General technical conditions for OPC interfaces

Within the scope of services as offered, an OPC interface has been agreed upon for exchanging data between the systems of the client and the system of atlan-tec Systems GmbH (hereinafter referred to ats).

It should be noted that networked OPC access - especially according to the OPC DA-standards - requires extensive user privileges/ permissions. These privileges will be granted by the ordering party as required.

Especially in the case that the OPC-interface follows the OPC data access standard, the use of an OPC-tunnel and an appropriately configured firewall is recommended by ats, to protect the process control system from network threats. In the case of the OPC UA standard, a firewall is recommended by ats.

An OPC tunnel translates OPC DA data access operations to TCP/ IP protocols which communicate in a transparent manner using TCP/ IP ports. This limits the risk of malware, like computer viruses, obtaining access to the control system via the OLE interface of the OPC server.

Alternatively, the ats OPC client can directly access the OPC server, without a firewall, provided that OPC server and OPC client both share the same network with the control system and firewalls insulate this network from the outside world. However, it needs to be considered that networked OPC UA communication without an OPC tunnel is always reducing the security of both sides.

The ordering party or their automation specialists make sure that the OPC server is installed on a computer with adequate performance reserves. This can be either a separate computer or a control system server, as long as it is not overly stressed by other control system functions. If a control system server has an intermittent workload of more than 50% during normal operation, or if it contains a database, or if it connects to a database, ats and the ordering party will agree upon not using this server as an OPC server in addition to its normal tasks.

Regarding the OPC interface, the partners agree to maintain stability and functionality of the ordering party's system by using only an OPC server of at least version 2.X which has been tested and certified by the OPC foundation (www.opcfoundation.org). The usage of an untested or noncertified OPC server will result in a partial loss of warranty.

The ordering party may secure their control system by placing a firewall between the ats system and the OPC server of the control system; however, they must make sure that the firewall processes the OPC queries to both directions. In addition, the ordering party may switch off the writing permissions to all OPC variables which are not manipulated variables or setpoints according to the common definition.

The ordering party will make sure that all necessary variables are available on the OPC server for reading, or, if necessary for the system as installed by ats, also for writing. The ordering party will transfer a systematic list of variables including OPC addresses, SI units, variable names, plain language variable designations and comments in an Excel file, once, at the beginning of the works. This list must be complete and correct. If such a table is missing or such a table is not in accordance with the OPC variable configuration of the server, a cost increase will be incurred.

Once the system is in operation, the ordering party will ensure the availability of current measured (and where necessary calculated) values on the OPC server at any time. The OPC server has to produce these values constantly and in real time according to the standards OPC DA (data access) or OPC UA (unified architecture). Also, the OPC server must immediately accept all values from the ats system when they are written to the server, and it must then transfer them to the receiving system reliably. For this purpose, the ordering party ensures the functionality of their internal interfaces and takes care of the allocation of sufficient resources for their systems, networks and interfaces. Delays of the OPC server response are not a liability of ats.