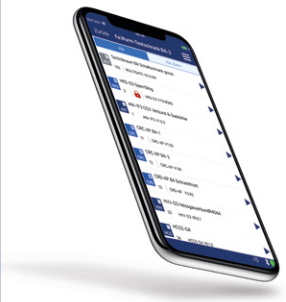
INCREASED PROTECTION FOR MANUAL ACCESS



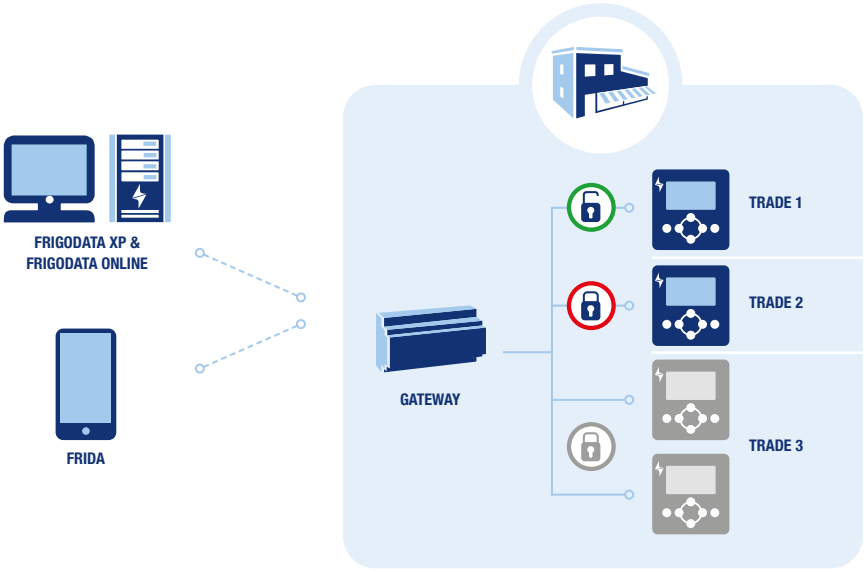
WURM

NEW SECURITY FUNCTION FOR THE NEW GENERATION OF DEVICES

Security has always been a top priority at Wurm. For this reason, we have established an effective security structure over the years that is continuously being adapted to technological progress and the constantly changing risk factors.

We have now expanded our security mechanisms once again. Specifically, we have developed additional protection from improper or unauthorised manual access directly at the device in the respective plant. This additional protection measure will be implemented in the next generation and will also be available for a selected number of devices currently in use in the form of a software update.

We have outlined the core products of this expanded security for you in this flyer. Because the current high security standard, in which users must authorise themselves for remote data transfer with their Gateway ID and a password for reading or writing for the respective system, will be expanded by a new step by means of this new function.



MANUAL ENTRY ONLY WITH TEMPORARY RELEASE

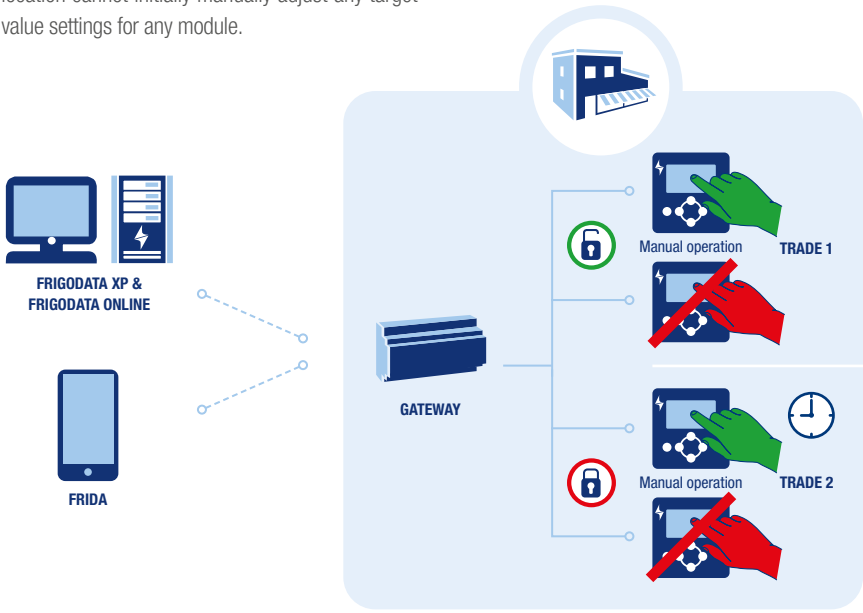
DEVICE BLOCKING PREVENTS UNAUTHORISED MANUAL ENTRY

To put a plant into operation that contains Wurm devices, the latter must first be released for manual setting by the authorised service technician on location. In order to prevent any incorrect entries or unauthorised interventions regarding the target value settings from the outset after the plant has been put into operation we have now developed an additional security barrier.

In this step the administrator at the service company headquarters blocks individual devices or even the entire plant after it has been put into operation. This means that even authorised technicians on location cannot initially manually adjust any target value settings for any module.

Instead, the specific module must be released again by the administrator beforehand. After the technician's individual access rights have been clearly identified, the administrator can release the manual setting for the technician for a predetermined period of time. Only then can the service technician undertake the target value settings within this time frame. After the time has elapsed, the device will be automatically blocked for manual adjustment again.

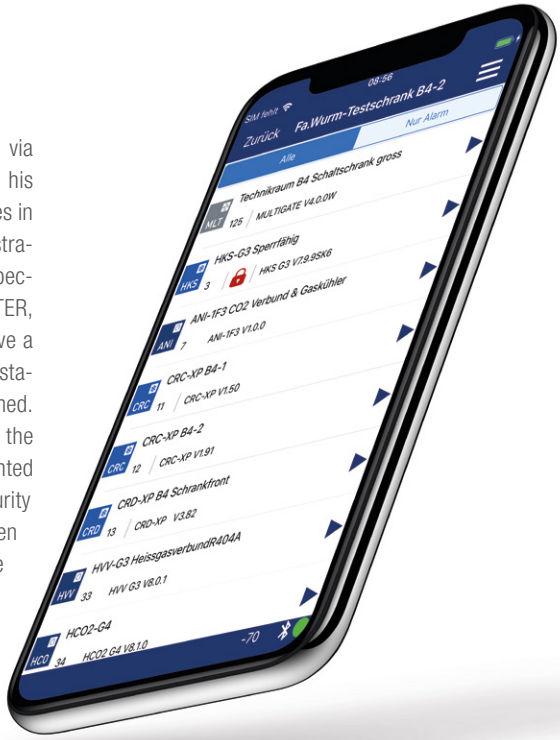
Protection from unauthorised access will therefore be further enhanced.



FRIDA APP PROVIDES CLARITY

EVERY DEVICE BLOCK APPEARS ON THE DISPLAY

The service technician on location can, via Frigodata XP or the Frida app installed on his mobile device, recognise directly what devices in the plant have been blocked by the administrator. As soon as he has downloaded the respective project from the Wurm DATA CENTER, onto the Frida App, for instance, he will have a complete overview of all devices and their statuses after the connection has been established. The precondition for this is, of course, that the employee is recorded as having been granted access to the project at the Wurm Security Centre. After the device in question has been temporarily released by the administrator, the service technician can perform the target value settings as required as long as the time window is open.




i
CIRCULATION
PUMP
TRIPPED

ADDITIONAL PROTECTION FOR MANUAL ACCESS – BENEFITS AT A GLANCE

- Increased protection of your plant from unauthorised and improper target value settings by means of device locking by the service company's administrator
- After the employee on location has been clearly identified in terms of rights at the Wurm Security centre, temporary release for manual settings on the specific device is possible.
- The individual short-term granting of the employee's rights and the temporary lifting of the block for the specific device means that it is possible to react very quickly to a change of personnel (e.g., an employee leaving).
- This means that the plant configuration is even better protected.
- Release by the administrator can be granted to the entire plant or individual devices.
- This additional security measure prevents any loopholes – even if a device has been separated from the bus system, no individual manual intervention would be possible because the block applies to the device itself.
- The new mechanism will become a component of all the main modules of the next generation of devices. Existing devices can receive the new function via software updates.

WURM

Wurm GmbH & Co. KG Elektronische Systeme
Morsbachtalstraße 30
D-42857 Remscheid

Tel: +49 (0) 2191 - 8847 300
Fax: +49 (0) 2191 - 8847 9300
Email: info@wurm.de

030A-EN