Success Story

Branch
Oil & Gas Industry

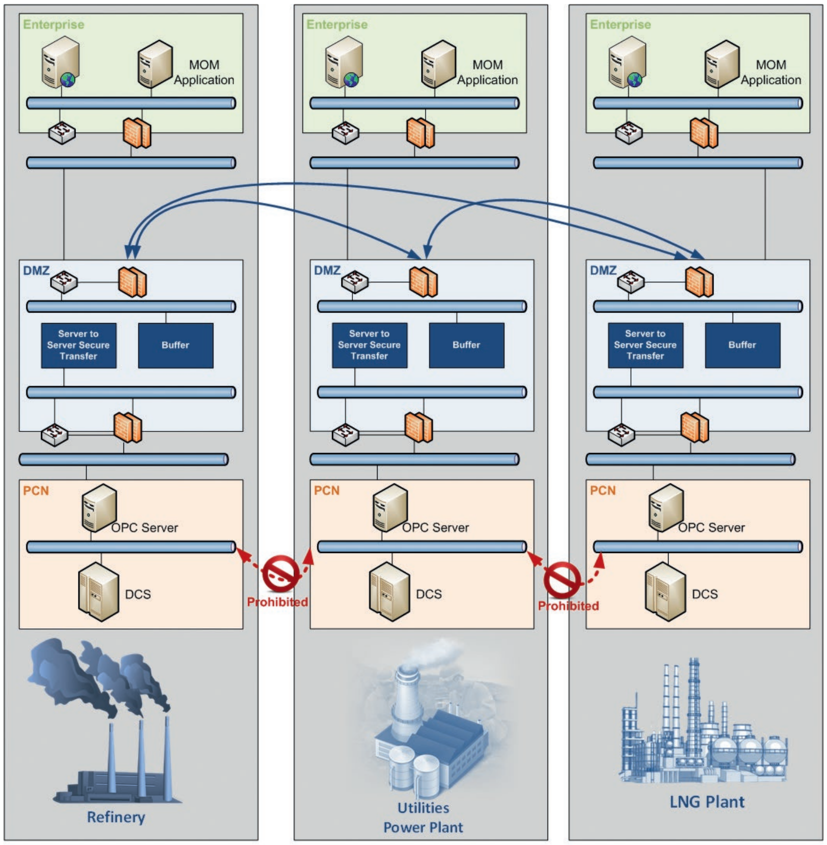
V1.0-en

OPC® FOUNDATION
WWW.OPCFOUNDATION.ORG

Exchanging your control systems data outside of your network securely is possible!

The need to share process data between production sites, refinery, petrochemical, gas and utility plants has been increasing for the past decade. These plants and production sites are typically located in the same area and have the need to exchange feed stocks, naphtha, ethane and utilities streams such as hydrogen, electricity, water, steam, and fuel gas, which created the requirement to exchange data between their metering and control systems.

With the tight network security policies of the different companies in the chemical, oil & gas and utility industries, it has become significantly challenging to integrate with third party systems.
Integration Objects has designed an OPC based solution to enable such integration while complying with the ISA 99 network security standards and the different stakeholders' policies. Such systems have already been deployed successfully to integrate refinery, utility, oil & gas stabilization, and LNG plants.



Companies with rigorous cyber security policies protect their process control assets by implementing a demilitarized zone (DMZ) physically separating and eliminating direct communication between the enterprise and the control networks. The challenge is how to continue exchanging critical data for accounting, safety and controls purposes with third party systems without introducing security risks, and at a minimum cost.
Integration Objects' OPC based secure solution for DMZ allows users to exchange critical data with third parties in real-time while:

- Respecting security policies of all stakeholders and ensuring the confidentiality of their data,
- Benefiting from an OPC UA interface allowing applications at the enterprise level to also securely send data back to the control system through the DMZ,
- Deploying an easy to maintain architecture by ensuring robustness against network disruptions and providing a quickly set-up graphical environment with only a few clicks needed,
- And avoiding significant capital investment as the solution takes advantage of the existing classic OPC based infrastructure.

OPC Based Secure DMZ Solution – Architecture

Note: Given the critical nature of such application and the number of companies involved in implementing this solution and their security policies, we were not able to obtain a common authorization to expose the success story. The following is a quote of the project manager, one of the stakeholders:
"Our project of integrating our systems with third party networks was delayed by nine months because we could not find a solution that works and complies with our network policy and all the third party's involved. We were pleasantly surprised to see Integration Objects providing not only a highly secure solution, but an OPC highly robust one".

Seamless data flow

The secure DMZ hosts a buffer that does not have any read or write capabilities, and includes only the tags that are needed for the specific data exchange. The server-to-server secure transfer, located in each side, will collect the data, on as needed basis and from the DMZ buffer, and will then transfer it to the OPC Server located in the process control network (PCN) and vice versa.

Tighten the security without complicating the configuration

All transferred data are encrypted to ensure data integrity and confidentiality. Therefore, data will be protected against malicious attacks, as it will not allow any spoofing, sniffing or hacking. In addition, the data access requires user authentication from the buffer server level down to the tag level:

- User authentication is based on Active Directory in order to confirm the identity of the user trying to connect and access the data. This mechanism prevents unauthorized access that can be issued either internally or from an outside network.
- Granual access rights are configured using user profiles and specifying the set of permissions that defines which tags, assigned users are allowed to browse, read or write, or read/write.

The firewalls are configured such that only one TCP port is authorized. This port can change any time at the discretion of the network security team of each company.

All of these security features are easily configurable using an intuitivegraphical interface. They also do not require a public certificate provider or access to the Internet.

Advantages

The OPC based secure DMZ solution has the following main advantages:

- None of the DMZ is bypassed. All communications with the PCN are initiated from the DMZ.
- Remote communications are not based on classic OPC/DCOM.
- The communications between the different components within the same side or between different sides are reestablished automatically after recovering from network glitches.
- No data loss is encountered when the network communications are down. This is ensured by using a buffering solution for data history catch up purposes.
- Only a single TCP port is needed to be open in the firewalls. This port is configurable and is not a public or known port. Moreover, each party can use a different port for the communications to their PCN and does not need to disclose this information to the third party.
- Data is encrypted and therefore, it is invisible to hackers, as it does not allow any spoofing or sniffing.
- Thanks to an OPC UA interface, applications at the enterprise level such as production planning or asset optimization applications can also securely exchange data with the control system through the DMZ.
- The remote communications can be established from different domains, across VPN and through, VSAT and WANs. Users can also fine tune communication timeouts and data compression parameters for better performance of data transfers across their network.

The OPC based secure DMZ solution allowed to integrate refinery, utility, oil & gas stabilization, and LNG plants by exchanging real-time process data in a secure way. It implements an open architecture without compromising the security, takes advantage of the classis OPC infrastructure and Active Directory and still benefits from the current industry standards in particular OPC UA and ISA 99.

About Integration Objects

integrationobjects.com

Integration Objects is a world-leading systems integrator and solutions provider specialized in OPC connectivity, plant automation, cyber security, enterprise integration, knowledge management solutions, operational and manufacturing intelligence, preventive detection of abnormal events, online diagnostics and root cause analysis, for power and utilities, as well as process and manufacturing industries around the globe. Our goal is to help our clients maximize plant safety, increase asset availability, and efficiently drive decision-making process.

Integration Objects offers an extensive OPC product line, with more than 40 out of the box software products including client and server products for security and connectivity with data tunneling, brideging, archiving and data history catch-up.

For more information about Integration Objects, and its solutions, please visit the website at www.integrationobjects.com

About OPC Unified Architecture (OPC UA)

OPC UA is the interoperability standard for multi-vendor, multi-platform data exchange that is secure and reliable from small sensors up to IT Enterprise level systems. This technology provides open connectivity across multiple products, regardless of hardware platform or software operating system. OPC UA (the IEC 62541 standard) includes automated discovery, security by design, data encryption, and exceptionally powerful information modeling.