

Data reliability and security kit

Read the guides, clarify the project questions and complete the worksheet with your team.

01 Store & Forward: how to size an outage buffer

Build a transparent estimate from record rate, outage duration, record size and destination recovery capacity.

02 OPC UA certificates: a secure connection checklist

Check trust, application identity and access rights separately to build a repeatable commissioning process.

03 Project worksheet

Space for meeting notes, owners and acceptance evidence.

13 September 2026 | English

This workbook is a planning aid. Product version, plug-in availability and licence scope must be verified for the project.

Store & Forward: how to size an outage buffer

Build a transparent estimate from record rate, outage duration, record size and destination recovery capacity.

A buffer is a capacity decision

Temporarily retaining data when a database or network is unavailable supports continuity. OPC Router offers Store & Forward as an add-on; confirm availability and behaviour for the selected version and connection. Storage is finite. Power loss, disk failure, queue limits or misconfiguration can still affect delivery, so buffering should not be described as an unconditional zero-data-loss guarantee. Decide which outage you need to cover and for how long before choosing storage.

Estimate the raw volume

Raw space is approximately records per second multiplied by bytes per record multiplied by outage seconds. At 100 records/s, 500 bytes/record and a four-hour outage, the raw volume is 720,000,000 bytes, or about 0.67 GiB. Field names, indexes, queue representation and filesystem overhead may increase actual storage. Multiply the raw estimate by a measured overhead factor and a safety margin. The calculator's default factor is an editable planning assumption, not a product specification or capacity guarantee.

Calculate backlog recovery

New data continues to arrive after the connection returns. If the destination can process 150 records/s while the source produces 100 records/s, the old backlog drains at only 50 records/s. A four-hour backlog of 1,440,000 records therefore takes approximately eight hours to clear. If destination throughput is equal to or lower than source throughput, the backlog cannot drain. More disk space alone does not remove this bottleneck; investigate destination writes, batching and source sampling.

Verify behaviour on site

Set alert thresholds for disk use and the age of the oldest queued record. Test ordering, persistence through restarts and duplicate handling at the destination. Reconcile source and destination record counts. Redundancy and Store & Forward address different failure modes; neither automatically replaces the other. Before production, run an outage and recovery experiment using a representative workload. Update the estimate from observed record sizes, throughput and queue behaviour rather than treating the initial calculation as a final hardware design.

Technical references

OPC Router Store & Forward

<https://www.opc-router.com/add-on-store-and-forward/>

OPC UA certificates: a secure connection checklist

Check trust, application identity and access rights separately to build a repeatable commissioning process.

Separate identity from permission

An OPC UA application certificate helps establish the identity of the application at the other end of a connection. Deciding which tags a user may read or write is a separate authorisation decision. Connecting to a trusted application does not mean every user should have every permission. Start with the read access needed for the use case. Apply a separate account, explicit scope and the plant's change procedure to write operations. Document why each permission is needed.

Manage the certificate lifecycle

Assign responsibility for certificate creation, distribution, trust-list approval, renewal and revocation. Verify fingerprints through a trusted channel. Do not enable automatic trust for every certificate simply to make an error disappear. Synchronised client and server clocks matter for validity checks and incident analysis. Recheck endpoint and certificate matching after machine or hostname changes. Record the renewal procedure while commissioning, when the people responsible for both ends of the connection are available.

Keep network boundaries intact

OPC UA security does not replace plant network design. Limit access to the systems that need it and avoid exposing controllers directly to the internet. Document data flows, firewall rules and ownership at the IT/OT boundary. Diagnose certificate, endpoint, DNS and permission failures separately instead of permanently disabling security to restore connectivity. Remove passwords and private keys from diagnostic packages shared with support. A temporary troubleshooting change needs an owner and an explicit reversal step.

Include negative acceptance tests

In a test environment, try an invalid certificate, an expired certificate, an unauthorised user and an incorrect endpoint. The system should reject them as intended and produce useful diagnostics. Also test reconnection after certificate renewal. Manage private-key backup, access and storage under the organisation's security policy. Add the certificate owner, expiry date and next review date to the commissioning record so security remains an operational process after the integrator leaves.

Technical references

OPC UA Security Model

<https://reference.opcfoundation.org/specs/OPC-10000-2/4>

03 / PROJECT WORKSHEET

Complete with your team.

Project / plant: _____

Date / owner: _____

Decision / check	Notes, owner and verification
Records/s / bytes/record	
Outage / overhead / safety margin	
Destination rate / recovery time	
Disk and queue alert threshold	
Certificate owner / renewal date	
Outage and restore test	

Next step

Share your open questions and source-destination systems with info@opcturkey.com. Interactive tools:
opcrouter.com.tr/en/tools