



Boulevard Marcelin Leroy
CS10015
16915 Angoulême cedex 9
Tél. : 05 45 64 54 54

D700

Ref. D251013 01 RDE MS A
Date: 13/10/2025

D700 CYBERSECURITY INFORMATION




Document pages
Number: 17

D700 Cybersecurity Information

RELEASE LIST

INDICES	DATE	MODIFICATION
A	13/10/2025	Creation

VALIDATION

Action	Responsible	Date	VISA
Writer	Moser, Samuel	13/10/2025	
Check by	Morisseau, Vincent	19/12/2025	
Validation	Péru, Philippe	28/10/2025	

- Summary -

D700 CYBERSECURITY INFORMATION	1
VALIDATION	1
1 INTRODUCTION	3
2 DOCUMENTS REFERENCES	3
3 GENERAL INFORMATION	3
4 COMMUNICATIONS, PHYSICAL LAYERS & PROTECTIONS	4
4.1 Device overview	4
4.2 Disclaimer for cybersecurity	5
4.3 Cybersecurity best practices	5
5 D700 FIRMWARE AND EASYREG ADVANCED APPLICATION RELEASES	6
6 D700 HARDWARE DETAILS	7
6.1 Connector and interface identifications.....	7
6.2 Communication ports details	8
7 SOFTWARE PACKAGE	11
7.1 D700 core.....	11
7.2 D700 digital AVR features package.....	12
7.3 D700 firmware upgrade package.....	13
7.4 EasyReg Advanced Software	13
7.4.1 Managed files description	13
7.4.2 Software access levels	14
7.4.3 EasyReg Advanced optional modules.....	14
7.4.4 D700 communications write locking configuration.....	15
7.5 MicroSD card content	15
8 MAINTENANCE PRACTICES, SECURITY ENHANCEMENTS AND RECOVERY PLAN	16
8.1 Disclaimer for NIDEC POWER LEROY-SOMER Technical Support.....	17
8.2 NIDEC POWER LEROY-SOMER Technical Support	17



D700

D700 CYBERSECURITY INFORMATION

INTRODUCTION

1 INTRODUCTION

The aim of this document is to provide a comprehensive information related to the cyber security of the D700 on any critical applications such as marine application.

Remark: This document is not a Cybersecurity Certificate of Compliance for the D700 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. D700 Safety Instructions 5707fr/en
2. D700 datasheet 5420_en
3. D700 Installation and maintenance 5513_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 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. Industrial control systems common threat categories.

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 D700 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.

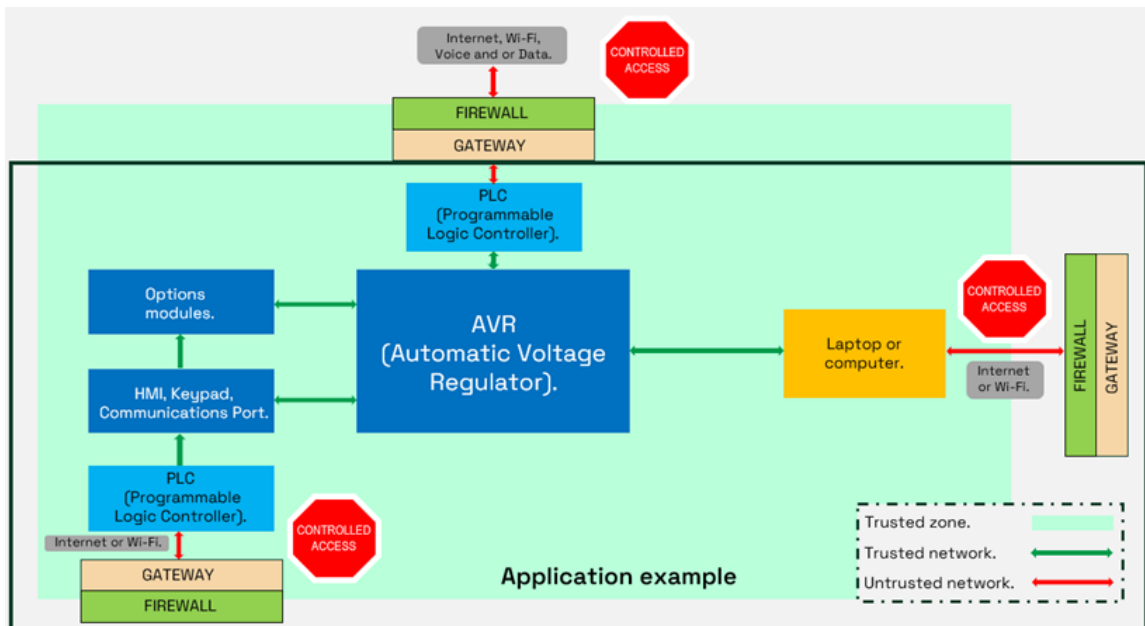


Figure 1. Application example: trusted zone, trusted, untrusted networks

4.1 Device overview

The D700 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 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 25A continuous excitation current and temporary 50A for the forcing.

The D700 can operate with internal setpoints in complete autonomy without need of external equipment or can work as a part of a complete interconnected industrial system with a remote control from 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 field communication bus or/and via an ethernet communication. It is also possible to operate the unit with the control panel on the front cover of the device (embedded HMI).

4.2 Disclaimer for cybersecurity



The D700 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 possibility offers to the final user a wide range of possibility and functionality. NIDEC POWER LEROY-SOMER highlight that it remains the sole responsibility of the customer to provide and continuously ensure a secured 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 proposes recommendations for the D700 AVR usage with a best cybersecurity resilience. It provides basic recommendations and best practices to ensure that the D700 integration into systems is considering the cybersecurity risks at the good level. We highly recommend:

- The D700 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 D700 safety instructions. The 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 D700 is designed to be integrated in an electric generation installation or an excitation control circuit of an electrical machine and can under no circumstances be considered to be 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 D700 AVR must be configured only by a trained qualified people who has knowledge on the electric power generation, their limitations, and their protections. This recommendation is also applicable on all remote access of the D700 disregards if it's hardwire digital/analog or by a communication bus that could be external of the electric room.
- The D700 is configurable through many interfaces like USB, Ethernet, front control panel (embedded HMI). To ensure a correct understanding of D700 behaviors, the system designer should limit as much as possible the number of configuration interfaces. All unused interfaces in the system must be disabled.
- Never connect the D700 AVR to any network if not required.
- The D700 could operate isolated without need of an external equipment. If a connection to a network is required, make sure the D700 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 secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.
- We highly recommend using the dedicated network that is exclusively configured for the intended purpose (monitoring, process) and separate it physically from other networks especially the internet network. If this cannot be possible, ensure that control systems and devices are situated behind firewalls, ensuring their

isolation from the corporate network. We highly recommend you to consider only the monitoring capability of the D700 in usage of ethernet connection. If possible, the control processes should be hardware 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 to the D700 by a computer and EasyReg Advanced software. Prior to connect to the D700 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 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 D700 excitation systems must be configured with a locking pin code to ensure a full writing protection to fulfil the basis of cybersecurity protection.

5 D700 FIRMWARE AND EASYREG ADVANCED APPLICATION RELEASES

To ensure having the latest cybersecurity protections on the D700 and the software configuration application, check the latest official releases of the D700 on the NIDEC POWER LEROY-SOMER official website with details of corrections/improvements :

- D700 Firmware release note : <https://moen.nidec.com/en/power/Products/electronic-products/digital-voltage-regulator/D700-voltage-regulator>
- EasyReg Advanced release note and download: <https://moen.nidec.com/en/power/Downloads/Softwares/EasyReg-Advanced>

On the D700 AVR, the firmware version can be checked by these methods:

- On the D700 HMI, click and maintain the left button to display the D700 firmware version screen:

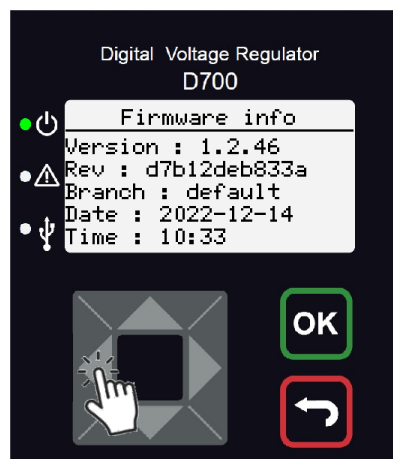


Figure 2. Firmware version example

- On the D700 EasyReg Advanced software application, click Info button to display EasyReg Advanced version (module version) and D700 firmware (Application release) if the D700 is connected to the computer:

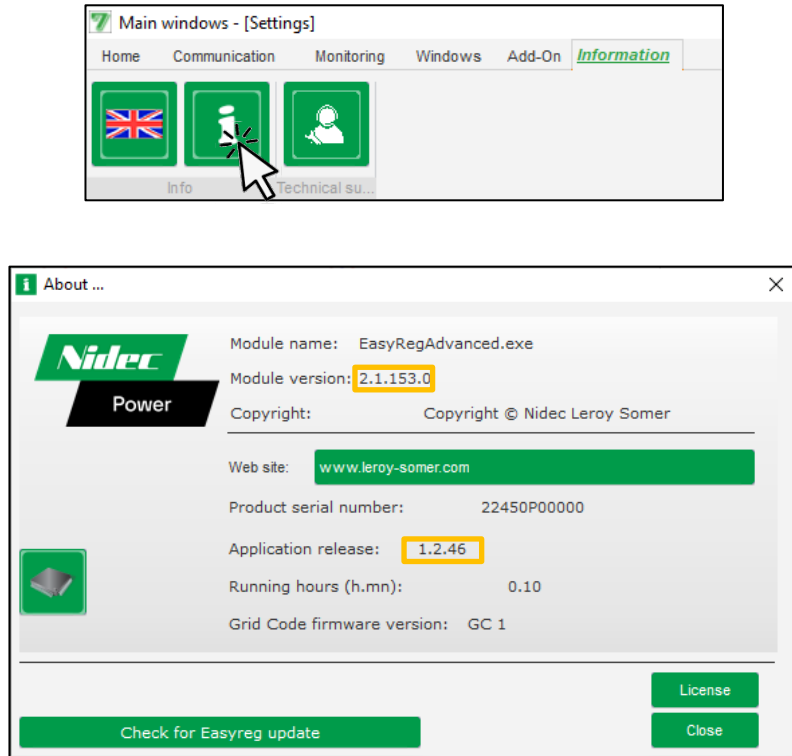
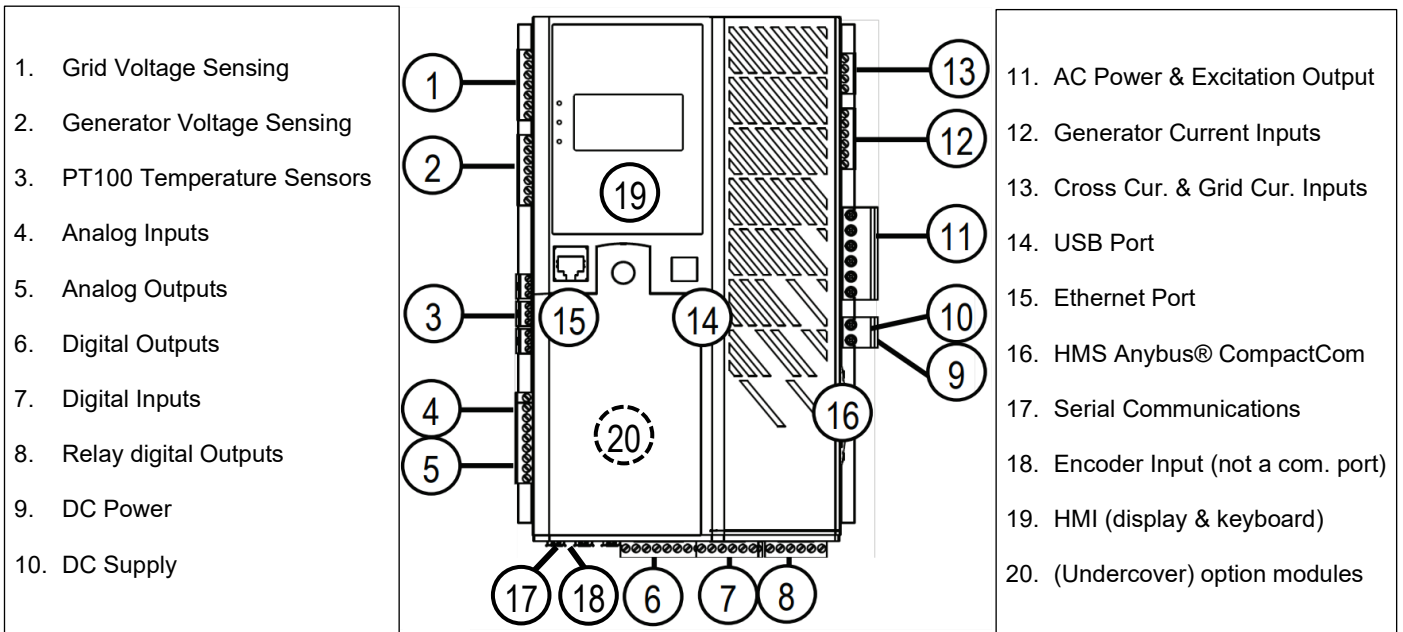


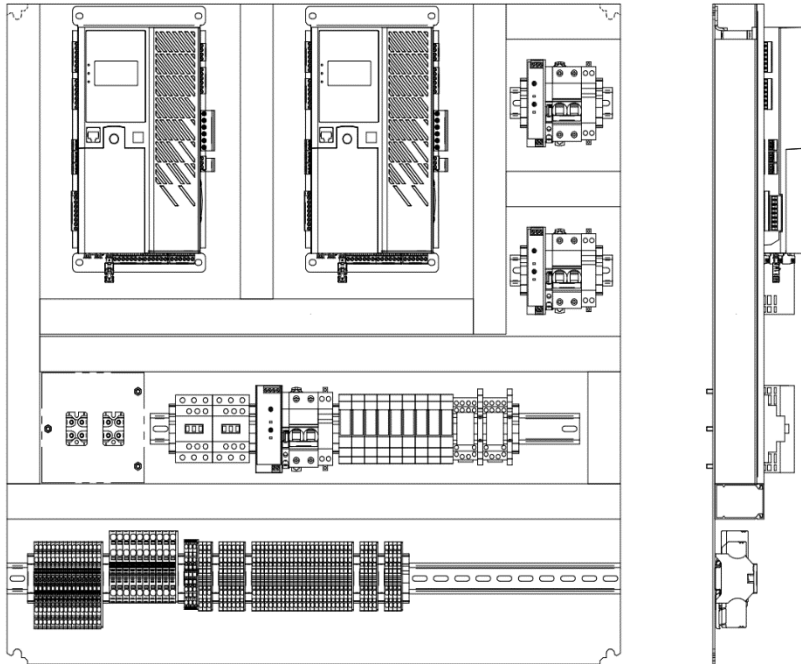
Figure 3. EasyReg info screen example

6 D700 HARDWARE DETAILS

6.1 Connector and interface identifications



Dual plate option



Note: The dual plate option consists of an assembly of 2 D700 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 D700 USB is configured as a HID device with VID 0x1D65 and PID 0x0006 with full speed interface. USB activity is displayed on front LEDs with the USB symbol. It should light on blue when connected, correctly enumerated and active with the application software. If the Ethernet is also active with a communication activity, this LED could light purple/white. This USB port is not designed to perform a permanent communication with a computer. It should remain disconnected during normal operation.
 - **Mass storage:**
The D700 embeds a datalogging system based on a microSD slot for data storage. Thanks to a dedicated button in EasyReg Advanced application software, the D700 could be identified as a mass storage device (with VID 0x1D65 and PID 0x0009) to give access to the microSD card internal content. This will automatically open on the computer Windows® operating system the explorer mass storage device disk with the file contents. Datalogging files are based on CSV file format. This special mode should be used only when the D700 doesn't operate because the datalogging process is stopped. To switch back in configuration mode, the USB should be disconnected and reconnected again.

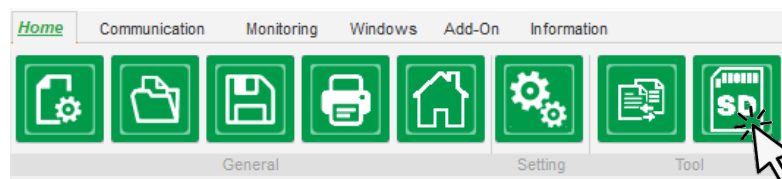


Figure 4. MicroSD card management



- **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 of these protection could be combined.

- **Ethernet port**

This interface is a RJ45 Ethernet 10/100BaseT connector. The Ethernet could be used with the D700 for many usages like monitoring data flow with UDP protocol or process control with Modbus TCP protocol, embedded web server, E-mail client management through SMTP. An automatic clock synchronizer option is also available by enabling the SNTP configuration. The DHCP automatic configuration is available on the Ethernet configuration page described below.

- **DHCP client:**

The D700 is capable to exchange with DHCP server to automatically get a complete network configuration (IP, netmask, gateway). Even though it proposes an easy way to configure the product on a network, if the Ethernet communication is defined in a complete process system, it is highly recommended to define a fixed IP address for the D700. This function could be enabled or disabled on the D700 configuration page.

- **UDP proprietary protocol server:**

This is the exchange protocol between one (or more) D700 and the EasyReg Application using Ethernet communication instead of USB. This protocol is not accessible for the customer and not documented for a particular system usage. Main advantage of UDP proprietary protocol server is the fast-broadcasting capability which propose monitoring up to 20 parameters with a very fast sampling proposing useful features for commissioning. This mode should not be used for process control, the Modbus TCP must be the preferred Ethernet remote solution.

- **Modbus TCP server:**

The Modbus TCP server is proposed in D700 for process control like changing the regulation mode, setpoints, ... and to monitor specific parameter that could be used for an external process control. This protocol should be used to ensure a correct data reading / writing in the complete process.

- **Embedded Web Server:**

The web server gives a monitoring interface directly accessible with an internet browser by connecting to the D700 IP address. This function could be enabled or disabled on the D700 configuration page.

- **SMTP client:**

The D700 has possibility to send 2 customized messages to any e-mail box triggered by an internal digital flag. This digital flag could be assigned to an internal logic gate or an internal parameter like an alarm or a regulation mode. A SMTP server should be configured to use this feature.

- **SNTP client:**

The D700 could enable the SNTP function to synchronize its internal RTC (Real Time Clock) with a SNTP server.



- **Cybersecurity considerations**

The Ethernet port is considered as the most critical port regarding the Cybersecurity. All other options should be considered before using it in the system design.

It would be preferable to use hardwire digital and/or analog I/O than Ethernet port despite the complexity of use.

If Ethernet is used in the system design, it should be connected on a trusted local process network, without any bridges to other networks like business networks or Internet. All equipment on this network should be known and no free ports should be accessible without any physical barriers.

The Ethernet writing should be configured for write locking with a pin code preferring the read only mode. Write orders for any adjustments or mode changing should be hardwire. Configuration of this write locking function is described in § 7.4.3.

The system design with Ethernet link must use Modbus TCP for data processing and not any other protocol available. It is the system designer responsibility to allow only the specified components to access the Modbus TCP server.

Never use the web server on critical applications.

Never use or configure the SMTP messages for your maintenance organization. Never trust any message that appears received from the D700 AVR.

Never save the D700 configuration file that could contain Ethernet configuration details in a public server or a not secured private server or any not-trusted storage space on the clouds.

Never attach to an E-mail a D700 configuration file for a not-trusted recipient which could contain an Ethernet configuration details.

Regarding the SNTP, a special care should be taken if an external untrusted SNTP server is configured for clock synchronization. If not useful in the application, the SNTP should be disabled.

On any cases, all requested protections should be configured to ensure an Ethernet secured connection.

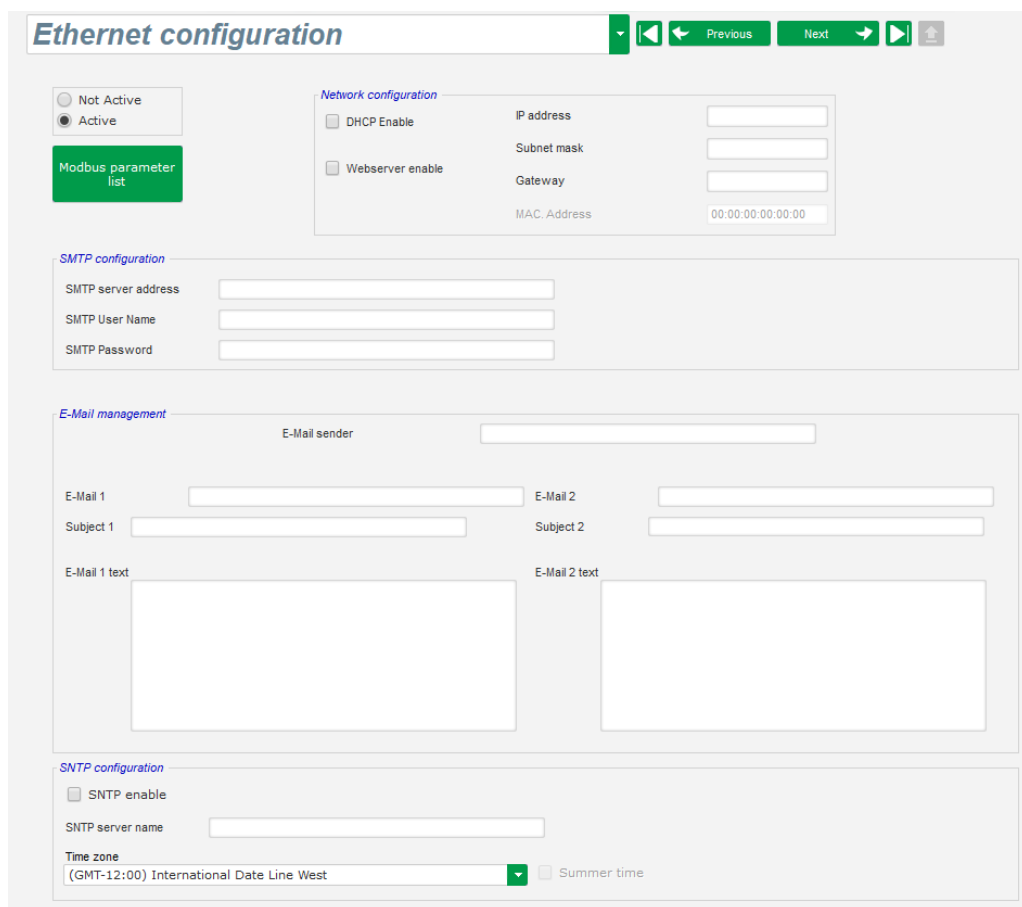


Figure 5. Ethernet configuration page

- **HMS Anybus® CompactCom**
 The D700 embeds a CompactCom slot dedicated to field bus communication modules made by HMS NETWORKS. It exists many references available adapted to the different fields bus that could be used in an industrial system.
 The CompactCom module could be considered as a local bridge between the D700 and the field bus. The internal software of each HMS NETWORKS module model is a HMS NETWORKS development and protected by them.
- **Cybersecurity considerations**
The Cybersecurity assessment for this third-party equipment is directly managed by HMS NETWORKS and described on their website (<https://www.hms-networks.com/cyber-security>).
On the D700 product, the cybersecurity protection consists of the write lock system with a pincode, similar as Ethernet or USB and described in § 7.4.3.



○ **Serial communications ports**

The D700 is equipped with 3 serial RS485 communication ports. These 3 communication ports are replicated on the 3 Mini I/O ports on the D700 bottom side. These serial communications are dedicated for specific functions with optional Nidec equipment like special HMI, I/O extension module, power static converter, ... The option doesn't care the communication port position between the 3 connectors available. These communication ports are not usable for the installer/customer and the communication protocol is not documented. These communication ports don't offer the possibility to access to the D700 internal configuration.



○ **Cybersecurity considerations**

Considering these serial communication ports are NIDEC POWER Leroy-Somer proprietary with very restrictive control features according to the option used in the system, the Cybersecurity risk is very limited. However, we recommend to ensure that these communication ports are free of any connected cable if no D700 options are used in the system.
If cables are connected on these ports, these should be identified on both ends and inspected on the full length to ensure that no other unknown derivation are put in place.

7 SOFTWARE PACKAGE

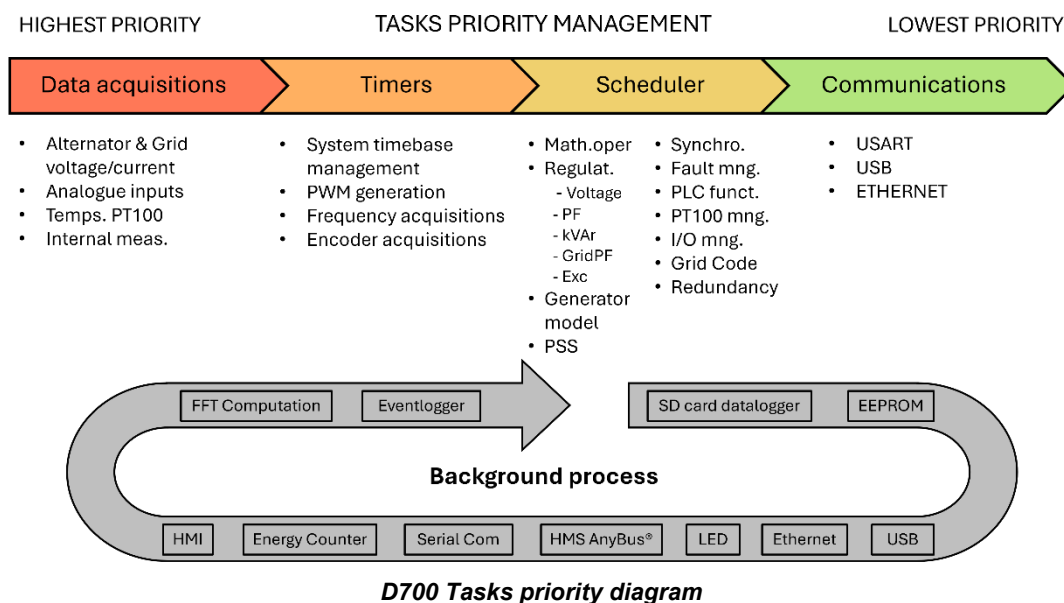
7.1 D700 core

The D700 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 25A continuous and 50A for field forcing. For more excitation currents, requested in bigger alternators or to control an external static excitation power bridge, the D700 generate a control signal to the external power bridge with a dedicated serial port.

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, Ethernet, field bus...) is executed in the lowest priority tasks of the program. This strategy ensures to the D700 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:



7.2 D700 digital AVR features package

The D700 firmware is managing these functions:

- **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
- **HMI:**
 LCD control
 Keyboard control
- **Generator configuration:**
 Generator data (dataplate)
 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
- **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
 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
- **Engine helps:**
 Equalization with grid
 Synchronization
- **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
- **Datalogger:**
 Monitored parameters list
 Trigger management
 Record file definition
- **Ethernet:**
 Protocol activations and configuration
 Mailing management
- **RTC:**
- **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
- **HMS Anybus:**
 Field bus cartridge configuration
- **Monitoring:**
 FFT analysis
 Complete electrical parameter measurements

Note: this is not an exhaustive list



D700

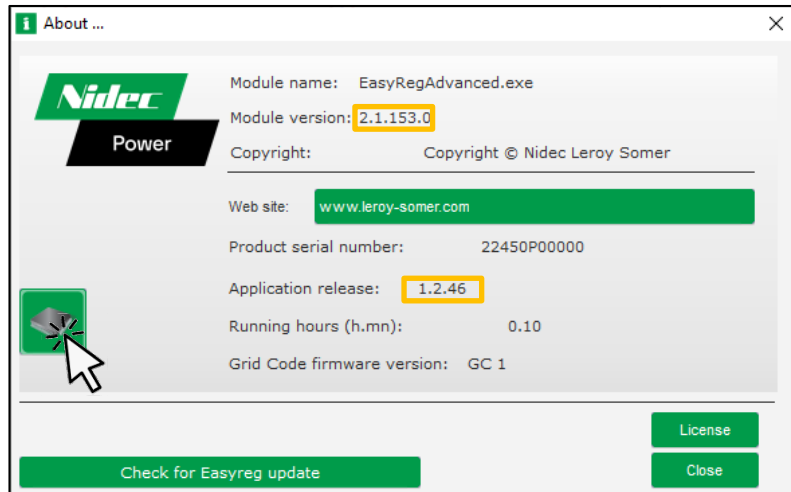
D700 CYBERSECURITY INFORMATION

SOFTWARE PACKAGE

7.3 D700 firmware upgrade package

To upgrade the D700 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.



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-software 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 voluntarily 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 D700 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.

EasyReg Advanced

Download

Version 2.1.77
2024.01 - 218.8 Mb

Hash (SHA-256):
bda055ca59bce1996307cc2d18a6f80d45b9dc6b692a9cc773362e3b8384a8bb

Changelog

Older versions

Download section for EasyReg Advanced (example)

- Configuration file (.700 file)
The EasyReg Advanced software on the D700 Sub-software create/open/write the configuration file with “.700” extension. This “.700” 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 D700 electric cabinet avoiding any access to not trusted people. With this minimum level of protection, we ensure that only skilled people can access to the D700.

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

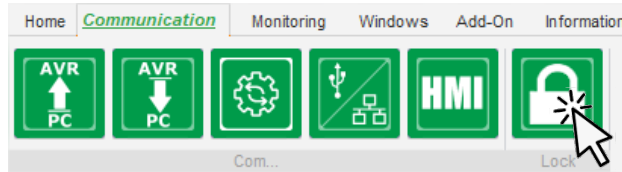
Special applications could require specific configurable modules:

- **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

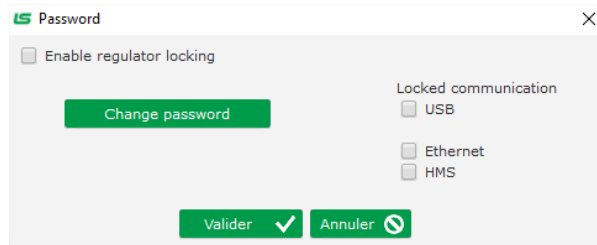
7.4.4 D700 communications write locking configuration

To guaranty no further configuration change after the system commissioning and to enhance cyberattack resilience, the D700 could be write locked. Once configured, the D700 will internally reject any write attempt coming from the selected communication interfaces.

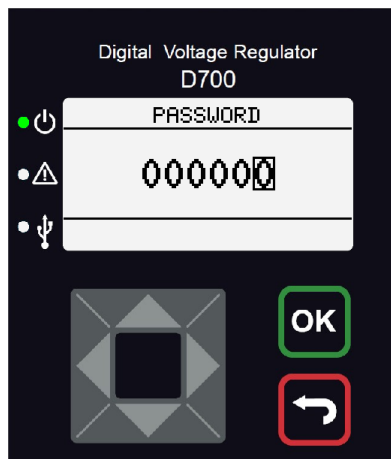
The configuration page is accessible by clicking on this EasyReg Advanced button when a D700 is connected on the computer.



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.



Note: The HMI write locking function is different and is not managed by EasyReg Advanced. This is locally controlled on the HMI with keyboard and the definition of the password is done directly on the HMI, Menu 13, parameter 001. This password could be different than the communication write locking function password.



7.5 MicroSD card content

The D700 embeds a datalogger with a microSD card port which can record many parameters in continuous or triggered by an event. It's also an event logger for the system behavior and a configuration logger to record any configuration changes during the life cycle of the product.

The microSD must be formatted in FAT32 and compatible capacity is up to 32GB.

Those parameters are recorded in .CSV format for further customer use with predefined file size according to the configuration done with EasyReg Advanced software.

8 MAINTENANCE PRACTICES, SECURITY ENHANCEMENTS AND RECOVERY PLAN

NIDEC POWER LEROY-SOMER recommend the maintenance organization to save and secure each D700 configuration file (1 per D700 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 and HMI after a commissioning.

In case of maintenance purposes, the skilled authorized maintenance people could replace the current D700 by a new D700 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 D700.

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 D700, 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
- “.D700” configuration files if available.
“.700” configuration files could be generated by connecting the USB on D700 and import parameters from D700 to computer with EasyReg Advanced. This operation is still possible with a D700 write locked.
- D700 serial numbers
- D700 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