

THE STRONGEST LINK.

STAHL

UPGRADE INSTEAD OF REPLACE

A Cost-Effective Path to a Cybersecure HMI



UPGRADE YOUR HMI TO THE LATEST CYBERSECURE TECHNOLOGY

Cybersecurity is more important than ever and has become a top priority for industrial production facilities. New European legislation and international regulations are introducing increasingly stringent cybersecurity requirements for the process industry.

HMI operator workstations must also be assessed and evaluated accordingly. We support you throughout this process, from analyzing existing systems to developing future-proof cybersecurity concepts for your HMI infrastructure.

WHY? NEW CYBERSECURITY REQUIREMENTS FOR OPERATORS

NIS2 (EU 2024)
Network and Information Systems Directive 2

The NIS2 Directive requires organizations in critical sectors, including the pharmaceutical and chemical industries, energy and water utilities, healthcare, manufacturing, and digital infrastructure, to strengthen their cybersecurity, systematically manage cyber risks, and report significant cybersecurity incidents.

What Do Operators Need to Do?

- Assess cybersecurity risks
- Identify outdated hardware and software
- Ensure regular security updates and effective patch management
- Secure or replace unsupported systems
- Incorporate cybersecurity considerations into investment and migration decisions

R. STAHL HMI CYBERSECURITY UPGRADE

Older HMI systems deserve particular attention. How old is the operating system? Are the security software and patches up to date? Does the existing hardware still provide sufficient resources to reliably run modern software applications?

We provide comprehensive support in answering these questions.

As an HMI specialist for hazardous areas, we offer a detailed assessment of your installed HMI landscape based on device serial numbers.

Based on this analysis, we develop customized upgrade scenarios ranging from targeted modernization measures to migration to the latest ORCA HMI platform running Windows 11 IoT Enterprise LTSC.

YOUR PATH TO A CYBERSECURE ORCA HMI



ORCA HMIs running Windows 11 IoT Enterprise LTSC currently represent one of the most advanced and future-ready standards for industrial HMI applications in hazardous areas.

Your Benefits:

- Hardware and software assessment and analysis
- Development of an individual cybersecurity concept for each HMI
- Resource-efficient and cost-effective reuse of existing components such as cabling, keyboards, RFID readers, and barcode scanners
- Flexible configuration of multiple Ethernet interfaces within the ORCA HMI
- Compatibility of the latest REMOTE HMI V7 generation with existing system versions

BOOK YOUR HMI CYBERSECURITY ASSESSMENT TODAY



Scope of Services:

- One-day on-site plant assessment
- Analysis of the installed HMI infrastructure
- Development of a device-specific cybersecurity concept
- Creation of concrete upgrade and migration strategies

Kontaktieren Sie uns:
sales.dehm@r-stahl.com

ID 354267 | 2026-11 / ENs | Printed in Germany

R. STAHL
Am Bahnhof 30
74638 Waldenburg, Germany
T +49 7942 943-0
F +49 7942 943-4333
r-stahl.com

Follow us:
R. STAHL Group
R. STAHL Group
rstahl_group

EXpert Mail registration: