



AUTHOR

Hadrien Pinault

Staff Engineer at Rehiko Power Systems EMEA

Ensuring Genset Reliability Through Robust Generator Controller Design and Validation

INTRODUCTION

In modern power generation systems, the controller acts as the “brain” of the genset, ensuring safe and reliable operation, coordinating multiple units, optimizing performance, and enforcing safety and cybersecurity functions.

In mission-critical environments such as Data Centers, reducing uncertainty and ensuring predictable system behavior are essential requirements. Controller reliability therefore becomes a fundamental contributor to power availability, operational confidence, and long-term infrastructure resilience.



A NEW FRAMEWORK

A new development and validation framework was established starting with the APM804 controller program, reflecting the increasing complexity, cybersecurity requirements, and mission-critical expectations associated with modern power generation systems. The resulting methodology now serves as the foundation for the development and validation of Rehlko's latest generation of control platforms.

To address this, the Control Systems team at Rehlko has implemented a structured development and multi-level validation approach designed to ensure robustness and maintainability. This methodology is based on industry-proven Model-Based Design principles, enabling clear traceability from requirements to software and improving collaboration across engineering teams.

Controller software is defined through detailed specifications, decomposed into modular components, and validated through rigorous unit testing. Integration is followed by progressive validation across multiple levels, including simulation (MIL), real-time testing with hardware (HIL) and full-system testing. At each stage, iterative testing and systematic non-regression verification ensure predictable and consistent behavior across a wide range of operating conditions.

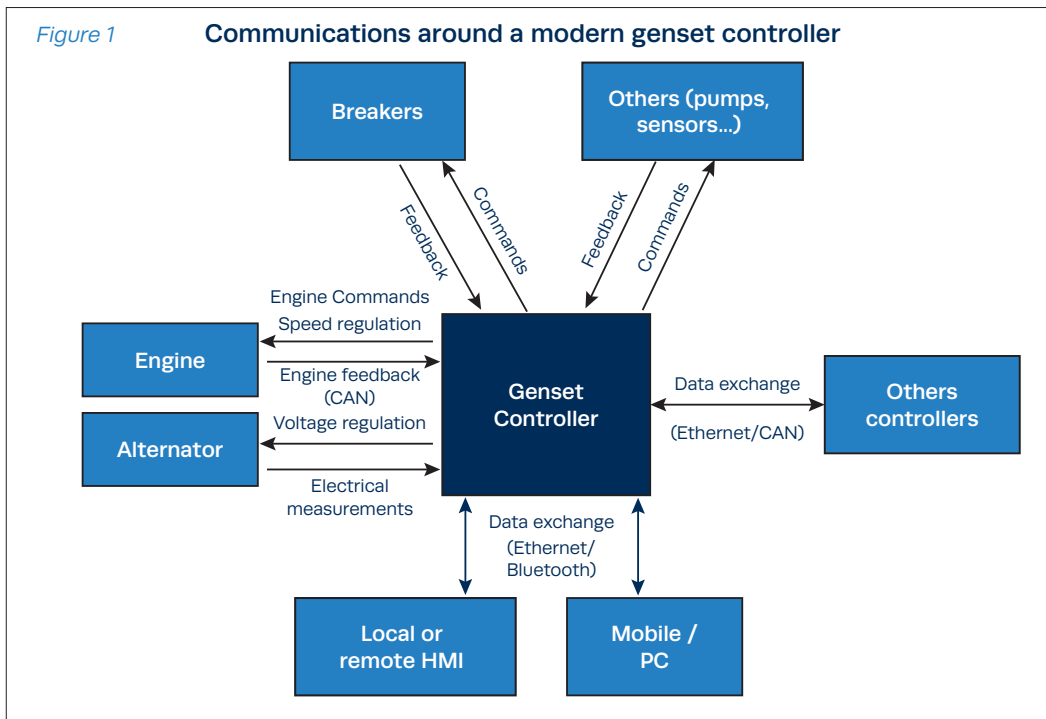
This approach enhances robustness, enables validation of critical edge cases, reduces testing costs and fuel consumption, and ensures high-quality, maintainable software — providing a high level of confidence in predictable controller operation across mission-critical and Data Center applications.

CHALLENGES IN GENSET CONTROLLER RELIABILITY

In mission-critical environments such as data centers, power system reliability is paramount. Backup generators are expected to start instantly, synchronize seamlessly, and operate flawlessly under all conditions. At the core of this performance lies the controller, the true “brain” of the genset, responsible for monitoring, decision-making, communication, and control execution across the entire system.

Beyond backup applications, gensets are increasingly contributing to the stability of electrical grids, particularly with the growing integration of renewable energy sources. While renewables introduce variability and intermittency, gensets provide stable and controllable power, playing a key role in maintaining grid balance. This evolution further increases the expectations placed on controller performance and reliability.

Modern genset controllers must therefore manage growing system complexity. They not only regulate engine and alternator performance, but also exchange data with other controllers, interface with a wide range of external equipment (switchgear, breakers, protection systems), and connect to external supervision and user interfaces (HMI, mobile devices, or PCs), while ensuring secure communication (*see Figure 1*). Some of these interactions require real-time responses with very tight latency constraints (typically around 10 ms). The safety and proper functioning of the overall power system rely heavily on the controller's ability to manage these interactions reliably.



In addition, each installation is unique, requiring tailored configurations and adaptable control strategies. Controllers must also operate reliably under harsh environmental conditions, including vibrations, extreme temperatures, and electrical disturbances.

Hardware redundancy, such as adding a second identical controller, can improve availability, but it only partially addresses the challenge. Software remains a critical point of vulnerability: it must handle a wide range of operating scenarios, including rare and complex fault conditions originating from the genset itself or from connected equipment. Ensuring consistent and predictable behavior under both normal and abnormal operating conditions is therefore essential to support conservative mission-critical power architectures.

Traditional validation approaches, primarily based on testing directly on physical gensets, provide realistic conditions but face major limitations. Testing capacity is constrained, and scenarios are often restricted to standard operations such as start-up or synchronization. Complex or destructive fault conditions cannot be safely explored, and the internal behavior of the controller remains difficult to observe in detail. When issues arise, system complexity makes root cause analysis time-consuming, delaying corrections and software releases. Moreover, the cost and environmental impact of the fuel consumed during testing are significant: a 3000 kVA genset consumes around 750 L/h of diesel at full power. This creates a difficult trade-off: testing on physical gensets must be limited, while performance requirements continue to increase.

These constraints also limit the ability to deploy frequent updates, which are increasingly required to address evolving cybersecurity threats and operational requirements. As a result, ensuring high reliability in modern genset controllers demands a more comprehensive and scalable development and validation approach.

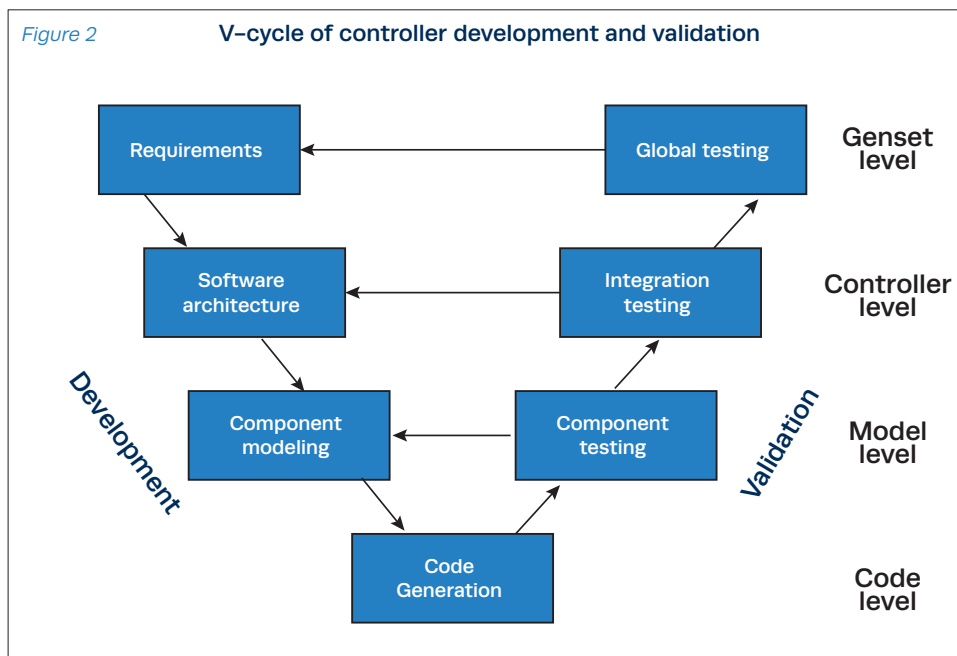
CONTROLLER DEVELOPMENT APPROACH AND SOFTWARE ARCHITECTURE

The methodology described in this paper was introduced during the development of the APM804 controller platform. As Rehlko expanded controller capabilities to support advanced power plant architectures, grid interaction, cybersecurity requirements, and Data Center applications, traditional development and validation methods no longer provided the required level of coverage, repeatability, and confidence.

To address this challenge, a structured and systematic development approach is required. The Control Systems team at Rehlko has therefore adopted a development methodology based on Model-Based Design principles. This approach, widely used in demanding industries such as automotive [iajit.org], enables development teams to define system behavior through executable models instead of command-line code, allowing early validation of control strategies and system interactions. By shifting validation activities toward the early stages of development, model-based approaches help identify issues sooner and reduce dependency on physical prototypes, thereby improving overall development efficiency and software quality.

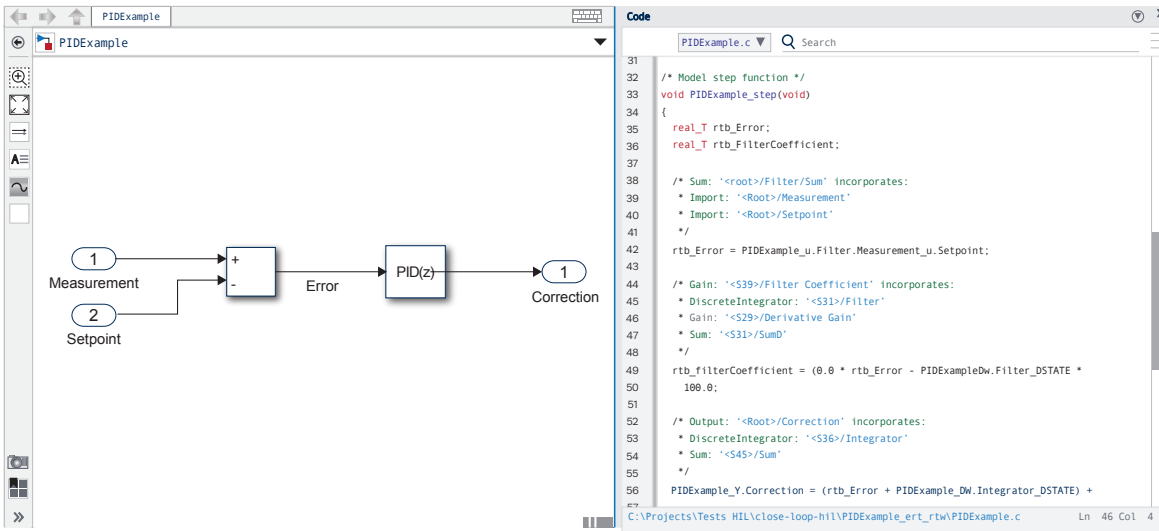
The overall process follows a V-cycle, shown in [Figure 2](#). Based on global requirements, the software architecture is designed. For Rehlko controllers, it is split into six main modules:

- **Metering:** electrical measurements, sampling, and signal processing
- **Monitoring:** electrical protection and signal quality assessment
- **Controller status:** global state of the controller, events management (incidence of pressed buttons or changes in the environment)
- **Power plant management:** interaction between controllers within a power plant and power-sharing algorithms
- **Power unit management:** start/stop, control of the engine (speed) and alternator (voltage), fuel and cooling control
- **Control device management:** control of breakers and switchgear



Each of these modules is further divided into unitary functions, called software components, designed to be reusable across all controllers of our brand. These components are expressed as models, which can be directly used as documentation for both engineering teams and field technicians. A simple example of a PID controller is shown in [Figure 3](#) (on the left).

Figure 3 Example of code generation for a simple PID controller



Finally, C code that follows industrial standards such as [MISRA](#) is automatically generated from each of these functions (on the right), concluding the development phase (left branch of the V-cycle in [Figure 2](#)). This modular decomposition improves clarity, facilitates parallel development across teams, enhances maintainability over the lifecycle of the controller, and supports long-term platform consistency across installations and software releases. In comparison, classical development would directly move from software architecture to C code, which is more difficult to understand and communicate about.

Each software component can be validated individually through rigorous unit testing, even if the rest of the code is not yet ready, ensuring compliance with its intended functionality before integration. This step is critical to building a reliable foundation, as it allows early detection and correction of defects in a controlled environment, reducing the risk of complex issues during later integration phases.

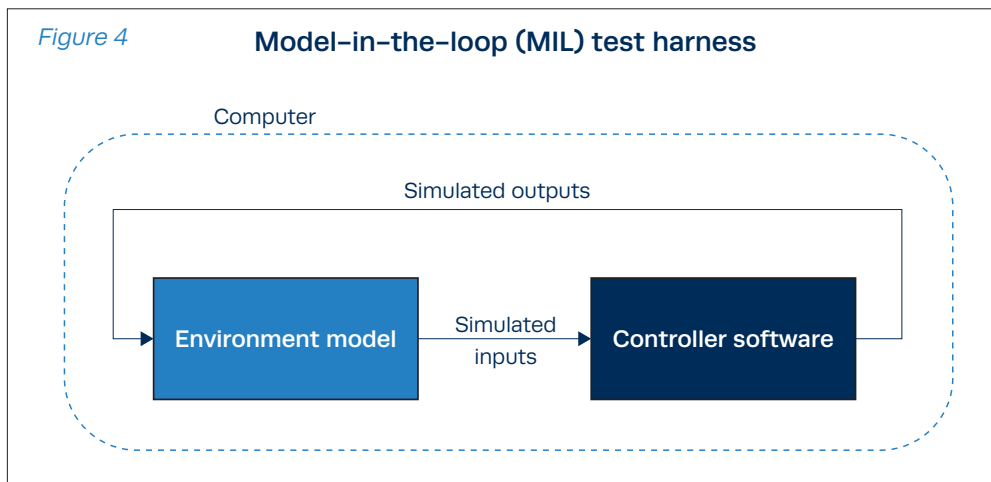
MULTI-LEVEL VALIDATION AND CONTINUOUS VERIFICATION

Ensuring the reliability of genset controllers requires an equally rigorous and comprehensive validation strategy. Given the complexity of modern control systems, no single test environment can fully represent all operating conditions. A progressive, multi-level validation framework is therefore essential to systematically reduce development and operational risk, build confidence in controller behavior, and support mission-critical power systems (right branch of the V-cycle in [Figure 2](#)).

The validation process implemented by Rehlko is based on successive testing environments of increasing realism, allowing both early detection of issues and validation under near-real operating conditions.

FIRST STAGE – TESTING EACH SOFTWARE COMPONENT

In the first stage, each software component is tested individually using Model-in-the-Loop (MIL). The environment of the software component is represented by an environment model which provides inputs and analyzes the outputs. The assembly of the model to be tested and the environment model is called a test harness, as shown in *Figure 4*. At this stage, control logic and interactions between functions can be evaluated early, allowing rapid iteration without hardware constraints.



SECOND STAGE – COMPLETE SOFTWARE VALIDATED

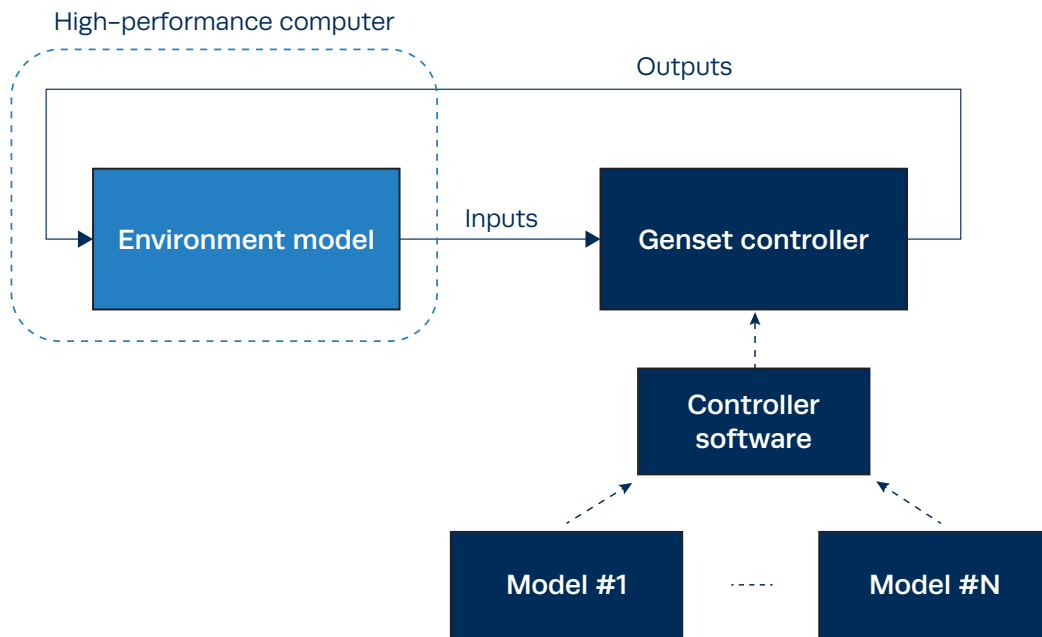
In the second stage, all the required software components are integrated into the complete controller software. This integration can also be tested first with MIL and a more complete environment model, whose behavior is similar to the actual genset response, validated independently by comparison with certified laboratory tests. At this step, the complete software is validated, but the interactions with the hardware (operating system, communication, etc.) are assumed to be perfect and the execution of the code is not real-time.

To achieve more precise validation, the complete software is embedded in the final hardware, while the environment model runs on a high-performance computer reproducing the behavior of a genset with real-time accuracy (see *Figure 5*). This computer is connected to the controller using the final connectors (CAN, Ethernet, digital or analog I/Os).

This setup is called Hardware-in-the-Loop (HIL) validation and provides a critical confidence-building step before full-system testing, enabling extensive verification of controller behavior while maintaining complete control over test conditions.

Figure 5

Hardware-in-the-loop (HIL) test harness

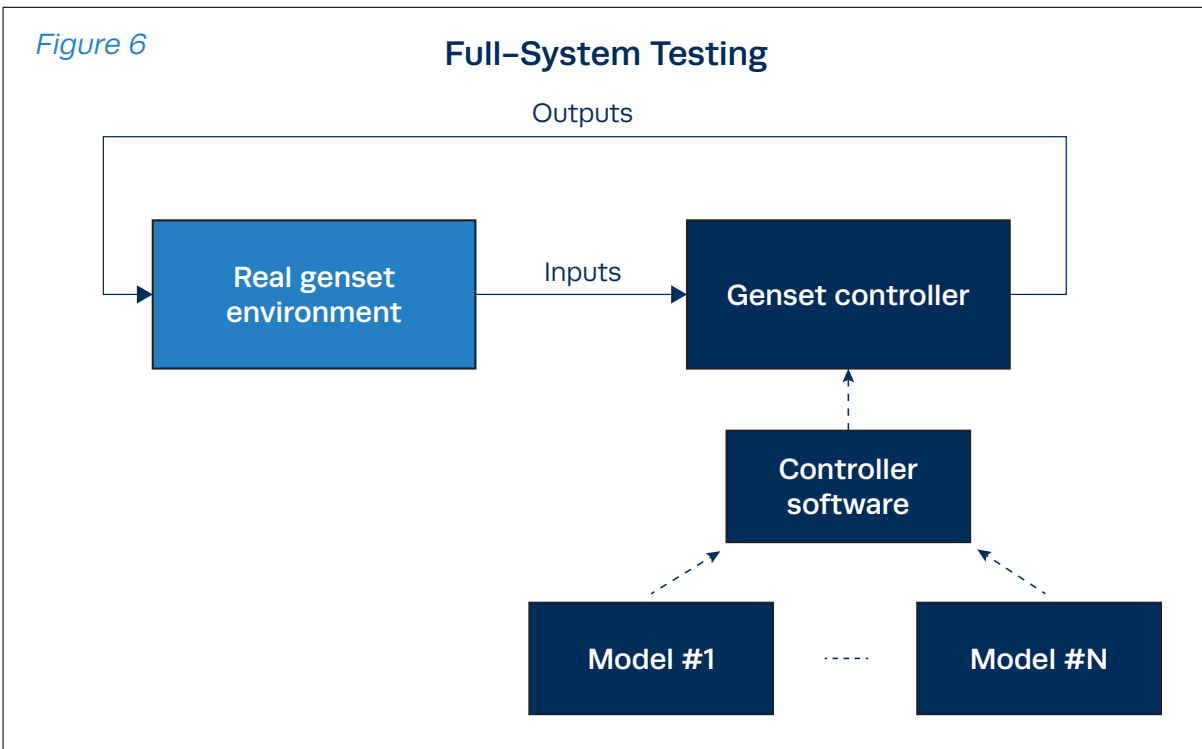


This crucial integration step is further extended through Power Hardware Simulation, where real physical components – such as alternators, breakers, and other electrical equipment – are integrated into the test environment. The fuel engine is replaced by an electric motor powered by the electrical grid, while the rest of the environment remains identical to the final one. This level allows the highest possible level of validation without using an engine.

This validation framework provides a controlled and scalable way to explore a wide range of operating scenarios, including rare and extreme fault conditions that would be difficult, unsafe, or impractical to reproduce on physical equipment. Typically, in our internal testing campaigns, more than 90% of identified software issues can be detected through this multi-level validation framework before full-system testing, reinforcing confidence in software maturity while avoiding fuel consumption.

FINAL STAGE – FULL-SYSTEM TESTING ON GENSETS

Finally, Full-System Testing is performed on real gensets in operational conditions (see [Figure 6](#)). This stage confirms overall system behavior, ensuring that all components – mechanical, electrical, and control – operate together as expected.



Beyond these validation levels, a key element of the approach lies in continuous verification. At each stage, iterative testing and correction cycles are conducted to identify and resolve defects as early as possible, as shown by the horizontal arrows in the V-cycle in [Figure 2](#). This automated testing framework ensures that any software modification does not introduce unintended side effects, maintaining system stability over successive releases.

KEY BENEFITS FOR END USERS

The combination of a structured development approach and a comprehensive validation framework delivers tangible benefits for end users across a wide range of applications.

First and foremost, it contributes to predictable and consistent system behavior. By validating controller operation across multiple environments and operating conditions, Rehlko ensures that the controller behaves as expected when reliability matters most.

It also contributes directly to risk reduction and operational confidence. This systematic verification throughout development and maintenance reduces uncertainty, which is required for long-term operation in mission-critical environments.

Another key benefit lies in the ability to validate extreme and rare scenarios. Simulation-based environments enable the testing of edge cases — such as electrical faults, abnormal operating conditions, or complex multi-generator interactions — that would be difficult, unsafe, or impractical to reproduce on physical systems. This leads to a higher level of system resilience under real-world conditions.

In addition, the approach improves cost efficiency and environmental performance. By reducing reliance on physical testing during development, it limits fuel consumption, test duration, and the need for extensive on-site validation campaigns.

Finally, the structured methodology enhances software quality, lifecycle support, and long-term maintainability. Clear architecture, modular design, and systematic non-regression testing help ensure that future updates can be deployed with confidence, supporting evolving requirements such as cybersecurity.

By delivering robust, validated, and maintainable control solutions, this approach enables operators to rely on their genset systems with a high level of confidence — ensuring continuity of operations in even the most demanding environments.

The methodology was first deployed on the APM804 controller platform and has demonstrated its ability to support complex applications ranging from standby power installations to large multi-generator Data Center architectures. The lessons learned from this program now form the basis for any future controller developments within Rehlko.

Why This Matters for Data Centers

Data Center operators prioritize availability, predictability, and risk mitigation above all else. Rehlko's controller development and validation methodology directly supports these objectives by delivering:

- Predictable generator response during utility failures.
- Consistent behavior across projects, sites, and deployments.
- Reduced operational risk through extensive validation.
- Compatibility with mission-critical power architectures.
- Confidence in the long-term software maintainability and lifecycle support.

This approach helps reduce uncertainty during both infrastructure design and long-term operation, providing a strong foundation for Data Center-ready power solutions.

CONCLUSION

Ensuring the reliability of modern genset controllers requires more than robust hardware. It requires robust software, which is achievable only with a disciplined development process focused on predictable behavior, systematic validation, and continuous verification throughout the software lifecycle.

By combining Model-Based Design principles with comprehensive multi-level validation, Rehiko has extensively applied a proven methodology that reduces uncertainty and increases confidence in controller operation across a broad range of operating conditions.

For Data Center operators and other mission-critical users, predictable behavior is often more valuable than peak performance. Rehiko's development and validation framework is designed to deliver consistent operation, support architecturally sound power systems, and enable long-term lifecycle reliability.

Through this commitment to engineering rigor and continuous improvement, Rehiko provides Data Center-ready control platforms that help customers reduce risk, maintain availability, and operate with confidence throughout the life of their installation.



ABOUT THE AUTHOR

Hadrien Pinault is a Staff Engineer at Rehlko Power Systems EMEA. He holds a PhD in numerical modeling applied to complex systems. His academic and industrial experience spans multiple domains, including railway systems and renewable energy, where he has developed advanced expertise in modeling, control, and system validation.

His work at Rehlko focuses on Model-Based Development methodologies and their application to the design and verification of embedded control systems. Through his work, he addresses the challenges associated with complex, interconnected power systems while contributing to the transition toward more sustainable and environmentally responsible energy solutions.

ABOUT REHLKO

A global leader in energy resilience, Rehlko delivers innovative energy solutions that sustain and improve life across home energy, industrial energy systems, and powertrain technologies with control, resilience, and innovation. Leveraging the strength of its portfolio of businesses — Power Systems, Clarke Energy, Home Energy, and Engines—and its more than a century of industry leadership, Rehlko provides power where and when the grid cannot. Rehlko goes beyond function and individual recovery to create better lives, communities, and a more durable and energy-resilient future.