. Diakont designated that each phase be conducted according to the following process:

1. INVESTIGATION – Including obtaining comprehensive plant information that would drive the design (equipment location, actual operating conditions, etc.)
2. ENGINEERING – Including development of specifications, design, documentation, and the integration plan
3. MANUFACTURING – Including fabrication of equipment, internal testing, initial regulatory qualification, and customer factory acceptance testing (FAT)
4. CUSTOMER TRAINING
5. DELIVERY AND PRE-COMMISSIONING
6. INSTALLATION AND COMMISSIONING – Including final regulatory qualification, and removal of legacy equipment

2.3 Phase 1 Design
2.3.1 Design parameters
In order to minimize risk and maximize efficiency, Diakont established the following general guidelines that would drive the design of the system architecture:

- Utilize existing equipment interconnections, whenever possible
- Utilize existing EDG sensor models, whenever possible
- In cases where the use of existing sensors is not advisable, duplicate their footprint and mounting
- During Phase 1, provision for elements to be included in Phases 2 and 3

2.3.2 Functional design considerations
In developing and manufacturing the equipment, Diakont established the following key new functional and performance characteristics:

COMPONENT SELECTION – The EDG control systems were to be designed and built using commercially-available, mature component lines manufactured by large, dependable companies with a long market presence and a history of reliability, such as Siemens or Schneider Electric.

CONTINUOUS DIAGNOSTICS – The EDG control systems were to perform continuous automatic diagnostics. Timely fault detection both while in standby or running modes was imperative to meet the required reliability and uptime rate.

RESISTANCE TO SINGLE AND COMMON-CAUSE FAILURES – To ensure resistance to single failures, the EDG control systems were to use dual independent logic systems. In Phase 1, this 2-train redundant design was employed for the critical EDG actuations: starting, on-load operation, and safe shutdown. To make the control system resistant to a common-cause failure, 1 of the control system
channels used hardwired (relay) logic, while the other channel used PLC components. Either the digital or the analog logic train could be selected for operation, with the other train remaining in hot-standby. Upon initial powering, the entire control system defaulted to the analog logic train. The system could then hot-swap to the standby train upon operator command, or automatically in the event that the operational train failed. Situations that would be classified by the system as a train failure include: improper voltage at a point, bad communication with a module, or the report of an impossible situation (such as a tank being both empty and full). Failure of a single train did not affect the operation of the other. Sensors were also designed with redundancy – critical sensors such as oil pressure and engine speed were installed in groups of 3, with analysis logic based on the “2 of 3” principle. A failure or incorrect output of just a single sensor would not result in EDG shutdown. Signals needed to be received at least from 2 of the 3 parallel sensors for actuation of the EDG protection system.

DATA LOGGING AND OPERATOR INTERFACE – The EDG control system included an operator interface panel for control and for display of operational data. The information output was organized in a tiered structure: from a general EDG readiness state, down to specific detailed information about the status of individual elements (at the module level). The internal archive was designed to store a hardware status log containing up to 1500 entries, and to record sensor signals and operator actions onto a data logger continuously. The system also included a single operator’s workstation (OWP), which provided a centralized access point for information on all of a particular reactor’s EDGs. It also provided the ability to reconstruct the evolution of emergency situations, including the actions of the operation personnel. In addition, the OWP was designed to have the means to transfer status information about any of the EDGs over the plant’s network using TCP/IP protocol.

PROVISION FOR MODIFICATION AND FUNCTIONAL EXPANSION – Since it was realized that sensors would need to be changed during the lifetime of the control system, the means were included to conduct this replacement through software modifications whenever possible, rather than hardware changes. Also, a computational reserve was allocated during the system design phase, to allow for future expansions. A 10% reserve was included for additional analog and discrete input connections, and a 30% reserve was included in controller processing.

The control system architecture detailed in Figure 2 was established.
The Control Cabinet (CP-1 and CP-2) elements processed information received from the EDG sensors, controls, and the EDG plant hardware. They generated control actions for the engine and its auxiliary equipment, transferred data to the reactor control room, displayed the current EDG and control system status information on the cabinet monitor, and transferred data to the EDG local operator interface over the Fipway network.

The Input/Output Cabinet (IOC-2) element received signals from the reactor I&C system and EDG sensors, generated control signals upon commands from the CP-1/2 cabinets, monitored electrical bus parameters, ensured synchronization with the power bus, output EDG condition feedback over the plant network, and supplied uninterruptible 220 V AC power to the CP-1/2 cabinets.

The Starting Devices Cabinet (SDC-1) element controlled the EDG actuators (pumps, gates, etc.).

The OWP element provided centralized status monitoring and remote control of each EDG. It also included the data logger, which stored data on recording media, and had the means to provide a hard copy printout.

2.3.3 Digital upgrade stability, safety, and security considerations

This project was fundamentally significant since it incorporated the upgrade of a Category 1 safety-related control system to a modern system that included digital logic processors. For this reason, disciplined practices had to be employed at a fundamental level throughout the development process. All work was to be compliant not only with Russian standards for digital control systems, but also with European and international standards. Experts from Fortum (Finland) and SwedPower (Sweden) were involved in the project from its start, providing guidance with regard to compliance.

The selection of PLC controllers was also extremely important. The Schneider Electric Quantum series was utilized for the Phase 1 project, as it met all the design criteria and had previously been qualified for use in safety-related European nuclear plant applications. The principal requirement (as of 2002) was that the controller was certified to safety integrity level (SIL) 3 per IEC 61508.
Software programming had to be compliant with IEC 61131-3. The software development process virtually eliminated the potential for logic errors, through the use of iterative simulations that were later verified through factory and on-site testing. The programming was designed to be simple, with a very limited number of final conditions. All control elements were to be isolated from external connections, to eliminate the possibility of software corruption from external sources. The sub-system that was connected to the plant network incorporated industrial anti-virus software. Operator access was password-protected, and physical security measures were implemented that limited unauthorized access to data connections inside the control cabinets. A required criterion was that the plant operator be able to maintain the system throughout its life cycle, exclusive of the control system supplier. To support this requirement, the Diakont programming source code was supplied as a project deliverable.

2.3.4 Design for installation and commissioning

In order to meet the required short installation timeframes, each electrical cabinet incorporated an electrical wiring kit (EWK). The EWKs were comprised of pre-wired interconnections for each cabinet, external elements, and other cabinets.

A computerized test fixture was designed and fabricated as part of the Phase I development program. This fixture was crucial for testing the elements of the EDG control system, and also for qualification and operator training. The use of the fixture provided a means to test the control system’s response to normal and abnormal scenarios, alarms and warnings, and operation of interlocks and protection systems.

2.3.5 Design validation

A probabilistic risk assessment (PRA) program was developed during the design process, which incorporated a comprehensive quantitative safety analysis that identified all potentially critical situations and the control system’s response. This analysis was run repeatedly as the system and software were developed, allowing Diakont engineers to make iterative adjustments to the system’s logic, redefining responses to various sensors and operating scenarios. The PRA guided the developers toward realizing the safety benefits of using a modularized system.

Following production, all failure scenarios were replicated using a test fixture to validate performance. The theoretical analysis demonstrated an uptime greater than 99.5%, and an MTBF of >100 years (with specified preventative maintenance).

2.4 Phase 1 Regulatory Qualification

In order to satisfy stringent regulatory concern surrounding the upgrade from an analog to a digital system, Rostechnadzor dictated that the following criteria be met for successful equipment qualification:

1. Confirm that software had been developed and tested in compliance with IEC 60880-2006 (Category A) and IEC 62138-2010 (Category B and C) standards
2. Confirm that an independent lab had verified compliance with required EMC and low-voltage regulatory standards
3. Confirm that plant documentation had been modified to designate that a representative of the regulator shall issue quality approval for the product at all stages of its lifecycle
4. Confirm compliance with designated standards during the FAT
5. Approve compliance and functionality during on-site testing, for operational and design basis accident (DBA) scenarios

2.5 Phase 1 Plant Site Installation and Commissioning

The two-part design of the control system cabinets allowed for advance delivery of each cabinet’s EWK, so that cables could be laid. Then each control cabinet was mounted on its EWK and connected.
Once the plant refueling outage had been started and the EDG was tagged-out, installation was conducted on an expedited timeframe according to the following process:

1. Installation of sensors and switchover of interconnections
2. Independent operability checks of system actuators, in manual mode
3. Verification of signal communication with EDG sensors
4. Verification of engine and generator signaling and interlocks
5. Verification of signal communication with reactor I&C system
6. Operability checks of system actuators, in automatic mode
7. Independent EDG control system startup and idle check, in automatic mode, with all protection and interlocks enabled
8. Comprehensive EDG system performance verification, including EDG protection in simulated emergency situations

All 13 base EDG control systems were successfully installed and commissioned at Kola.

2.6 Kola Upgrade Phase 2

During the period from 2007 to 2009, Diakont developed, manufactured, qualified, delivered, and commissioned automatic voltage regulators (AVR) for the 13 EDGs at Kola NPP. The AVR controlled the current of model BC-34/26 and PM1110M-5 cross-field regulators, on model SGDS-15-74-8 and SGDS-15-54-8 synchronous generators. The AVR units interfaced with the already-installed Phase 1 elements of the EDG control systems.

![Figure 3. Phase 2 Diakont AVR cabinet (Kola NPP)](image)

2.7 Kola Upgrade Phase 3

During the period from 2010 to 2011, Diakont developed, manufactured, qualified, delivered, and commissioned generator relay protection systems (GRP) to accompany the Phase 1 and 2 EDG system components at Kola, hereby completing the EDG control system upgrade. The GRPs provided protection and emergency control of the model SGDS-15-74-8 and SGDS-15-54-8 synchronous generators. The GRP protections were divided into 3 groups:

- Group 1 (always activated): Stator winding short circuit, Power output short circuit
- Group 2 (able to be disarmed only for testing): Reverse current (when over 10% power, cuts fuel), Stator winding ground fault (of more than 5 A, isolates generator), etc.
- Group 3 (able to be disarmed at any time): Overcurrent, Internal generator ground fault, etc.
Even when disarmed, these protection systems had the ability to generate operate alerts. The GRP also provided the means to connect the generator in parallel with the electrical bus during trial starts, using either automatic or precise manual synchronization.

2.8 Analysis of Kola EDG Control System Upgrade Project

Diakont received extremely favorable feedback about the upgrade project from Kola plant management, Rosenergoatom, Rostechnadzor, SIP, and the Russian nuclear community [1]. No significant unforeseen problems arose during development, qualification, integration, or commissioning. It should be noted that the implementation of a digital control system for a diesel engine and generator is significantly simpler than large-scale turbine or reactor I&C systems. Particular achievements included:

- Introducing reliable, economical, easy-to-use, easy-to-maintain EDG control systems that met all regulatory requirements, and have since operated without any notable faults
- Meeting tight schedule targets for installation and commissioning
- Developing a unique dual-channel speed sensor
- Gaining digital control system upgrade experience on the part of the utility, equipment manufacturer, and regulatory group

There was some retrospective negativity about the phased methodology utilized for this upgrade, since it resulted in a longer overall process and increased cost due to the production of extra equipment that later became redundant. However the general consensus was that the phased approach significantly reduced overall project risk.

In the 9 years following the upgrade at Kola, Diakont’s EDG control systems had amassed over 100 reactor years of operation with no critical failures and not a single unsuccessful EDG starting sequence, neither initiated by the reactor protection system nor in mandated biweekly test starts.

3 DESIGN CONSOLIDATION AND STANDARDIZATION

3.1 Large-EDG Application

Following the favorable outcome of Phase 1 and the progress in Phase 2 of the Kola project, in 2008 Rosenergoatom contracted Diakont to conduct 4 EDG control system upgrades for the VVER-1000 reactors at Novovoronezh NPP and 6 EDG control system upgrades for the RBMK-1000 reactors at Kursk NPP, all to be completed by 2011. Both Novovoronezh and Kursk nuclear plants utilized model 12ZV40/48 diesel engines manufactured by the Adriadiesel company in Croatia, with model S2445-10 (on a complete EDG that was to be installed new) and S2445-12 (on the EDGs to be upgraded) generators. These EDG units were considerably larger than those at Kola.

<table>
<thead>
<tr>
<th>TABLE II. Parameters of Novovoronezh and Kursk EDG engines and generators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Diesel Engine</strong></td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Number of cylinders</td>
</tr>
<tr>
<td>Displacement, cubic inches</td>
</tr>
<tr>
<td>Rated power output, hp</td>
</tr>
<tr>
<td>Rated speed, rpm</td>
</tr>
<tr>
<td>Starting method</td>
</tr>
<tr>
<td>Cooling system</td>
</tr>
<tr>
<td><strong>Generator</strong></td>
</tr>
</tbody>
</table>
3.2 Expanded Functionality and Design Consolidation

Now that the technology had been proven, each of the Novovoronezh and Kursk EDG control system upgrades was to be conducted all at once, rather than using the phased approach employed in the pilot project at Kola. As part of the development work for this project, the phased elements of the Kola project were to be consolidated into one unified system.

The system design was to include all of the functionality from the Kola systems, and also be expanded such that 100% dual-channel (parallel analog and digital train) architecture was incorporated on all elements, including the uninterruptable power supply and the AVR. The Siemens SIMATIC S7-300F platform, also certified to SIL 3, was chosen as the PLC logic controller for the consolidated design. Also during this development project, the analog train was further bolstered through the incorporation of dual parallel relay channels for actuation of the most critical functionality (starting, protection, shutdown, and lockout).

The control system architecture detailed in Figure 4 was established.

![Figure 4. System diagram of Diakont EDG digital control systems at Novovoronezh and Kursk](image)

The upgrade projects at Novovoronezh and Kursk were successful. An additional project output was the finalized design for the consolidated EDG digital upgrade, which has since been applied to other plants and other EDG models.
4 CONCLUSIONS

At the time of inception the EDG digital upgrade project was considered to be quite ambitious, particularly due to the extensive development and regulatory compliance requirements associated with conducting an analog-to-digital upgrade of control systems for Category 1 safety equipment. The use of an iterative development process effectively mitigated the risk, through distribution, since at each stage certain new aspects of the project were deployed.

The use of dual-channel architecture with parallel digital and analog logic trains was successfully proven to make the system resistant to common-cause failures. The use of redundant sensors with a “2 from 3” logic was successfully proven to make the system resistant to single sensor failures. The implementation of continuous diagnostics was the most significant contributor to designing what many consider to be the most reliable EDG control system ever designed. This functionality presented a paradigm shift in operating principles for the EDG control system – the evolution from a sensitive, reactive system prone to initiating EDG shutdown, to a robust, proactive system that maximized EDG uptime and kept EDGs operational.

![Figure 5. 15D100 EDG with complete Diakont digital control system (Kola NPP)](image)

![Figure 6. Diakont EDG digital control system (Kursk NPP)](image)

**Table III. Diakont EDG control system upgrades**

<table>
<thead>
<tr>
<th>Period</th>
<th>Plant</th>
<th>EDG System Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002-2011</td>
<td>Kola</td>
<td>13</td>
</tr>
<tr>
<td>2008-2010</td>
<td>Novovoronezh</td>
<td>4</td>
</tr>
</tbody>
</table>
5 ACKNOWLEDGMENTS

The authors wish to thank all those involved in the EDG digital control system upgrade development project over the last 10 years, including those at Kola, Novovoronezh, and Kursk nuclear power plants, Rosenergoatom, Rostechnadzor, Swedpower, Fortum, and our worldwide Diakont colleagues.

6 REFERENCES