Cyber security Information and Guidance – Altivar Drives

1/20/2016

Overview

Schneider Electric has become aware of a presentation and news article on how modification of Altivar drive parameters can be used to modify the power drive system behavior.
The research was presented by Reid Wightman, of Digital Bond Labs at the S4 conference event and reported in Wired magazine.

Conscious about user Cyber Security concern, Schneider Electric considers this case as high priority and is producing this document to advise drive users on mitigations they can take.

Presentation Overview

The use case identified by the researcher on the ATV12 product demonstrates the ability to modify drive parameters so that the drive is no longer configured appropriately for the motor being controlled, potentially affecting system operation.
In this use case, parameters are modified using the Modbus protocol, a serial protocol operating within a limited distance, and with a dedicated master/slave relationship.

Product(s) Affected

All Altivar Variable Speed Drive products

Mitigation

Why is remote access available/necessary?

During the commissioning of a drive, many users prefer to be next to the driven mechanics rather than next to the Altivar device itself, thereby requiring remote access to the parameters.
Depending on application needs, a controller is able to change the drive configuration to facilitate things such as easy replacement, or configuration of switches for different motors.

General practices

Unauthorized persons may gain access to the drive as well as to other devices on the network/fieldbus of the machine and connected networks via insufficiently secure access to software and networks.
To avoid unauthorized access to the drive, users are advised to:

• Perform a hazard and risk analysis that considers all hazards resulting from access to (and operation on) the network/fieldbus, and develop a cyber security plan accordingly.

• Verify that the hardware and software infrastructure that the drive is integrated into (along with all organizational measures and rules covering access to the infrastructure) consider the results of the hazard and risk analysis, and are implemented according to best practices and standards such as ISA/IEC 62443.

• Verify the effectiveness of the IT security and cyber security systems using appropriate, proven methods

Mitigations

There are 2 different configurations to consider for mitigation:

- Drives that can only be connected with a local Modbus Serial Line
- Drives that can be connected to any local fieldbus

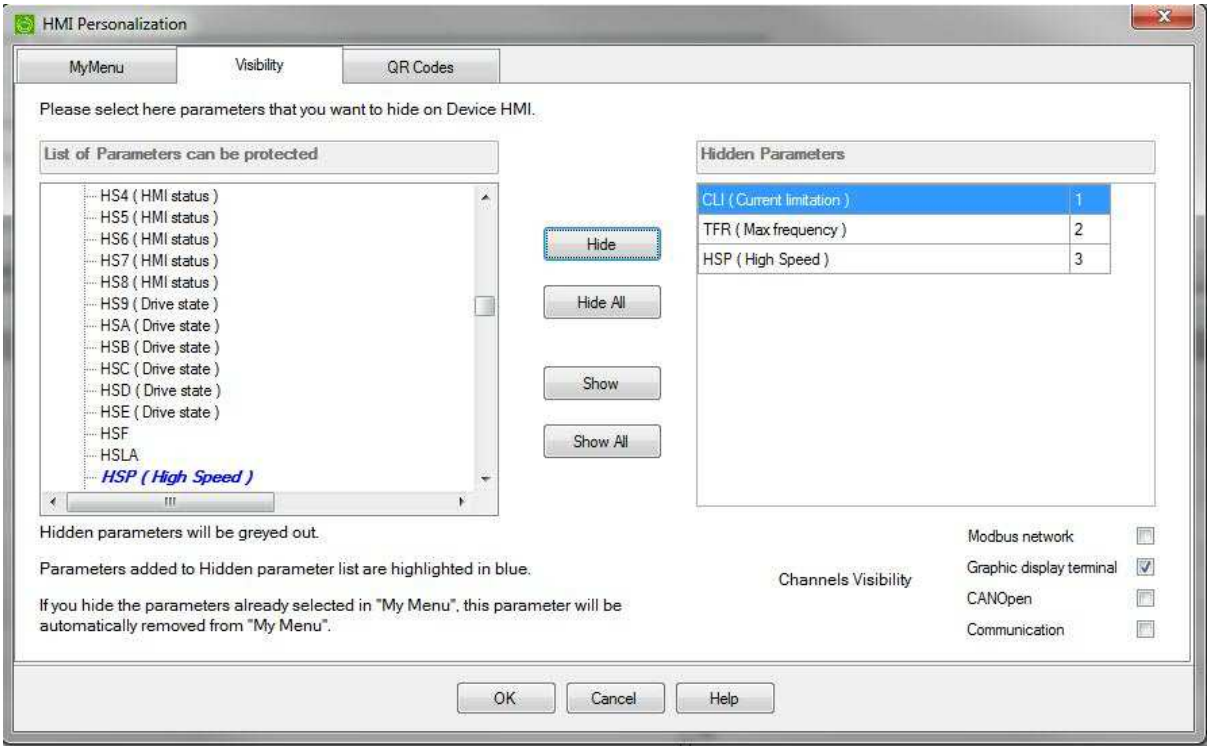
Drives that can only be connected with a local Modbus Serial Line

For this drive configuration, the general practices outlined above are advised.

Drives that can be connected to any local fieldbus

In addition to the general practices outlined above, this configuration offers an **"HMI Personalization"** feature to restrict access to drive parameters.
This feature is configured with SoMove software (or Drives DTMs), and differs slightly depending on the product.

- **<u>for Altivar Process products (ATV6xx / ATV9xx), access the feature through the "Visibility" tab in the DTM</u>**



Follow this procedure in the drives DTM:

- Select the parameters to be protected from the list of all parameters on the left,
- Use the "Hide" button to move the parameters into the hidden parameters list.
- Select the channel through which the parameters will be visible.
  All parameters added in the "Hidden Parameters" list will have the same visibility defined with the 4 possibilities:
  - Modbus network (embedded Modbus SL and embedded ModbusTCP)
  - Graphic display (local HMI)
  - CANopen
  - Communication (all other field buses over optional communication module).

In this example, the access to the TFR, HSP, CLI parameters is not possible for

- Modbus Network (embedded Modbus SL and ModbusTCP)
- CANopen
- Optional communication module.

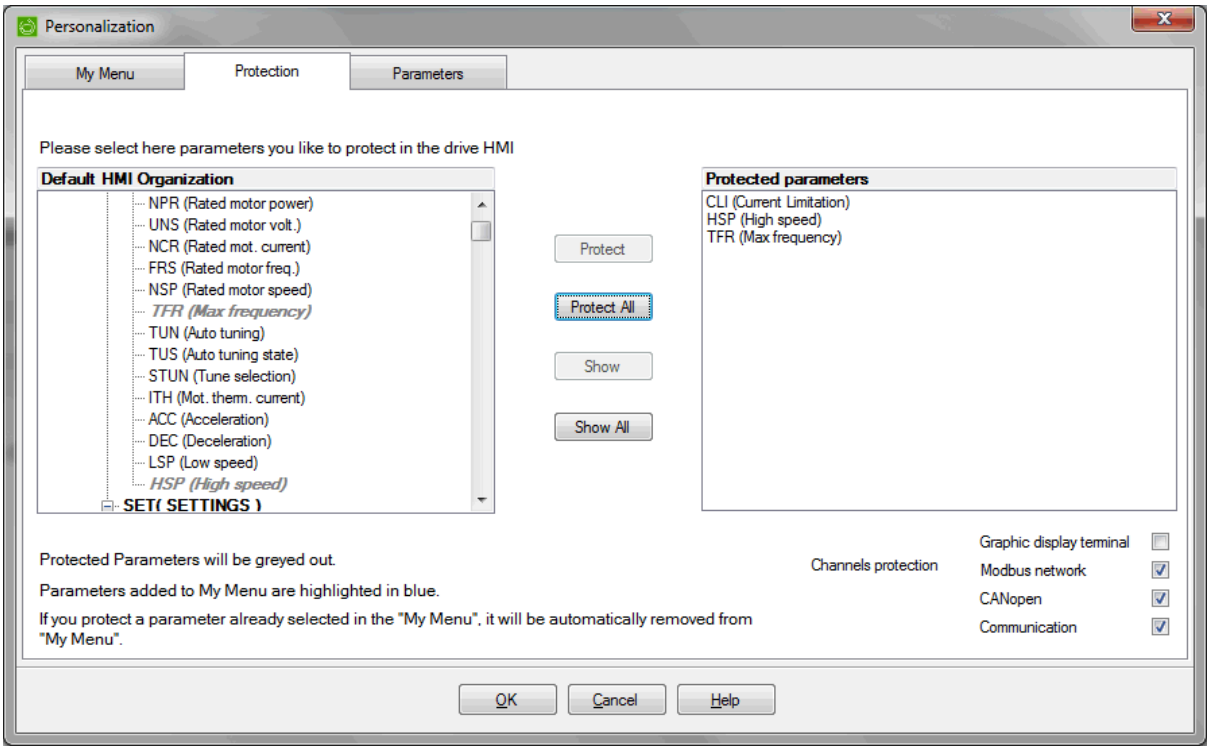
NOTE:
EtherNet/IP protocol is available in the ATV9xx embedded Ethernet connection. For this protocol the function will be available in version 1.3.

In the meantime, to protect the access to parameters over this channel the ConneXium TOFINO firewall can be used.

The ConneXium Tofino firewall provides deep packet inspection capabilities which allow restriction of access to specific registers. The addresses of the drive parameters can be found in the ATV900 Communication parameters (NHA80944)
on www.schneider-electric.com/ww/en/download/document/NHA80944

To protect drive parameters using a ConneXium Tofino firewall refer to the ConneXium manual and apply a rule set which restricts access to the appropriate registers for the targeted drive.

- **<u>for the other Altivar products, access the feature through the “Protection” tab in the DTM</u>**:



Follow this procedure in the drives DTM:

- Select the parameters to be protected from the list of all parameters on the left.
- Use the “Protect” button to move the parameters into the protected parameters list.
- Select the channel through which the parameters will be protected.
  All parameters added in the “protected Parameters” list will have the same visibility defined with the 4 possibilities:
  - Modbus network (embedded Modbus SL)
  - Graphic display (local HMI)
  - CANopen
  - Communication (all other field buses over optional communication module).

In this example, the access to the TFR, HSP, CLI parameters is not possible for:

- Modbus Network
- CANopen
- Optional communication module.

For More Information

Schneider Electric products are designed to operate in an environment with layered security defenses. For assistance with the security features available in a specific product, contact your local Schneider Electric representative.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cyber security web page at

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com