Schaeffler SmartCheck / ProLink IT Security Information

Valid for firmware version 1.26.0 and newer (last update August 2024)

SCHAEFFLER

Table of content

1 Introduction

When using the devices Schaeffler SmartCheck or ProLink in a network, there are several questions regarding IT security which need to be addressed. On the one hand, SmartCheck and ProLink need certain network properties to be able to work properly in the network. On the other hand can each network device pose a threat to the IT-security of the network. To assess this, the IT administrator needs information about the network functions of the device. This document tries to provide as much information as possible for optimal operation in a network.

2 Needed network services

2.1 HTTP / HTTPS

All user interaction with SmartCheck or ProLink device uses http (TCP port 80) or https (port 443). In case of https, the openSSL library is used. The webserver has been developed by Schaeffler and is not based on an external library. The communication layer uses gSOAP webservices to send configurations to the device and to read configurations and measurement data from the device.

The https-connection uses a self-signed certificate issued by Schaeffler. Since such a certificate is always bound to a device name, IP address or domain name, it is not possible to provide a valid certificate from the factory. It is however possible to replace this by a customer issued x509-certificate with a private key. This must be done via the device’s maintenance system.

When connecting to the assigned IP address using a web browser, the local webserver will deliver the Schaeffler SmartWeb as a complete package including html, JavaScript and images to the browser. Schaeffler SmartWeb runs as an application in the browser. It communicates with the SmartCheck or ProLink device using gSOAP.

2.2 UDP Broadcast

The Schaeffler SmartUtilty uses a UDP broadcast to find all SmartCheck and ProLink devices in the current network segment. The broadcast is sent by the Schaeffler SmartUtility to devices on UDP port 18001 (open port on the device), the SmartCheck or ProLink will reply on UDP port 19000 (open port on PC). The user can configure the port on the PC to any port, in the settings of the Schaeffler SmartUtility. If traffic on either port is blocked e.g. by a firewall, then it is not possible to search for SmartCheck or ProLink devices by the Schaeffler SmartUtilty. It is however still possible to use the SmartUtility by entering the devices IP address or network name by hand, without opening a UDP port on the PC.

2.3 NTP

If configured, Schaefffler SmartCheck and ProLink can synchronise their real time clock via a TCP NTP connection to the defined NTP server.

2.4 DHCP

By default, the Schaefffler SmartCheck and ProLink will try to obtain its network settings (IP address, gateway and DNS) using a DHCP request. In the network settings of the device, the user can select whether the device sends its name to the DHCP server or of the name of the device is received from the DHCP server.

3 Outgoing network traffic

3.1 SLMP

The Schaefffler SmartCheck or ProLink can connect to a Mitsubishi-PLC to read and write values. It then uses the SLMP protocol via TCP. The user defines the communication settings for the PLC in the SmartCheck's or ProLink's configuration. This configuration then defines the IP address and port for this network connection.

3.2 Email

Both Schaeffler SmartCheck and Prolink can send emails. To do this, the device will communicate with an SMTP server, on port 25 (when not encrypted), port 587 (StartTLS encryption) or port 465 (SSL encryption), with optional user authentication. It is also possible to route this connection via a proxy server, also with optional user authentication at the proxy server via basic authentication or NTLM authentication.

3.3 OPTIME Cloud

When devices are configured to communicate with the OPTIME cloud, they use an encrypted MQTT-connection to Microsoft's IoT Hub on port 8883. For the authentication the device has an individual certificate, that Schaeffler provides on customer request and is installed on the device using the Schaeffler Cloud onboarding function in the device's SmartWeb. It is also possible to route this connection via a proxy server, also with optional user authentication at the proxy server via basic authentication or NTLM authentication.

3.4 Field busses PROFINET and EtherNet/IP

Optionally the user can plug a fieldbus module into the ProLink, to be able to use either a PROFINET connection or an EtherNet/IP connection. This network is completely separated from both the external Ethernet connection (to the company network) as well as to the internal Ethernet connection (between the CPU and the measurement modules).

4 Provided network services

4.1 OPC/UA

OPC/UA can be used on both Schaeffler SmartCheck and ProLink to provide values to a client or to receive values from a client. For this a TCP port on the device if opened, which can be configured by the user. Optionally, a user authentication can be enabled.

5 Other security relevant information

5.1 Operating system

The Schaeffler SmartCheck and ProLink use an embedded Linux operating system specifically configured for the device. Except for the described services, no other network services (e.g. SMB, NFS, …) are running on the device.

5.2 Firmware updates

The Schaeffler SmartCheck and ProLink can be updated by the user. These firmware updates can contain new features, bug fixes or fixed security issues. The device only accepts firmware packages which match the device (i.e. SmartCheck or ProLink) and which are signed by Schaeffler, to ensure, that only valid firmware files are used to perform an update. The SmartUtilty PC-software checks for new firmware versions on start-up, alerting the user when new versions become available. The device itself does not check for updates.

5.3 Password services and user management

All webservices on the Schaeffler SmartCheck and ProLink are secured by username and password. When the user management is disabled, which is the default state, default values for username and password are used. On activation of the user management, the user will define usernames and passwords to limit the access to the device. Each defined user is a member of a user group, for which the access rights for this device are defined. Users are defined per device, the usage of external services like LDAP are not possible.

5.4 Usage of certificates

The firmware of both Schaeffler SmartCheck and ProLink use certificates for encryption or authentication for some of the communication protocols:

UDP	Not encrypted, no certificate is used
SLMP	Not encrypted, no certificate is used
HTTPS (webserver/webservices)	Server certificate on the device, which can be changed in by the user in the maintenance system
OPCUA	Server certificate on the device, which can be changed in by the user in the maintenance system (same as HTTPS certificate)
OPTIME cloud	Uses client certificate of the cloud server for authentication

5.5 Data export container (firmware version >= 1.14)

When downloading measurement data from Schaeffler SmartWeb, the data container is encrypted and can only be decrypted using the Schaeffler SmartUtilty software. By default, every user of the software can decrypt and open the data via the data import feature. On the Schaeffler SmartCheck and ProLink devices, the user can additionally set a device specific password for the data container, which is needed when importing the container into Schaeffler SmartUtility.

5.6 Monitoring of security updates

For all used open-source components including the Linux operating system and libraries, there is a permanent monitoring in place. If security issues are reported, the development team decides if action is needed, depending for example on if the security problem can be exploited for the way the component is used on the system. They also decide when the fix needs to be implemented: depending on the severity of the issue and the impact on the security of the system, this fix can be implemented in the next planned firmware version or as soon as possible for severe security issues. Via the menu “Show open-source licenses” a list of all used open-source components including their version is shown.

5.7 Report a new security issue

When a security issue is found in our software, this can and should be reported to the Schaeffler cyber-security team, by sending an email to psirt@schaeffler.com.

5.8 Development process

During the development of the firmware and software, several mechanisms are in place to ensure the quality. A continuous integration server automates all steps of the build process, like compilation, static code analysis, automated tests, creation of update packages including signing them, etc. Code reviews and pair programming help to prevent logic errors during software development. Test automation for unit, integration and system tests as well as manual tests ensure the development quality. In the end, also the deployment process is automated.