Digitale Sicherheit in Bergbauanlagen der RAG Austria AG – Übersicht und Beispiele

Ing. Mag. (FH) Markus Ripka, Chief Information Security Officer, RAG Austria AG, Wien

Die RAG Austria AG entwickelt und betreibt 11 Untergrund Gasspeicherstationen, sechs davon im Rahmen von Joint-Ventures sowie die Forschungsspeicher Pilsbach und Rubensdorf mit einem Gesamtspeicher-volumen von mehr als 6,2 Mrd. m3 für Speicherung von Erdgas und Lagerung von Wasserstoff.

Für eine Sicherstellung der Gasversorgung ist die Sicherheit im Bergbau der neben der Anlagenverfügbarkeit eines der wichtigsten Elemente. In den letzten Jahren hat sich die „konventionelle“ Sicherheit - i.S. von Einhaltung von technischen Normen und Rechtsvorschriften - verstärkt auch in Richtung digitaler Sicherheit im Bergbau entwickelt (Cyberattacken, etc.). Bei der digitalen Sicherheit geht es um den Schutz von Daten sowie Telekommunikations- und IT-Systemen. In Bezug auf Anlagen zur Energieversorgung sind dabei die Kriterien Verfügbarkeit und Datenintegrität von höchster Wichtigkeit. Die RAG setzt auf höchstmöglichen Standards hinsichtlich organisatorischer und technischer Maßnahmen.

Um die Organisation eines genormten Sicherheitsmanagements (z.B. ISO27000) voranzutreiben sollte zuallererst die Position eines Informationssicherheitsbeauftragten geschaffen und qualifiziert besetzt werden. Dieser führt dann eine Business Impact Analyse und Risikoanalyse über die Anlagen und IT- Systeme durch, um die Kritikalität und den Schutzbedarf zu bestimmen.

Die Durchführung einer Risikoanalyse bedingt ein aktuelles Inventar aller netzwerkangebundene IT und OT Geräte (z.B. PLS Steuerungen) pro Standort, weshalb eine automatisierte Inventarisierung anzustreben ist.

RAG Austria AG erarbeitet und verbessert die Maßnahmen digitalen Anlagensicherheit in periodischen Sicherheitsworkshop gemeinsam mit den Betriebsingenieuren, der IT-Infrastruktur und dem Informationssicherheitsbeauftragten (CISO). In diesem Rahmen werden mögliche Risiken für die Anlagen, Wirksamkeit bestehender Maßnahmen, neue Sicherheitsthemen und Vorfälle besprochen.

Die folgenden Themen entstammen dieser Workshopreihe und sollen als Anregung zur Verbesserung der digitalen Anlagensicherheit dienen.

Die Absicherung der Leitstandrechner, Engineering Laptops und Warten erfolgt mit zentral verwalteten Basissicherheitsmaßnahmen für Windows Betriebssysteme wie zum Beispiel Virenschutz, Updates, Applocker. Als zusätzliche Schutzmaßnahmen gibt es kein Internet, keine Emails, keine USB-Datenträger und keine Administratorberechtigungen für Benutzer auf Leitstandsrechnern und Warten.

Belegt wirkungsvoll ist die Netzwerksegmentierung des OT/IT Netzwerks nach dem Purdue Sicherheitsmodell mittels Firewalls. Dabei wird der Netzwerkverkehr von Anlage (OT), Leitständen und Servern (SCADA) und Büronetzwerk streng getrennt.

Eine Softwarelösung zur Angriffserkennung im OT Netzwerk überwacht mittels Portspiegelung auf den Netzwerkgeräten den Netzwerkverkehr auf abnormes Verhalten und Hinweise auf Angriffstätigkeit.

Ein Zentrales Logdatenmanagement im Anlagenbereich erfasst die Logdaten von PLS Steuergeräten und Netzwerkgeräte und kann so zusammen mit Systemüberwachung & Verbindungsüberwachung der PLS Steuerungen am SCADA System jederzeit Unregelmäßigkeiten im Anlagenbetrieb erkennen und melden.

Um einer Datenmanipulation auf den Steuerungen oder Sensoren vorzubeugen sind Grenzwerte für Sensorwerte in PLS Steuerprogrammen bzw. Grenzwertliste am SCADA Server zu hinterlegen. Zu diesem Zweck sind auch Passwörter auf PLS Steuerungen vergeben und es dürfen keine ungeprüften Fremdgeräte im Anlagennetzwerk betrieben werden.

Die Datensicherung aktueller PLS Steuerprogrammen sowie von Festplattenimages von Leitstands Rechnern und SCADA Servern hat regelmäßig zu erfolgen und überprüft werden. Die Daten werden monatlich zusätzlich auch auf Band dupliziert und an einen sicheren Ort ausgelagert. Die laufende Sicherung muss auch flüchtige Daten wie Regelparameter und Grenzwerte umfassen.

Zur Erhöhung der Resilienz sind ausreichend Redundanzen einzuplanen und Notfallpläne für ausgewählte Szenarien zu erstellen. Es ist dabei auf ausreichend Redundanzen und Ersatzteile für kritische IT/OT Systeme, Netzwerkgeräten und Prozesssteuergeräten zu achten. Auch redundante Kommunikationsleitungen, unterbrechungsfreie Stromversorgung und wenn erforderlich ein Ersatzleitstand sind einzuplanen.

Ein gemeinsamer Vorfallreaktionsplan für IT und OT inklusive Alarmierungs- und Ablaufprozessen für definierte Szenarien (Cyberangriff, Netzwerkausfall, Blackout, …) sorgt für rasches und koordiniertes Handeln.

Für Force Majeure Events wie Cyberangriffe oder Blackout Szenarien muss eine MSR Notfallplanung erfolgen. Der MSR Wiederanlaufplan pro Anlage beschreibt den Kaltstart der Anlage von Null inklusive Einspielen der PLS Steuerprogramme, restore der SCADA Server und Leitstände, einlesen der Grenzwertlisten und mechanischem Anlauf der Anlage.

Ein etabliertes Passwortmanagement stellt die Verfügbarkeit aller wichtigen IT und OT Passwörter im Notfall sicher, selbst wenn zentrale IT-Systeme nicht zur Verfügung stehen.

Nur durch enge Kooperation von IT und OT und im Zusammenspiel können die genannten Maßnahmen die digitale Sicherheit der Anlagen, in einem sich ständig wandelnden Umfeld, gewährleisten.

RAG Austria AG

Ing. Mag. (FH) Markus Ripka
Chief Information Security Officer

Markus.ripka@rag-austria.at
T +43 (0)50 724-5243

RAG Austria AG
Schwarzenbergplatz 16
A-1015 Wien

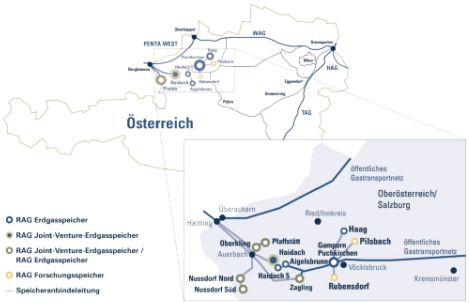
www.rag-austria.at

Agenda

- Überblick der RAG Speicher Standorte
- Organisatorische Sicherheitsmaßnahmen
- Absicherung Leitstandrechner, Engineering Laptops und Warten
- Sicherheitsmaßnahmen PLS Steuerungen und Anlagennetz
- Datensicherung PLS und SCADA
- MSR Notfallplanung und Resilienz

Überblick RAG und JV Speicher Standorte

- Die RAG entwickelt und betreibt 11 Speicherstationen, sechs davon im Rahmen von Joint-Ventures sowie die Forschungsspeicher Pilsbach und Rubensdorf mit einem Gesamtspeicher-volumen von mehr als 6,2 Mrd. m^3



Erdgasspeicher Puchkirchen/Haag		
Arbeitsgasvolumen	12,27 TWh	1.080 Mio. m³
Max. Ausspeicherkapazität	6,9 GW	520.000 m³/h
Max. Einspeicherkapazität	6,9 GW	520.000 m³/h

Erdgasspeicher Haidach 5		
Arbeitsgasvolumen	181 GWh	16 Mio. m³
Max. Ausspeicherkapazität	227 MW	20.000 m³/h
Max. Einspeicherkapazität	227 MW	20.000 m³/h

Erdgasspeicher Haidach		
Arbeitsgasvolumen	32,67 TWh	2.900 Mio. m³
Max. Ausspeicherkapazität	13,1 GW	1,16 Mio. m³/h
Max. Einspeicherkapazität	11,9 GW	1,05 Mio. m³/h

Erdgasspeicher Aigelsbrunn		
Arbeitsgasvolumen	1,5 TWh	130 Mio. m³
Max. Ausspeicherkapazität	567 MW	50.000 m³/h
Max. Einspeicherkapazität	567 MW	50.000 m³/h

Erdgasspeicher 7Fields (RAG)		
Arbeitsgasvolumen	6,2 TWh	550 Mio. m³
Max. Ausspeicherkapazität	2,6 GW	226.600 m³/h
Max. Einspeicherkapazität	1,7 GW	151.100 m³/h

Erdgasspeicher 7Fields (UNIPER)		
Arbeitsgasvolumen	17,6 TWh	1.550 Mio. m³
Max. Ausspeicherkapazität	0,1 GW	867.300 m³/h
Max. Einspeicherkapazität	6,1 GW	538.200 m³/h

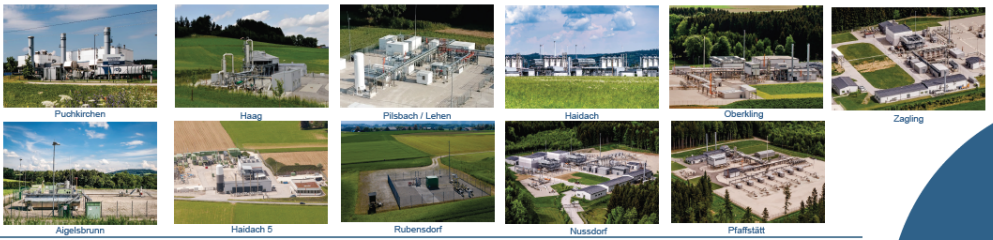
Summe der von RAG betriebenen Speicher		
Arbeitsgasvolumen	70,5 TWh	6.226 Mio. m³
Max. Ausspeicherkapazität	31,5 GW	2.783.900 m³/h
Max. Einspeicherkapazität	26,4 GW	2.329.300 m³/h

Leistungskennzahlen RAG Speicher im Stand Dezember 2020

* Haidach: Joint Venture mit Gazprom export und Wingas ** 7Fields: Joint Venture mit Uniper Gas Storage

Überblick RAG und JV Speicher Standorte

- Für eine Sicherstellung der Gasversorgung ist die Sicherheit im Bergbau der neben der Anlagenverfügbarkeit eines der wichtigsten Elemente.
- In den letzten Jahren hat sich die „konventionelle“ Sicherheit - i.S. von Einhaltung von technischen Normen und Rechtsvorschriften - verstärkt auch in Richtung digitaler Sicherheit im Bergbau entwickelt (Cyberattacken, etc.). Die RAG setzt dabei die höchstmöglichen Standards hinsichtlich organisatorischer und IT Maßnahmen.

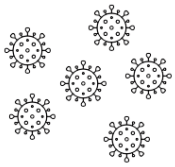


Organisatorische Sicherheitsmaßnahmen

- Sicherheitsmanagement z.B. ISO27000 und CISO Position etablieren
- Inventar aller netzwerkangebundene IT/OT Geräte pro Standort, möglichst automatisiert
- Durchführung einer Business Impact Analyse und IT Risikomanagement
- Jährlicher OT Security Workshop mit MSR Technikern, IT und CISO

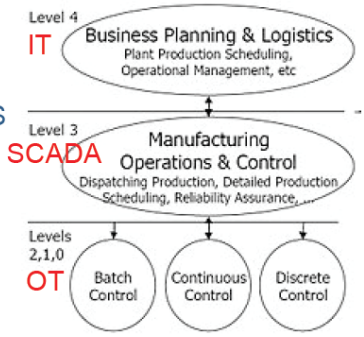
Absicherung Leitstandrechner, Engineering Laptops und Warten

- Basis Sicherheit Windows Betriebssystem (Virenschutz, Updates, Applocker) mit zentralem Management
- Kein Internet, keine Emails und keine USB Datenträger auf Leitstandsrechnern und Warten
- Keine Administratorberechtigungen für Benutzer
- Redundanzen z.B. Ersatzleitstand und duale Netzwerkanbindung



Sicherheitsmaßnahmen PLS Steuerungen und Anlagennetz

- Netzwerksegmentierung IT/SCADA/OT nach dem Purdue Sicherheitsmodell mittels Firewalls
- Systemüberwachung & Verbindungsüberwachung der PLS Steuerungen am SCADA System
- Zentrales Logdatenmanagement Anlagenbereich (Erfassung und Auswertung)
- Softwareunterstützte Angriffserkennung OT Netzwerk
- Passwörter auf Steuerungen
- Keine ungeprüften Fremdgeräte im Anlagennetzwerk
- Grenzwerte für Sensorwerte in PLS Steuerprogrammen bzw. Grenzwertliste am SCADA Server hinterlegen
- (Updates einspielen wo möglich)



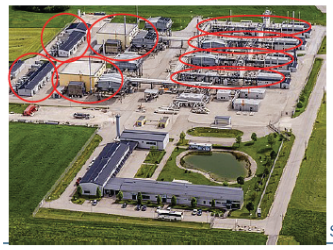
PERA Reference model: Decision-making and control hierarchy, (1992)

Datensicherung PLS und SCADA

- Backup und Auslagern der aktuellen Steuerprogramme (auf Festplatte und externe Datenträger)
- Festplattenimage/Backups von Engineering PCs, Leitstands Rechnern sowie SCADA Servern
- Laufende Sicherung flüchtiger Daten wie Regelparameter und Grenzwerte

MSR Notfallplanung und Resilienz

- Vorfallreaktionsplan für IT und OT inkl. Alarmierung über Dispatching Leitstand
- Wiederanlaufplan pro Anlage inklusive MSR von Null (Kaltstart inkl. Einspielen der Steuerprogramme und Anlauf der Anlage)
- Passwortmanagement (sicherstellen Verfügbarkeit der Passwörter im Notfall)
- Ausreichend Redundanzen und Ersatzteile kritischer IT/OT Systeme (Stromversorgung, CPUs, SCADA Server, Switches, Kommunikationsleitungen, Ersatzleitstand)



Strangprinzip Speicher Haidach (Schaltstationen, E-Verdichter, Gasbehandlungsstränge)

Disclaimer