Fronius
SHIFTING THE LIMITS

Wels, September 2017

FRONIUS CYBER SECURITY STATEMENT

For the security of its customers, Fronius works intensively on cyber security. This document sets out the principles of security in data communication.

A potential risk only exists when inverters are connected to the internet. Devices that are not connected to the internet are not vulnerable.

The Fronius Datamanager – the communication hub of Fronius inverters – is designed for use in a LAN, behind a firewall. This means the infrastructure within which the Datamanager is operated, is crucial for the security of the system. Please therefore ensure that your firewall is enabled and your router is configured in such a way that all ports that are not required are blocked and no ports are forwarded.

The inverter control system is deactivated as standard at Fronius. The control system can be established via Modbus RTU or Modbus TCP. In a Modbus RTU connection the bus participants are directly connected and therefore are not subject to external influence. If the inverter is controlled via Modbus TCP, we recommend providing additional protection in the network in which the control system and the Datamanager are installed.

Fronius takes the issue of cyber security very seriously and therefore makes updates available for system components at regular intervals. Security experts at Fronius also focus on improving our security concepts to meet increasing requirements. All these measures help to make your system even more secure.