D550 Cybersecurity Information

RELEASE LIST

INDICES	DATE	MODIFICATION
A	18/11/2025	Creation

VALIDATION

Action	Responsible	Date	VISA
Writer	Moser, Samuel	18/11/2025	
Check by	Morisseau, Vincent	19/12/2025	
Validation	Péru, Philippe	19/12/2025	

- Summary -

1 INTRODUCTION

The aim of this document is to provide a comprehensive information related to the cyber security of the D550 on any critical applications such as marine application.

Remark: This document is not a Cybersecurity Certificate of Compliance for the D550 regulator.

Remark: Two acronyms used in this document are identical with different significations. IACS could mean Industrial Automation and Control System and could mean International Association of Classification Societies relative to marine certification.

2 DOCUMENTS REFERENCES

1. D550 Safety Instructions 5779_fr-en
2. D550 Datasheet 5723_en
3. D550 Installation and maintenance 5744_en
4. IEC 62443 Industrial Security Standards Series.
5. Directive (EU) 2022/2555 - NIS 2 Directive Legislative Act Aiming to Achieve a High Common Level of Cybersecurity Across the EU.
6. IACS UR E26, UR E27
7. NIDEC POWER: Cybersecurity on Automatic Voltage Regulator (AVR)
8. Regulation (EU) 2024/2847 - Cyber Resilience Act

3 GENERAL INFORMATION

The following document covers NIDEC POWER LEROY-SOMER multi-layer approach to cybersecurity in an industrial automation and control system (IACS) with NIDEC POWER LEROY-SOMER Automatic Voltage Regulator (AVR) and following the IEC 62443 Industrial security series of standards including IACS UR E26 and UR E27.

NIDEC POWER LEROY-SOMER customers or integrators companies increasingly use commercial off-the-shelf (COTS) networked devices that are inexpensive, efficient, and highly automated. NIDEC POWER LEROY-SOMER products could be connected to untrusted networks for automation reasons. These COTS devices, open networking technologies and increased connectivity provide an increased opportunity for cyber-attack against control system hardware and software.

Company organizations may use business information technology (IT) cybersecurity solutions to address industrial automation and control system (IACS) security. While many business IT applications and security solutions can be applied, they need to be applied in an appropriate manner to eliminate inadvertent consequences. For this reason, the approach used to define system requirements needs to be based on a combination of functional requirements and risk assessment, often including an awareness of operational issues as well.

The fundamental principle of cybersecurity is a strong cybersecurity process lifecycle. This lifecycle needs to include adequate training, tools, resources, and processes to develop, harden and maintain the resiliency of the equipment under control (EUC) against cyberattacks. The lifecycle approach is also a fundamental premise of best practices utilized for various cybersecurity standards and approaches.

Cybersecurity of industrial control systems can often include three threat categories:

Industrial control systems threat categories	
Hacking	An attacker targeting an industrial control system this could be by creating dedicated malware.
General malicious software	An employee connects a laptop to the system network or inserts a USB stick into a server. The purpose of these actions could be benign, but there is a significant risk of infected devices transferring an infection to the automation system. Even though it is not designed to damage systems, it can be very harmful.

Employee mistakes	An engineer wants to update the control logic in an embedded device, but by mistake connects the engineering tool to the wrong device. Similarly, an engineer connects a network cable to the wrong port of a network switch.

Table 1. Common threat categories for industrial control systems.

There are various Directives, Requirements and Technical Rules which cover cybersecurity, and which use IEC 62443 Industrial communication networks - Network and system security. Examples are briefly covered in this document along with IEC 62443 Industrial communication networks - Network and system security series of standards.

Note: When designing a control system to meet the set of control system requirements associated with specific target security levels, it is not necessary that every component of the proposed control system supports every system requirement to the level mandated in IEC 62443 Industrial communication networks - Network and system security series of standards.

NIDEC POWER LEROY-SOMER has decided to engage a wide cybersecurity approval for their digital excitation systems to become the first automatic voltage regulator to achieve it on the market. Those ongoing processes are on one side focusing marine applications to certify the product under IACS UR E27, also meeting the IACS UR E26 requirements, to contribute to the security of the vessels against cyber threats. On the other side and to offer cybersecurity resilience beyond the marine application for all critical applications such as datacenters, hospitals, government agency emergency power generation, NIDEC POWER LEROY-SOMER engaged also IEC62443 component certification process.

To ensure resilience in the face of potential cyber threats, the D550 has been internally evaluated for compliance with the Cyber Security Profile 3 (IACS UR E27), which is based on industry standard IEC 62443-3-3 security level 3. The certification processes are ongoing with some marine certification bodies, which are the world's classification society leaders, as well as a recognized advisors to the maritime industry.

4 COMMUNICATIONS, PHYSICAL LAYERS & PROTECTIONS

The following diagram shows an example system with NIDEC POWER LEROY-SOMER Automatic Voltage Regulator with a trusted zone and potential untrusted networks. From the cybersecurity approach there are several cybersecurity related risks. Remote connections have been implemented typically for programming, system management and servicing. The cybersecurity target is to secure the system and connections using gateways, firewalls, user security codes and controlling access to the system and any additional local networks and operator systems.

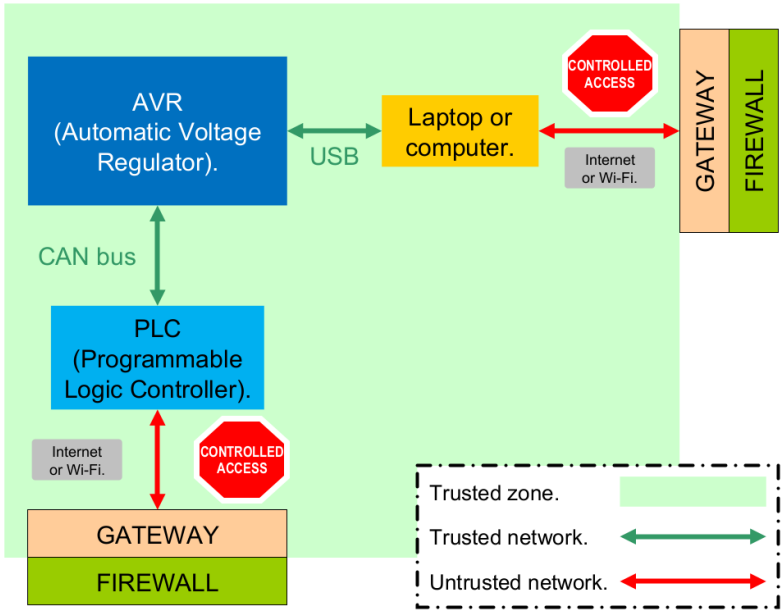


Figure 1. Application example: trusted zone, trusted, untrusted networks

4.1 Device overview

The D550 is a digital Automatic Voltage Regulator (AVR). It is one of the major components in an electric power generation system, measuring the electric constants and providing the required excitation current for brushless synchronous generators. It can operate many different regulation modes according to the system requirements such as island voltage regulation, parallel operation in generators voltage regulation, local or remote Power Factor regulation, local or remote Reactive Power regulation and direct excitation control. It can provide up to 7A continuous excitation current and temporary 15A for the forcing.
The D550 can operate with internal setpoints in complete autonomy without need of external equipment or can work as a part of a completely interconnected industrial system with a remote control from the control room or another control system. This remote control could be a hardwired analog or digital inputs / outputs or/and could be digitally controlled by a CANBUS connection.

4.2 Disclaimer for cybersecurity

The D550 is designed to operate as an isolated component without need of external control but can be configured for transmitting and receiving data via a network interface. This option offers the final user a wide range of possibilities and features. NIDEC POWER LEROY-SOMER highlights that it remains the sole responsibility of the customer to provide and continuously ensure a secure remote connection between the product and the customer network or another network if configured. The customer must take and maintain all suitable measures (such as, but not only, the installation of firewalls, the application of authentication measures, the encryption of data, the installation of virus protection programs, etc.) to protect the product, the network, its system, and the interface against any type of security breach, unauthorized access, interference, intrusion, leakage and / or theft of data or information. NIDEC POWER LEROY-SOMER and its subsidiaries are not liable for any damage and / or loss related to such security breaches, unauthorized access, interference, intrusion, leakage, and / or theft of data or information.

4.3 Cybersecurity best practices

This section offers recommendations for the D550 AVR usage with better cybersecurity resilience. It provides basic recommendations and best practices to ensure that the D550 integration into systems is considering the cybersecurity risks at the good level. We highly recommend:

- The D550 excitation system must be installed in a physically secured and controlled area like a mounting into an electric cabinet (secured by a key at minimum) or into the generator terminal box in respect of the D550 safety instructions. Electric room access must be secured and locked with restricted access to prevent bypassing the physical access barrier. All those restrictions should be maintained operational for the complete product life cycle.

- The D550 is designed to be integrated into an electric generation installation or an excitation control circuit of an electrical machine and can under no circumstances be considered as a safety device itself. It is therefore the responsibility of the designer of the installation or the user to consider all precautions to ensure that the system complies with current protection standards, and to provide any accessory devices required to ensure the safety of the equipment and the personnel (especially direct contact with connectors when the AVR is running).

- The D550 AVR must be configured only by trained qualified people who have knowledge of the electric power generation, their limitations, and their protections. This recommendation is also applicable on all remote access to the D550 disregards if it's hardwired digital/analog or by a communication bus that could be external of the electric room.

- Never connect the D550 AVR to any network if not required.

- The D550 could operate isolated without need of external equipment. If a connection to a network is required, make sure the D550 is used locally within a trusted network utilizing proper network infrastructure controls. This will help ensure that unused or unnecessary protocols from unauthorized sources are blocked.

- When remote access is required, use approved secure methods for field bus communication.

- We highly recommend using the dedicated field bus that is exclusively configured for the intended purpose (monitoring, process) and separate it physically from other field buses. If this cannot be possible, ensure that

control systems and devices are situated behind firewalls, ensuring their isolation from the corporate network. If possible, the control processes should be hardwire defined to avoid any cyberattacks on them.

- If a modification or an upgrade of the system should be applied, the cybersecurity assessment risk should be performed again, the analysis and the modification report should be well documented.

- If requested by the service, there are possibilities to access the D550 using a computer and EasyReg Advanced software. Prior to connecting to the D550 or to any component of the same communication network, the computer should be carefully scanned for viruses.

- The EasyReg Advanced application should be exclusively downloaded from a trusted source like the official NIDEC POWER LEROY-SOMER website or any trusted technical people from NIDEC POWER LEROY-SOMER. The latest release is highly recommended to ensure the best cyberattack protection. A SHA-256 hash key of installer package is provided and must be checked before installation on the computer to ensure having an original installation package.

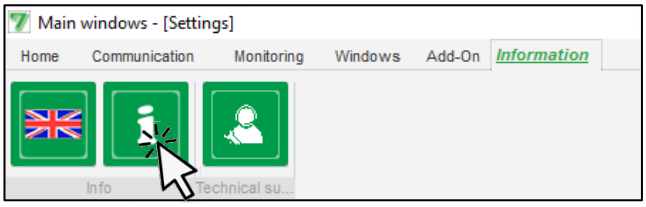
- The D550 excitation systems must be configured with a locking pin code to ensure a full writing protection to fulfil the basis of cybersecurity protection.

5 D550 FIRMWARE AND EASYREG ADVANCED APPLICATION RELEASES

To ensure having the latest cybersecurity protections on the D550 and the software configuration application, check the latest official releases of the D550 on the NIDEC POWER LEROY-SOMER official website with details of corrections/improvements:

- D550 Firmware release note: https://moen.nidec.com/en-US/power/Products/electronic-products/digital-voltage-regulator/D550-voltage-regulator
- EasyReg Advanced release note and download: https://moen.nidec.com/en/power/Downloads/Softwares/EasyReg-Advanced

The firmware version can be checked using the D550 EasyReg Advanced software application, click Info button to display EasyReg Advanced version (module version) and D550 firmware (Application release) if the D550 is connected to the computer:



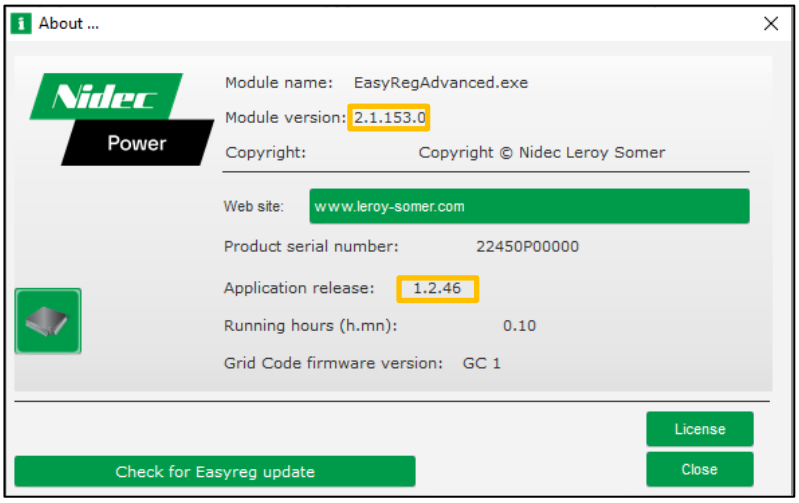


Figure 2. EasyReg info screen example

6 D550 HARDWARE DETAILS

6.1 Connector and interface identifications

1. Grid Voltage Sensing
2. Generator Voltage Sensing
3. PT100 Temperature Sensors
4. Analog Inputs/Outputs
5. Digital Inputs/Outputs
6. Relay Outputs
7. Generator Currents Sensing
8. AC Power supply
9. Excitation Output
10. DC supply
11. CANBUS port
12. USB-B port

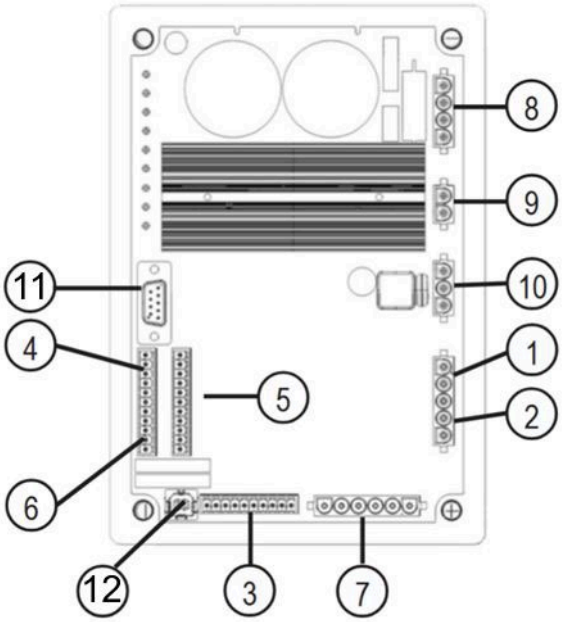


Figure 3. D550 inputs/outputs

Dual plate option

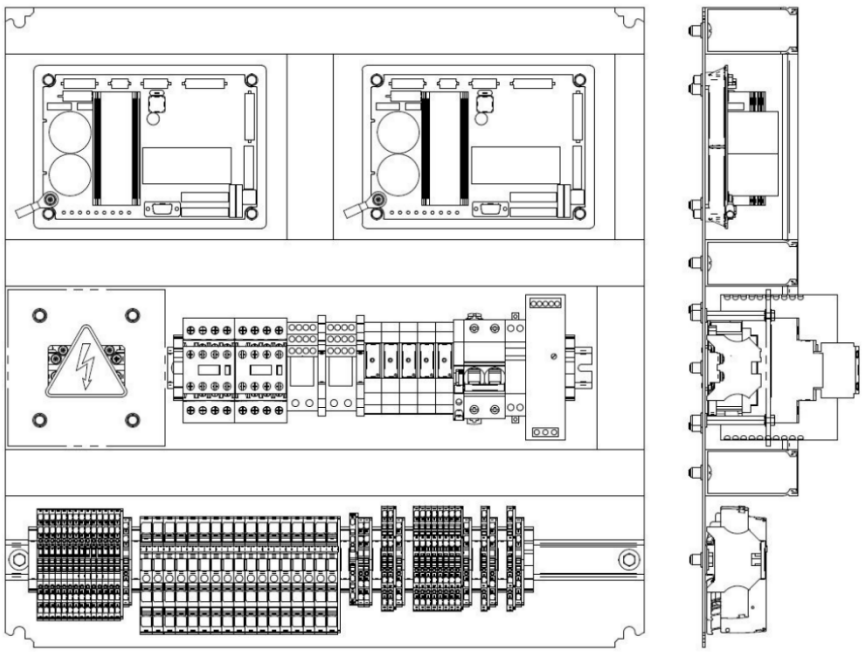


Figure 4. Dual plate drawing

Note: The dual plate option consists of an assembly of 2 D550 AVR and other necessary components to perform the active redundancy between the two AVR. In this configuration, to ensure the correct switching between the 2 AVR in a bumpless behavior, the usage of communication ports for writing operations is forbidden. Only monitoring (read only) is accepted in this configuration.

6.2 Communication ports details

- **USB port**

  - **Configuration:**
    This interface is a standard B USB connector dedicated for configuration and commissioning. The D550 USB is configured as a HID device with VID 0x1D65 and PID 0x000B with full speed interface. USB activity is displayed on front LEDs with the USB symbol. It should be light blue when connected, correctly enumerated and active with the application software. This USB port is not designed to perform permanent communication with a computer. It should remain disconnected during normal operation.

  - ***Cybersecurity considerations***
    The USB must not be defined as a permanent communication port especially in a critical system. All precautions should be applied to ensure the USB port is not accessible in operation. Per examples and not exhaustive list, these solutions are acceptable: a key closed door of electric cabinet, a technical room key locked, the need of tool to access the generator terminal box. In any case the USB writing must be configured with write locking with a pin code. Configuration of this write locking function is described in § 7.4.3. All these protections could be combined.

- **CAN port**

  - **Configuration:**
    The CAN BUS interface is available on the D550 on its D-SUB male connector placed near LEDs indicators. This connector drives CAN BUS lines and specific signals for D550 options which can be connected to it. A DC supply (15V 200mAmax.) is also available on this connector dedicated to supply light CAN BUS peripherals. This DC supply can be enabled or disabled by the product. See D550 CAN BUS Interface document for more details about CAN BUS configuration

  - **Cybersecurity consideration:**
    The CAN BUS interface is preferred for permanent communication over the USB port. During normal operation, protection measures should be applied to prevent tampering with the port, which can lead to service interruption of the devices connected to the regulator this way. Such measures include, but are not limited to, restricted access to the electric cabinet such as a key lock, restricted access to the operation room, required tool usage to access the device or generator terminal box. If not required by the devices, it is highly advised to disable configuration write over the CANBUS or enable the PIN write protection as described in § 7.4.3. All these mechanisms can be combined for best protection

7 SOFTWARE PACKAGE

7.1 D550 core

The D550 is a digital AVR based on 32 bits microcontroller and an IGBT power bridge controlling the excitation current of a brushless synchronous alternator. It embeds a power bridge capable to control an excitation current up to 7A continuous and 15A for field forcing.

The 32 bits microcontroller platform manages all AC voltage and current measurements, temperature probes and customer I/O.

The software is a proprietary internal development and not based on any Operating System. The main functions are measurements and regulations and are defined as the highest priority level in the tasks list. The communication layer (USB, CAN bus…) is executed in the lowest priority tasks of the program. This strategy ensures to the D550 a high reliability in case of communication fault or cyber-attack, the regulation will continue to run despite a frozen communication task.

Internal functions are prioritized as hereunder:

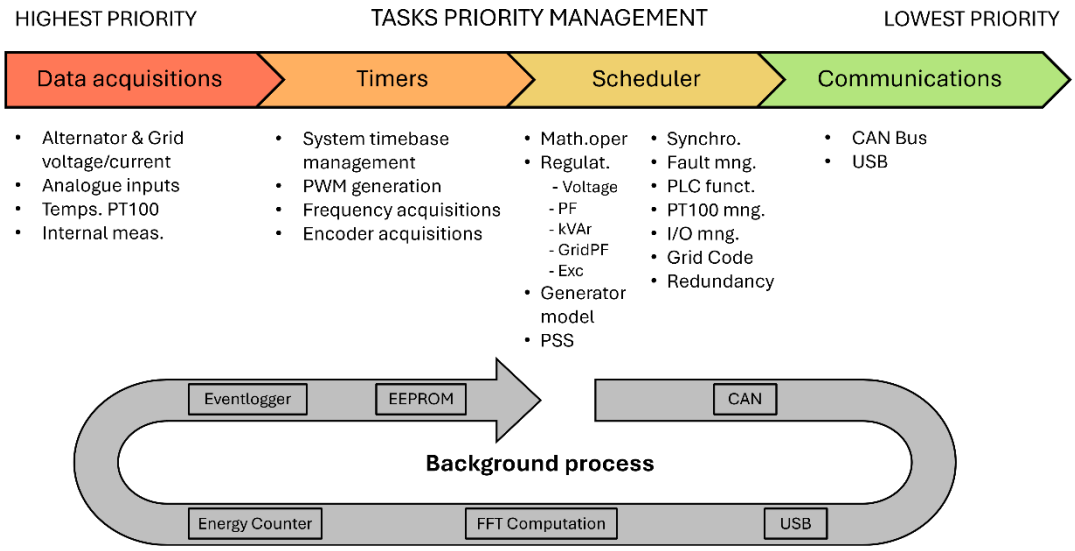


Figure 5. D550 Tasks priority diagram

7.2 D550 digital AVR features package

<u>The D550 firmware is managing these functions:</u>

- **Data acquisitions:**
  RMS for voltages and currents
  Frequency for generator and grid
  Unbalanced floating neutral composition
  I/O measurement
  Internal measurement
  Power calculations
  Encoder reading

- **Generator configuration:**
  Generator data (database)
  Excitation data

- **Wiring configuration:**
  Stepdown volt. transformers (Generator, Grid, …)
  Step-up voltage transformer
  Current transformer ratios
  Power bridge control
  Redundancy
  Temperature probes

- **Excitation limitations:**
  Thermal limitation
  Forcing limitation

- **Generator capability curve:**
  Limitation definition
  Absorption control PID

- **Start-up:**
  Soft-start
  Start on Threshold

- **Engine helps:**
  Equalization with grid
  Synchronization

- **Protection management:**
  Under/over voltage
  Under/over frequency
  Rotating diode faults
  Direct motor start failure
  Reverse or over active/reactive power
  Stator overcurrent
  Loss of sensing
  Short-circuit detection
  Unbalanced voltage/current
  Power supply fault
  Power circuit fault (internal/external)
  Excitation chain fault
  Phase rotation fault
  Pole slipping
  Temperature faults
  Fault redundancy
  Analog current input/output wirebreak fault
  Fault group management

- **Voltage regulation:**
  Setpoint limitation
  Setpoint control origin
  Knee and slope underspeed definition
  Reactive droop compensation
  Reactive load sharing
  Line drop compensation

- **Generator PF regulation / kVAr regulation / Grid PF regulation:**
  Setpoint limitation
  Setpoint control origin
  Autoswitch source
  Control switch

- **Field current regulation:**
  Setpoint limitation
  Setpoint control origin
  Follower
  Control switch

- **PID regulation loops:**
  Voltage
  PF/kVAr
  Field current
  Grid PF

- **I/O management:**
  Digital inputs/outputs affectation and logic level
  Analog I/O affectation and signal mode

- **PLC logic/analogic gates:**
  User variable management
  Source / destination management
  Gates management

- **Curves functions:**
  Curve definitions
  Source/destination management

- **User PID:**
  PID definitions
  Source/destination management

- **Grid code:**
  LVRT/HVRT Profiles
  Pole slipping monitoring
  Forcing control in PF/kVAr
  Q=f(U), Q=f(U)lim, Q=f(P) regulations
  Setpoint settling time control

- **Dual configuration:**
  Switch parameter control
  Analog parameter control

- **Monitoring:**
  FFT analysis
  Complete electrical parameter measurements

Note: this is not an exhaustive list

7.3 D550 firmware upgrade package

To upgrade the D550 on the field, the service people must use EasyReg Advanced software and an encrypted firmware ". Hex" file provided by the NIDEC service support team. The software will reject all firmware files that are not recognized with the right encryption.
To access the firmware upgrade mode, go to "Information" and click on the microcontroller button. A SHA-256 hash key could be provided to the customer to ensure the integrity and authenticity of the firmware.

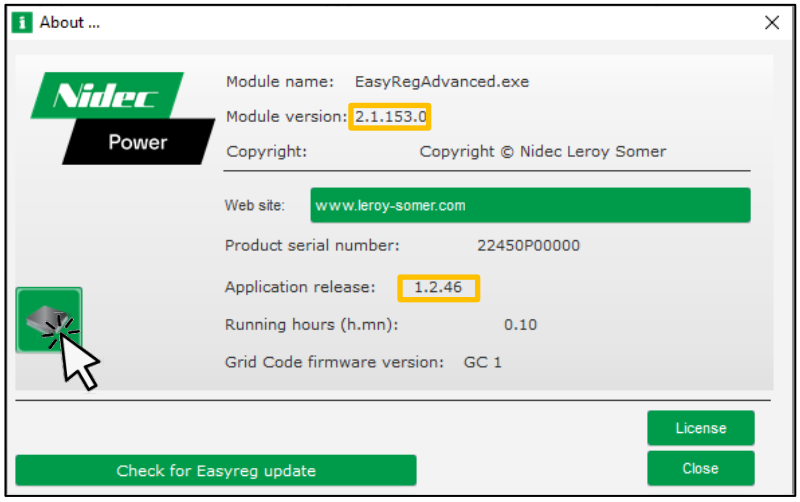


Figure 6. Firmware upgrade button

7.4 EasyReg Advanced Software

The EasyReg Advanced software is the main platform for product configuration. The software installation package comes with 3 sub-softwares dedicated to the 3 digital regulators D350, D550 and D700. Each sub-software uses the same common libraries, and the interface is customized according to the product options and capabilities.
EasyReg Advanced is an internal development developed for Microsoft Windows 10 and Windows 11 Operating Systems. This software is voluntary proposed as a freeware available on our official website to ensure limiting a third-party software development which is not guaranty by our technical team. This is the unique Windows based software to configure the D550 AVR. The tool must not be used in a system design and must be only used for configuration and commissioning purposes. The download link is described in paragraph 4.

7.4.1 Managed files description

- Installation package (.EXE file)
  A SHA-256 hash key is published next to the installation package downloaded by the customer to control the integrity of the file. The customer could generate himself the SHA-256 hash key and compare it to the published one. A changelog is provided for each software release. An access to older versions is also provided. The installation package is a ".exe" file extension and doesn't require administrative privileges.

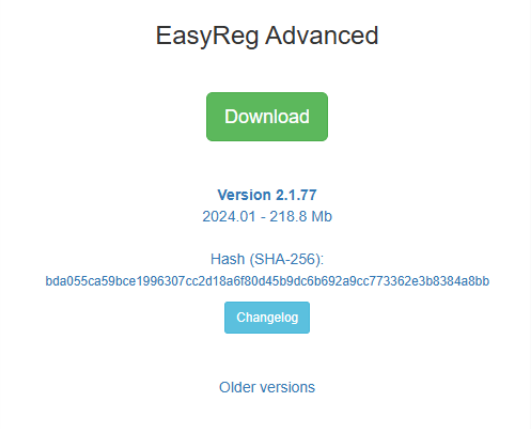


Figure 7. Download section for EasyReg Advanced (example)

- Configuration file (.550 file)
  The EasyReg Advanced software on the D550 Sub-software create/open/write the configuration file with ".550" extension. This ".550" is an encrypted file of the binary configuration file. Only the official software is able to manage this file format.

- Parameter list Configuration file (.xlsx file)
  The EasyReg Advanced software can export a parameter list file in Excel format with readable details. This ".xlsx" file can be used by the final customer to know all of the configuration details for personal use. This file format cannot be used by EasyReg Advanced for a configuration input.

- Oscilloscope configuration file (.7osc)
  This configuration file is a text readable file which contain all parameters for configuring the oscilloscope monitor proposed by EasyReg Advanced. It could be further opened to automatically configure the oscilloscope.

- Oscilloscope data file (.csv)
  This datafile is the record result of data stream displayed on the EasyReg oscilloscope. It contains all of the oscilloscope configuration (curve details, scales, color,…) for a further analysis.
  This file is not encrypted and can be opened with any CSV application. It could be loaded again by the EasyReg Advanced oscilloscope module.

- Monitoring configuration file (.tdbconf)
  This configuration file is a text readable file which contain all parameters for configuring the parameter monitor screen proposed by EasyReg Advanced. It could be further opened to automatically configure the monitor screen page.

- Configuration report (.pdf)
  The EasyReg Advanced software can generate an automatic report of the current configuration. This report is exported in pdf format for further use by the installer/customer.

7.4.2 Software access levels

EasyReg Advanced software is the official configuration tool developed and provided by Nidec Leroy-Somer. It's defined as a freeware and can be downloaded from the official Nidec Leroy-Somer website (see paragraph 4). That means that any people can download it and install it on their computer. We highly recommend the installer to secure

the electric area and the D550 electric cabinet avoiding any access to not trusted people. With this minimum level of protection, we ensure that only skilled people can access the D550.
There are 2 different access levels in the software according to the requested operation:

- USER:
  This is the read only mode. In this mode, the connected people are fully sure that no modification can be performed on the current configuration and no risks of bad software handling. This is the preferred mode for monitoring parameters.

- EXPERT:
  This is a read/write mode. In this mode, the connected people can adjust some parameters, modify the partial or complete configuration. It could be used for monitoring as well.

7.4.3 EasyReg Advanced optional modules

Special applications could require specific configurable modules:

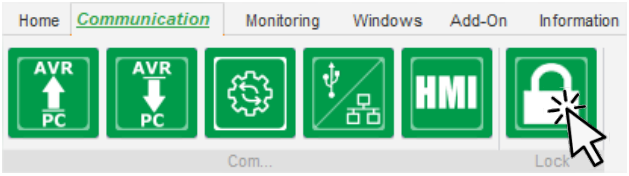
- PSS: Power Stabilizer System
  This enables a configuration page for configuring the PSS according to PSS2B model

- PID Auto:
  This enables a configuration page for the regulation loop autotuning

7.4.4 D550 communications write locking configuration

To guarantee no further configuration change after the system commissioning and to enhance cyberattack resilience, the D550 could be write locked. Once configured, the D550 will internally reject any write attempt coming from the selected communication interfaces.

The configuration page is accessible by clicking on this EasyReg Advanced button when a D550 is connected on the computer.



This opens a configuration window to enable the write locking function on the selected communication channels.
The password format is a 6 digits maximum numerical value.

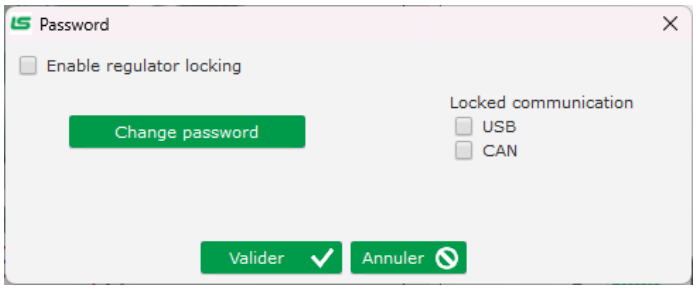


Figure 8. Write lock configuration window

8 MAINTENANCE PRACTICES, SECURITY ENHANCEMENTS AND RECOVERY PLAN

NIDEC POWER LEROY-SOMER recommend the maintenance organization to save and secure each D550 configuration file (1 per D550 of the current system) with EasyReg Advanced in a secured area only accessible by authorized peoples.

NIDEC POWER LEROY-SOMER recommend the maintenance organization to write lock every communication port after a commissioning.

In case of maintenance purposes, the skilled authorized maintenance people could replace the current D550 by a new D550 that could be preconfigured in their office with the pre-saved configuration files. The write locking passwords could be defined in office before replacement on site to ensure completing the cybersecurity plan for D550.

In case of different firmware version between on-site product and replacement product, the maintenance organization could contact the technical support to ensure the full compatibility between products.

NIDEC POWER LEROY-SOMER recommend the maintenance organization to define a periodic password change task. This periodic task should be included in the global password change policy of the user company.

The user company should ensure to regularly train their people to the cybersecurity risks, the measures that can be put in place to mitigate those risks especially the regular password change.

We recommend to synchronize this password change with the maintenance schedule of the system.

The maintenance organization should ensure that all their authorized peoples are notified with this password change through their own communication channels or internal meetings. Passwords should be stored in a secured area only accessible by authorized peoples.

The maintenance organization should also define a periodic check of the available firmware and/or software update. This action ensures the organization to have the latest up-to-date cybersecurity protection for its system. Some upgrades are not mandatory and may not concern the cybersecurity. The maintenance organization should evaluate the impact of the upgrade to their own system to evaluate the usefulness of the available upgrade. In case of doubt, the maintenance organization could contact the NIDEC POWER LEROY-SOMER technical support for more details.

The password change execution and firmware/software upgrades control should be recorded in the system maintenance log with date, maintenance people in charge of execution and next planned password change and upgrade checks. This record could be presented for security audits or other security checks.

In case of lost password, lost configuration or commonly any issues with D550, the maintenance organization could contact the NIDEC POWER LEROY-SOMER technical support to help in the recovery plan execution. The maintenance organization must prepare these information/documents for the technical support to ensure a fast and precise support:

- Short description of the maintenance organization with name, role and contact of technical skilled peoples
- Global description of the system and numbers of AVR involved.
- Schematic diagram of the system
- ".550" configuration files if available.
  ".550" configuration files could be generated by connecting the USB on D550 and import parameters from D550 to computer with EasyReg Advanced. This operation is still possible with a D550 write locked.
- D550 serial numbers
- D550 current firmware release
- EasyReg Advanced current release

8.1 Disclaimer for NIDEC POWER LEROY-SOMER Technical Support

This is not the NIDEC POWER LEROY-SOMER (described as “our company” hereunder) responsibility to ensure the right identity of the maintenance organization contacts and to secure all the exchanges.
In case of file exchanges between our company technical support and the customer organization, our company considers that all these file exchanges are under control of the customer maintenance organization.
This is the entire responsibility of the customer maintenance organization to guaranty that no third party or not authorized people could have access to their stored and secured files (configuration, diagrams, ...). Our company considers that if those files are shared with us, the customer company has given the right to exchange those data with us.
This is not our company responsibility for any mistakes or damages that could occur or result in case of a remote support.

8.2 NIDEC POWER LEROY-SOMER Technical Support

Our technical support could be accessible on the website:

https://moen.nidec.com/en/power/Contact-us/Contact/Contact-us-SERVICE

Or by e-mail:

service.epg@leroy-somer.com