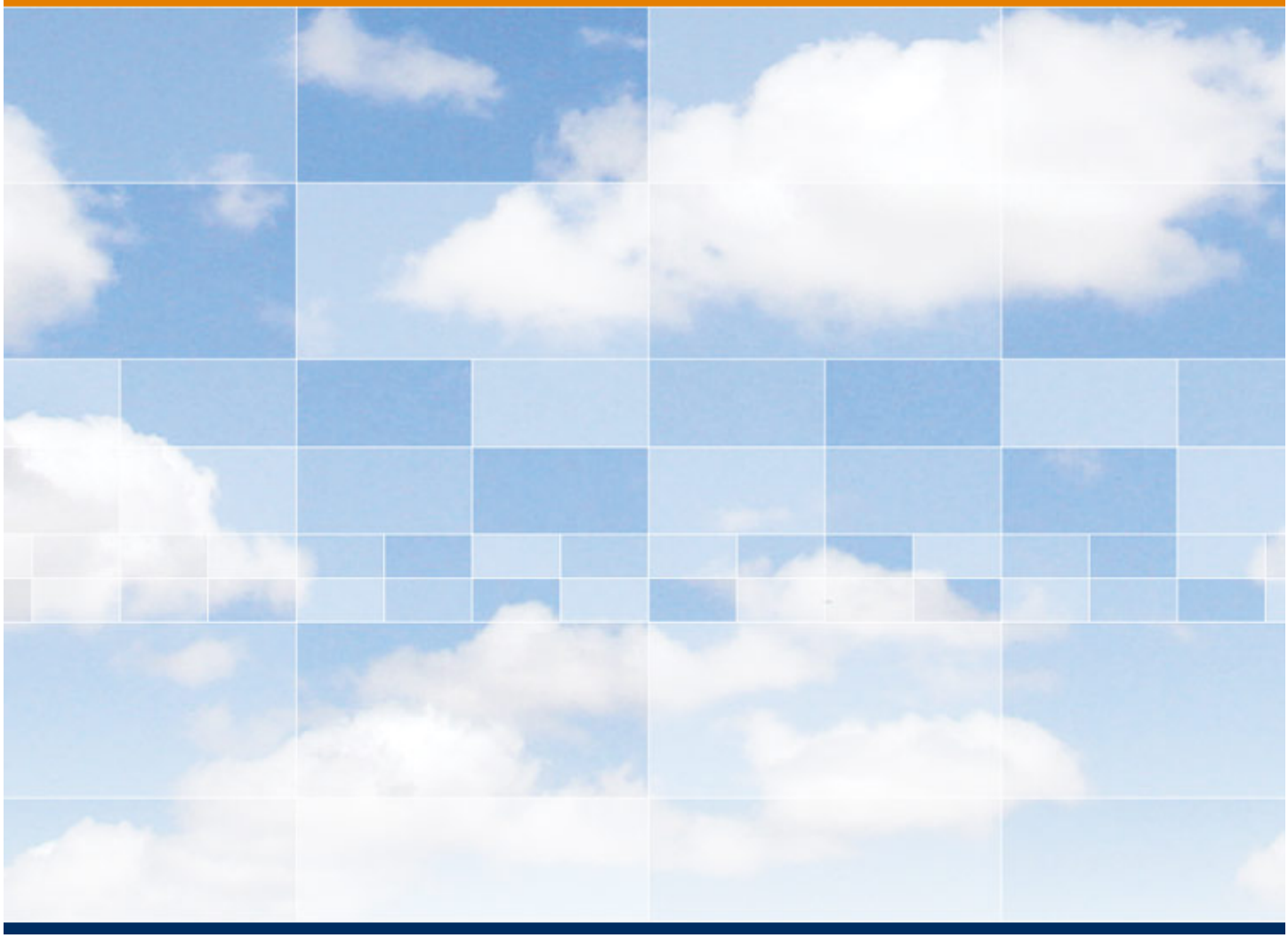
MatrikonOPC



Ensuring OPC Connectivity in Mission Critical Applications

Eric Murphy
Matrikon Inc.
September 2006

Ensuring OPC Connectivity in Mission Critical Applications

From oil refining to industrial manufacturing to power generation, no matter what business people are in, they depend on certain systems to run their business. Today's world turns on the uninterrupted flow of data and communications, and to keep it flowing OPC plays an increasingly mission-critical role in the enterprise.

In the early days of OPC adoption, systems tended to be limited to supervisory applications, history collection and auxiliary data systems. This was due to a reluctance to use PC based platforms in the control environment. As Microsoft operating systems and Ethernet based communications became more reliable and accepted, major control system vendors introduced operator stations, engineering consoles and application platforms running on PC hardware. These factors coupled with the rise of OPC as the preferred communication standard, led to an accelerating penetration of OPC into mission critical architectures. OPC is now a cornerstone component of many mission-critical or near safety-critical applications such as turbine-compressor monitoring, burner management systems, rail system management, radiation detection and reporting, and many more. This has significantly increased the need to assure that OPC can deliver reliable, 24 x 7 operation.

What Does Mission Critical Mean?

While there are differences of opinion about the definition of mission-critical applications, the general consensus of what "mission critical" means centers on the following attributes:

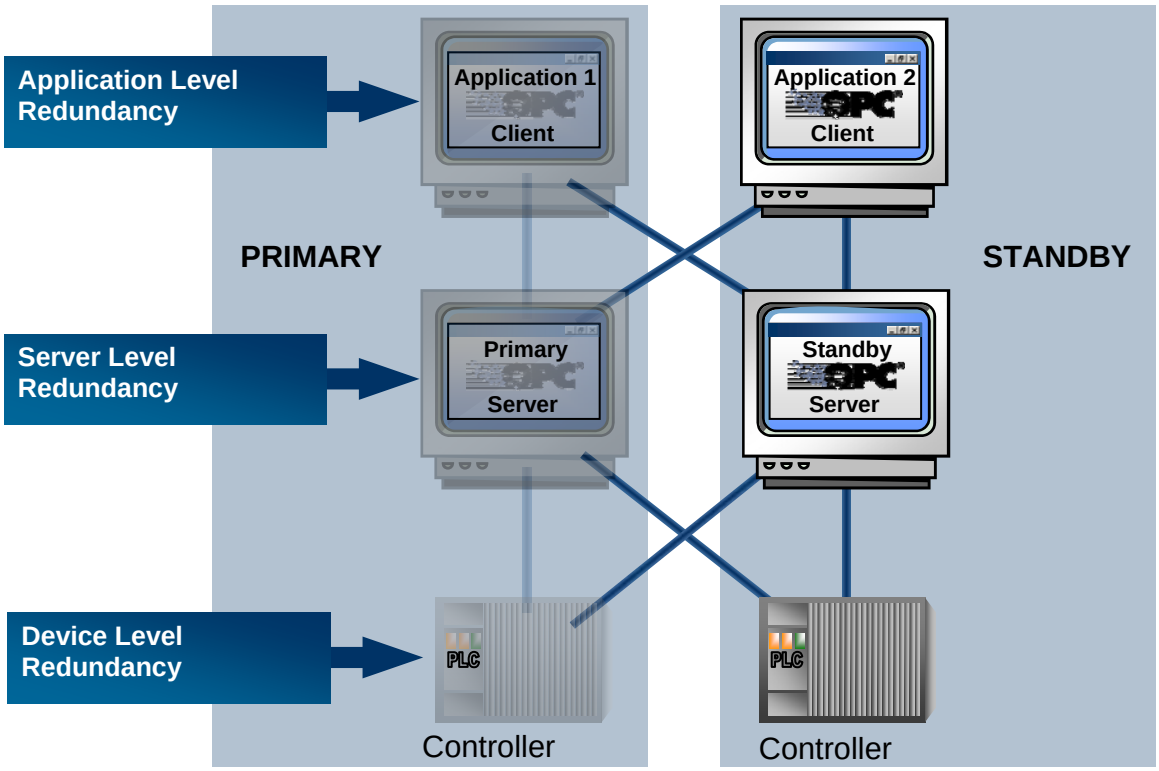
- Critical role: The role of software in fulfilling the mission must be crucial to the successful performance of the organization in which it is used.
- Critical view: The operational or controlling view of the system must be maintained at all times to ensure safe or proper operation.
- Critical data: Environments which monitor, store, support and communicate data cannot lose or corrupt the data without compromising their core function.

Once an application or components of an architecture are deemed to be mission critical, the next step is determining what can go wrong. A basic OPC system is comprised of an OPC client on one PC, communicating over the network to the OPC server on another machine. This involves multiple opportunities for system failure, including hardware faults, software or operating system incidents, and cabling or network routing failures.

What is the Solution?

One guiding principle for OPC mission-critical design is that the infrastructure is only as reliable as its components. The entire system must be made fault tolerant and able to remain functional in the event of a failure of one of the components. Adding redundant components significantly increases both fault tolerance and system reliability. In response to this need many OPC vendors are supplying products that enable OPC redundancy at multiple levels in the OPC architecture. A common system configuration is the three tier redundancy model.

OPC Three Tier Redundancy Model



As the name implies, this model applies redundant software and communication channels at the three major levels of the architecture; the OPC client application, the OPC server and the end device or data source.

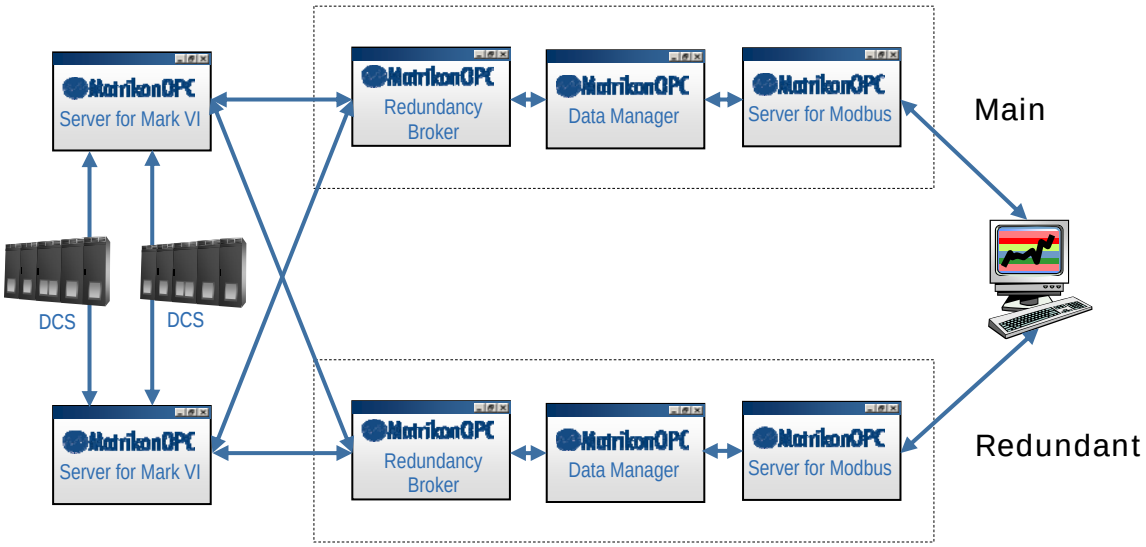
Often in mission critical systems, the controller or data collection device is of a fault tolerant design and is implemented in a redundant primary/secondary configuration. In order for an OPC server collecting data from these devices to seamlessly handle the dual configuration, it needs to have been designed to support *device level redundancy*. This means that a single OPC server can fail between two devices configured as a redundant pair, in a timely fashion without any action required by the OPC client. Increasingly more OPC vendors are offering OPC servers that support device or communication channel redundancy, particularly for controllers that are commonly installed in a redundant configuration.

Server level redundancy behaves in a similar manner, in that a single OPC client can fail between two OPC servers that have been implemented as a redundant primary/secondary pair. Typically this requires that the OPC vendor has implemented the redundancy functionality as part of the OPC client design. However, due to the nature of the OPC standard, server level redundancy is possible even if the OPC client has not been designed for redundancy. Since any OPC client can communicate with any OPC server, a redundancy enabled middleware application or broker can be inserted into any OPC architecture. The OPC redundancy wedge proxies all communication between the OPC client and the redundant OPC server pair and handles all aspects of the failover, such as how and when failover occurs, initiating connections, and OPC item management and clean up.

The final tier, *application level redundancy* often encompasses more functionality than just the OPC client connections. A typical configuration involves two applications running as a redundant pair that are continuously exchanging ‘heartbeat’ messages or status information. In the event the

secondary application losses communication to the primary application, it will establish a connection to the OPC server and assume the data collection responsibilities.

In some cases data collection is deemed critical due to regulatory requirements, such as the data required for U.S. Environmental Protection Agency (EPA) reporting. A real world use case is the Continuous Emissions Monitoring Systems (CEMS) used to collect data for the Environmental Group at Santee Cooper. The CEMS system provides information on gas turbine operation to ensure environmental standards are enforced. This critical system must function correctly and the data stream must be continuous. Emission reporting requires a minimum 98% uptime. Failure to meet reporting standards could result in fines and other penalties. Santee Cooper uses MatrikonOPC products in a multiple level OPC redundancy architecture to ensure meeting this requirement.



Although the stability of off-the-shelf computer hardware and operating systems has improved significantly over the last few years, system failures can and still do occur. In order to ensure the constant operation of their mission critical OPC applications, industry leaders turn to OPC vendors and products that provide redundancy. Oil and gas, power generation, waste water and utilities provide mission critical services to people every day. OPC redundancy ensures their crucial control data is always flowing.

Eric Murphy, Advanced Architecture System Design Engineer, MatrikonOPC

Eric Murphy, BSc, PEng (Alberta), Eric is a Chemical Engineer with a Process Control specialization and an OPC expert. Eric has been a part of the OPC community since its early beginnings in the mid-1990s. Eric is heavily involved with the OPC Foundation and currently acts as the chair for the OPC Historical Data Access (HDA) working group. Eric is also a member of the OPC Technical Steering Committee (TSC) and an active member of the OPC Unified Architecture (UA) working group.

Visit Eric at his Blog the OPC Exchange **http://blog.matrikonopc.com/** to follow the latest trends and discussions about OPC technology, or visit **http://www.matrikonopc.com** for free downloads.