IT-Sicherheitsdokumentation
IT Security Documentation

Allgemein:

Dieses Dokument umfasst Hinweise zu den Airleader Kompressor Steuerungen vom Typ 2403, 2404, 3203, 3204 und 0601. Des Weiteren werden relevante Informationen zur Software Airleader-Online-Visualisierung gegeben.

Datensicherheit:

Sämtliche Daten werden in binärer Form gespeichert, und sind nur in Verbindung mit der entsprechenden Software auslesbar.

Datenaustausch:

Der Datenaustausch zwischen Controller und Visualisierungssoftware erfolgt per TCP auf Port 10050. Die übertragenen Daten werden ebenfalls nur maschinenlesbar in binärer Form übertragen.

Web-Interface:

Das Webinterface ist per http auf Port 80, und per https auf Port 443 erreichbar.

Der http Support ist abschaltbar, womit dann ausschließlich nur noch der SSL-Zugriff möglich ist.

Es ist ein Self Signed Zertifikat mit RSA 2048 Verschlüsselung hinterlegt. Das Zertifikat kann durch ein eigenes CA zertifiziertes Zertifikat ausgetauscht werden.

Die GUI ist noch über einen Zugangscode geschützt.

Schreibende Zugriffe sind zusätzlich durch einen Time Stamp/Key Mechanismus vor Zugriffen von außen gesichert (Man in the middle).

Offene Netzwerk Ports:

eingehend:

http:	80
https:	443
Modbus-TCP:	502 (optional)
OPC-UA:	52530 (optional)

ausgehend:

UDP Com-Server:	3001 (optional)

OPC-UA Sicherheit: (optional)

Der OPC-UA Server erlaubt folgende Zugangsmethoden:

1. Anonym: Benutzer sind nicht authentifiziert
2. Sign: Client wird über Zertifikat authentifiziert
3. Sign & Encryp: Client wird über Zertifikat authentifiziert, Sitzung ist verschlüsselt

Airleader Online Visualisierung:

Die Airleader Online Visualisierung (im Folgendem AOV genannt) ist eine J2EE Applikation. Als Basis dient ein Apache Tomcat Server.

Das Java Runtime Environment ist Bestandteil der Installation.

Versionsstand:

Tomcat:	9.0.98
OpenJDK:	1.8.0_352-b08

Zusatzkompenenten:

Log4J Version:	2.23.1

Offene Netzwerk Ports:

http:	8080
https:	443

AOV enthält ebenfalls ein Self Signed SSL Zertifikat mit RSA 2048 Verschlüsselung, welches ebenfalls durch ein CA zertifiziertes Zertifikat ersetzt werden kann.

Sowohl die Tomcat Core Installation als auch das Java Environment werden regelmäßig auf Updates und / oder Schwachstellen geprüft und gegebenenfalls aktualisiert. Dies erfolgt in etwa alle 6 Monate, oder nach Auftauchen einer Schwachstelle.