QuantityWare Security Bulletin – Cyberattack Risks for Oil and Gas Companies

Synopsys

A current insideSAP article[i] targets security challenges and risks in the critical area of SAP Oil & Gas (and associated systems) bulk materials quantity data management. This security bulletin is our response to related customer inquiries, detailing how QuantityWare BCS (Bulk Calculations Solution) can assist in the governance of, and reduction of risk exposure in, this critical area.

Background

Industry business processes leveraging SAP OIL & GAS systems with SAP QCI (Quantity Conversion Interface), can be assigned to one of two quantity data flow models:

1. The historical **"distributed quantity data flow model"** – the SAP QCI is basically operated in **"blind mode"** – external measurement systems pass data such as temperatures, densities, pressures, volumes, weights etc. to the SAP ERP system and the SAP QCI merely accepts this data, typically performing only a rough check if volumes and weights are within pre-defined tolerance limits. This scenario is an acceptance of maximum risk exposure.
2. The modern **"integrated quantity data flow model"** – enabled with QuantityWare BCS, seamlessly configures the SAP QCI to allow it to act as a true **gate-keeper**, where all data passed from external systems are subject to rigorous validation and consistency checks; additional data requirements are calculated natively in the business system based on compliant and transparent calculation procedures. This scenario seamlessly minimizes risk exposure.

So, how does BCS enable risk minimization? BCS is based on three guiding principles:

- **Security** – quantity conversion data are the basis for all financial data. Unauthorized access to, & manipulation of, such data has to be prohibited. Calculations should be 100% ABAP-based.
- **Transparency** – quantity conversion calculations have to be auditable and trusted. Inspectors and business experts need to understand how the calculations work and be able to reproduce and validate calculation results
- **Compliance** – quantity conversion calculations have to be based on national and international measurement standards (API, ASTM, ISO, DIN, GERG, AGA and others)

These three principles are described in our working paper "Quantity data flow in the oil & gas supply chain– How can we ensure that our quantity data values are correct?"[ii]

Issues & Resolutions

As outlined in the insideSAP article[i], cyberattack possibilities must be taken seriously by oil and gas companies – neglecting this issue leads to exposure and risk:

"The researchers told attendees that cyberattackers could exploit SAP xMII and SAP PCo solutions that transfer data from tank information management systems to systems such as SAP IS-OIL in order to modify oil in-stock parameters. SAP systems connected with tank inventory systems such as Emerson Rosemount TankMaster also allow commands to PLC devices to adjust values such as the maximum fill limit of tanks, meaning a cyberattack could lead to an oil explosion" i

Here, the importance of any SAP QCI implementation's **gate-keeper function** is clear, i.e. the **"integrated quantity data flow model" should be considered a "must do".** Further risks within historical SAP QCI implementation are outlined in the insideSAP article[i]:

"According to the researchers, the easiest way for cyberattackers to falsify data about temperature, pressure, and other conditions is to hack an SAP or Oracle Asset Management solution. They outlined ways in which an ERP system can be compromised, including vulnerabilities, misconfigurations, unnecessary privileges and custom code issues. They also stressed that the oil and gas industry is susceptible to attack not just by USB but also remotely via the internet and corporate networks." i

"Vulnerabilities" and "Misconfigurations" translate to the usage of "CALL SYSTEM" with legacy calculation programs at the OS-level (e.g. "API 'C' routines"), or custom code (SAP QCI BAdI implementations). Such usage is **minimized or eliminated by BCS**. When paired with the QuantityWare automated test scenarios[iii], a transparent calculation results validation tool which is customer-definable, well documented, easily distributable, quick and stable, the customer can seamlessly reduce risk exposure in production. The current common scenario of manually testing bulk goods quantity values calculation before go-live (and then never again) can be seen to be an inacceptable risk exposure for such a critical application.

Conclusion

QuantityWare will continue to support its customers in their efforts to reduce such risks as described in this bulletin with the provision of our BCS – a fully mature software, additionally enhanced:

- through our network of certified BCS consultants implementing our solution
- via our continuous efforts on external certifications (Virtual Forge, SAP and others)
- via our proven in-house quality assurance and security processes
- through our proven PAIG implementation methodology

Remember, security does not come free. Additional effort for certified consultants or knowledgeable employees in implementation projects is required to allow leverage of the GRC potential delivered with BCS – as described in our PAIG methodology[iv].

For further information or discussion, contact john.mantle@quantityware.com

---

[i] SAP system vulnerabilities could leave oil and gas companies open to cyberattack - Posted on November 27, 2015 by Debra Hamilton in Market Insights (www.insidesap.com.au)

[ii] Quantity data flow in the oil & gas supply chain – How can we ensure that our quantity data values are correct? – QuantityWare working paper – 2012

[iii] BCP Test Manual – Test Case 07 – 2015

[iv] Bulk Calculations – Petroleum BCP 10B - Project Assessment and Implementation Guidelines (PAIG) - 2014