REMOTE ACCESS & MONITORING

KEEPING YOUR NETWORKS SECURE ANYTIME & ANYWHERE

Increasing digitalisation can lead to higher vulnerability of cyber attacks. This especially applies to the operation of industrial plants. However, in many cases components and methods are used that have not been developed in consideration of IT security aspects but are nevertheless used for long running times. In this regard, we develop customised concepts that provide the highest degree of IT safety and security, and thereby do not endanger stable plant operations.

The 'Defense-in-Depth' principle

Through consistent implementation of the 'Defense-in-Depth' principle, both accesses and also networks and systems can *(even retroactively)* be secured with suitable measures.

These measures are based on our long-term experience as system integrator and have been developed in consideration of applicable standards *(IEC 62443, ISO 27001 and BSI Basic Protection)* and guidelines of the control system manufacturers.

The introduction of malware or viruses through infected systems is securely protected. The firewalls work on the principle of white listing, which by definition prohibits everything that is not explicitly permitted from being accessed. In conjunction with a customised user administration, individual accounts can be assigned and further defined to what systems and in which way a user is allowed to connect to the systems.

Bilfinger Remote Monitor

With the Bilfinger Remote Monitor tool, you have a complete overview at a glance. The tool is specially designed and can be adapted to the customer's setup and the requirements of their automation technology. Its integrated monitoring system allows customers to oversee all of their available components within their network *(i.e. servers, switches or controls)*.

If the defined thresholds of the monitored components are exceeded, an alarm or warning is raised. These are depicted on a structural overview next to the components that are being monitored. The user can also drill-down further via the structural overview to get details of the affected component.

Benefits

- Secure remote access to the plant from remote offices or home offices.
- Ideal for critical infrastructures *(KRITIS)* through high degree of isolation.
- Remote support and maintenance.
- Unauthorised access is prevented through two-factor authentication.
- Simple user management.
- Login attempts can be recorded.
- Can be extended by an Intrusion Detection System *(IDS)*.

BILFINGER