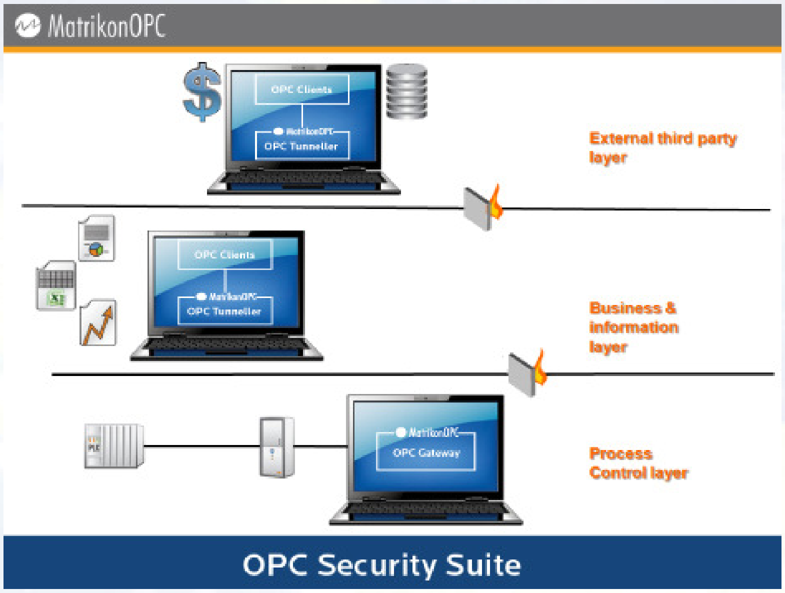
OPC Security - Providing Data Access on a Need-To-Know Basis

The amount of data required to complete a task is different for each level of personnel in your plant. The control system engineer might require having full read and writing access to all points in the automation system while an operator might only require access to a few points in the system in order to view the status of a machine and control it. This might be the same case for those at the management level - personnel at that level might only require read access to key performance data items.

With the Native support for the OPC Foundation's OPC Security specification, MatrikonOPC Servers offer complete control over item browsing, adding, reading, and writing - on a per-user-per-point basis. Granular control over data access helps deliver the right data to right people and prevents accidental or un-authorized OPC data access. This role based security adds another layer to a system's overall Defense-in-Depth strategy.

Typical Use Cases of OPC Security Suite

- **Process Control Layer:** Based on the plant floor operator's permissions, the operator will have control over the production machines to control the plant's operations For example, the operator requires full control over Area A and the ability to remotely monitor Area B - based on their login, they will be able to control Area A while only monitor Area B
- **Business and Information Layer:** Based on the plant manager's permissions, the manager will be able to monitor the plant's operations without having to control it in order to know the performance of their plant. For example, plant managers are only interested in monitoring the daily results of the plant's operations and the data of every single machine. Based on their permissions, they will be able to only monitor the daily results.
- **External Third Party Layer:** Users that are located outside the plant network might require access to the same level of data as the plant manager's level, but the data need to be secured. With the right encryption, the data will be delivered to them reliably and securely using the OPC Security Suite.



MatrikonOPC

OPC Security - Providing Data Access on a Need-To-Know Basis

The MatrikonOPC Security Suite provides the essential tools to secure existing OPC architectures. There is no need to replace or disturb any OPC components, regardless of whether they are OPC Security enabled or not. The MatrikonOPC Security Suite is compliant with the OPC Foundation’s OPC Security Specification and provides you with the security you need. If your business can be impacted by weak security, we have the tools to harden any OPC architecture. Future-ready and Legacy-friendly.

Enabling Products

- **MatrikonOPC Security Gateway**

  Supporting all vendor compliant OPC servers, MatrikonOPC Security Gateway fills security gaps in any existing OPC architectures. Security Gateway provides configurable access to the OPC architectures and full control for the user. Users can control who can browse, add, read or write per tag.

- **MatrikonOPC Tunneller**

  Eliminating the headaches associated with DCOM, MatrikonOPC Tunneller securely connects OPC software right out-of-the-box. For integrators looking to shorten integration time or improve performance, MatrikonOPC Tunneller is the tool of choice. MatrikonOPC Tunneller supports DA, HDA, data compression, encryption, and is extremely easy to install and configure.