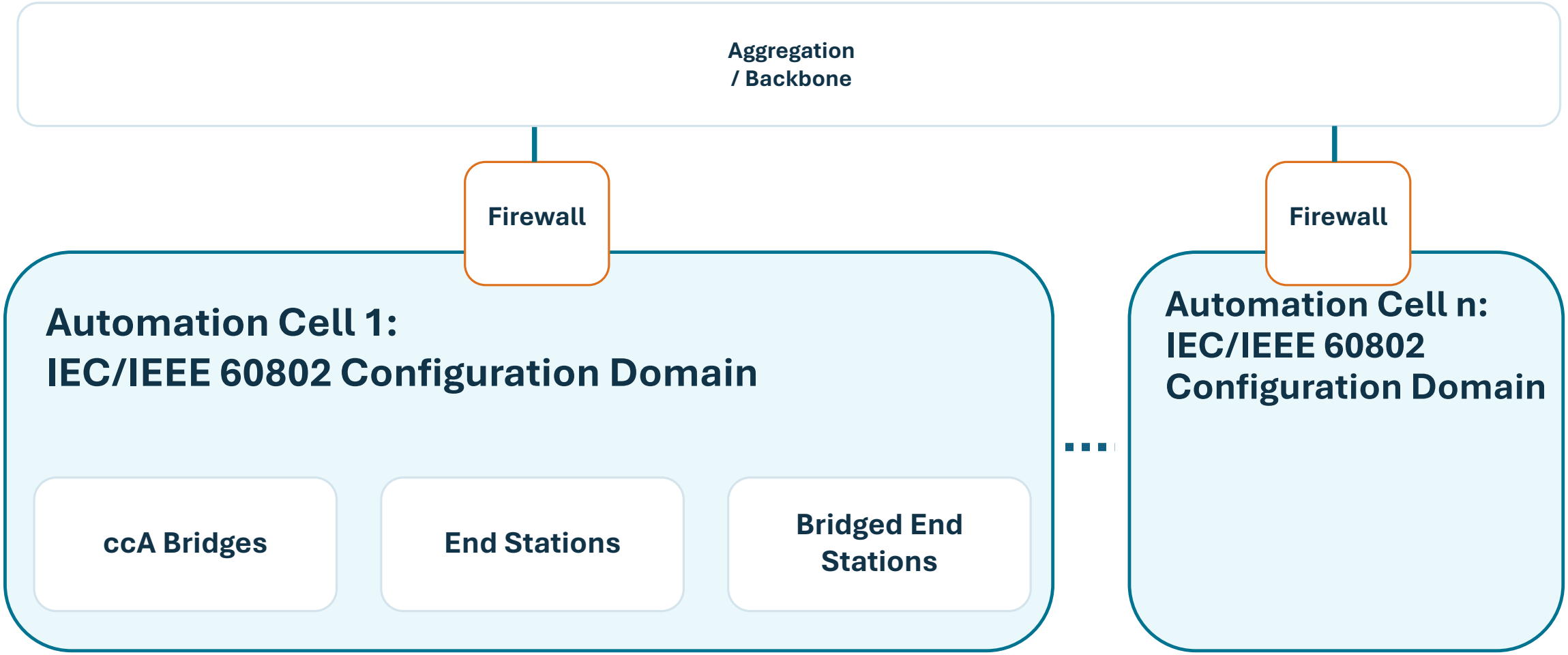
Seamless Redundancy in IEC/IEEE 60802 Configuration Domains

Architectural Requirements, Design Principles, and Constraints

Günter Steindl (SIEMENS AG)

Plant automation is structured into automation cells



Customer Requirements

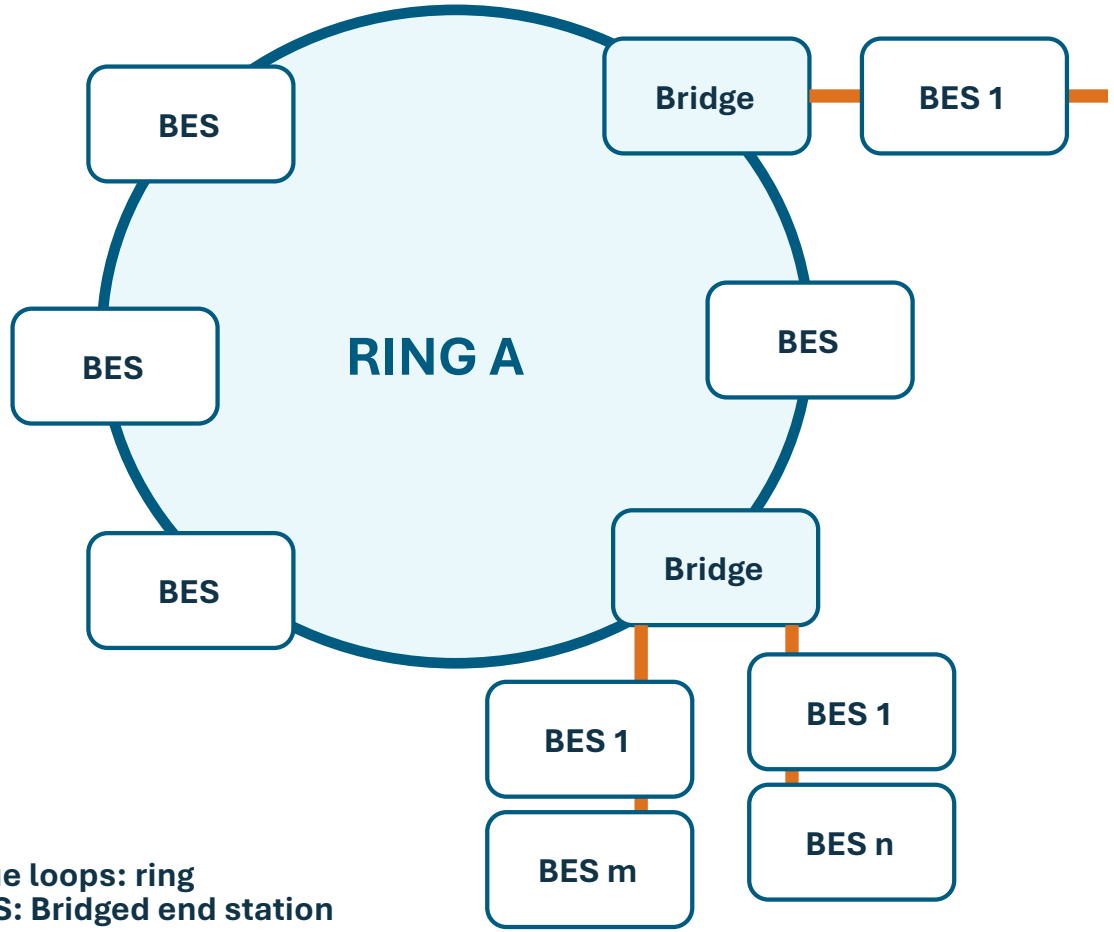
Protect any application traffic within the designated protection scope of the Configuration Domain

- Protocol-independent
- Unicast, multicast, and broadcast traffic

Support concurrent operation with other network functions

- Time synchronization
- Neighbor discovery
- MACsec
- Active network topologies
- …

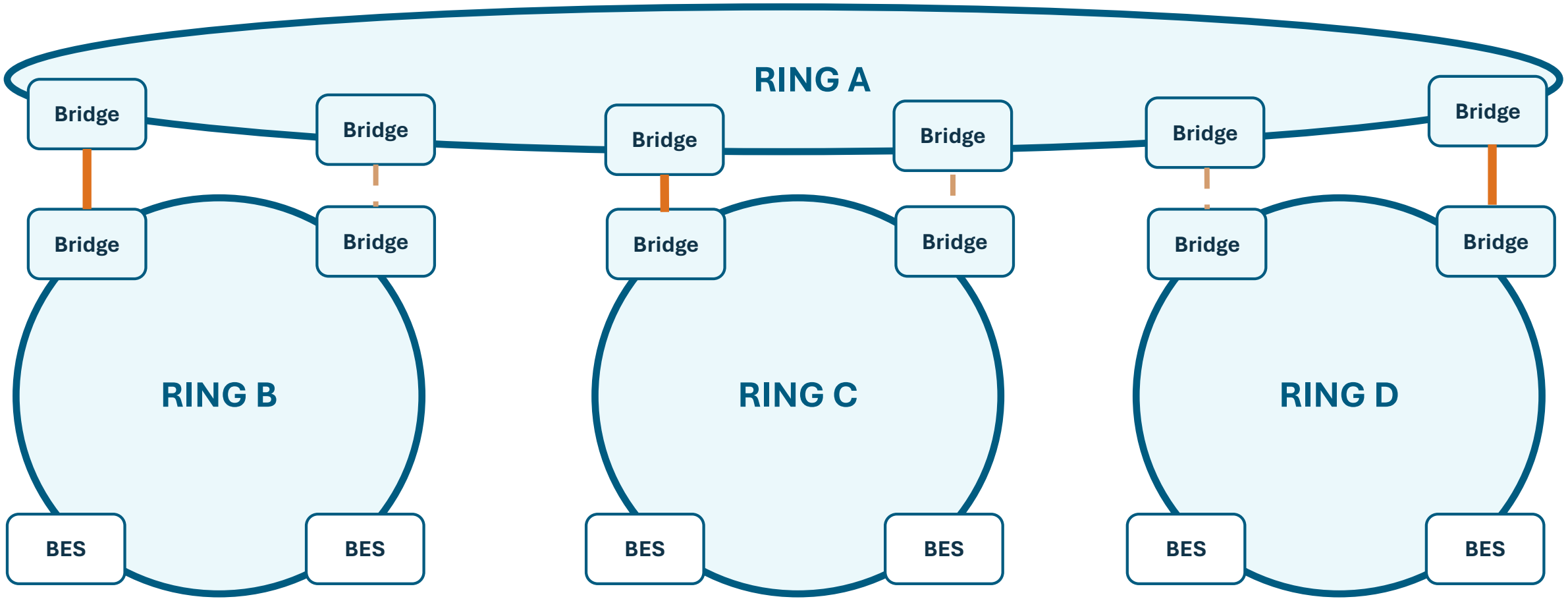
Bridged end stations and topologies



Blue loops: ring
BES: Bridged end station
Orange: spurs

- Bridged end stations(BES) are cost efficient
- Rings can be build using BES and Bridges
- Bridges allows the connection to additional stations or rings

More complex topologies



Blue loops: rings
Orange: coupling spurs
Dashed: optional second spur

One Automation Cell can be large

1,000

Stations in one Configuration Domain

50

Stations in one ring

64

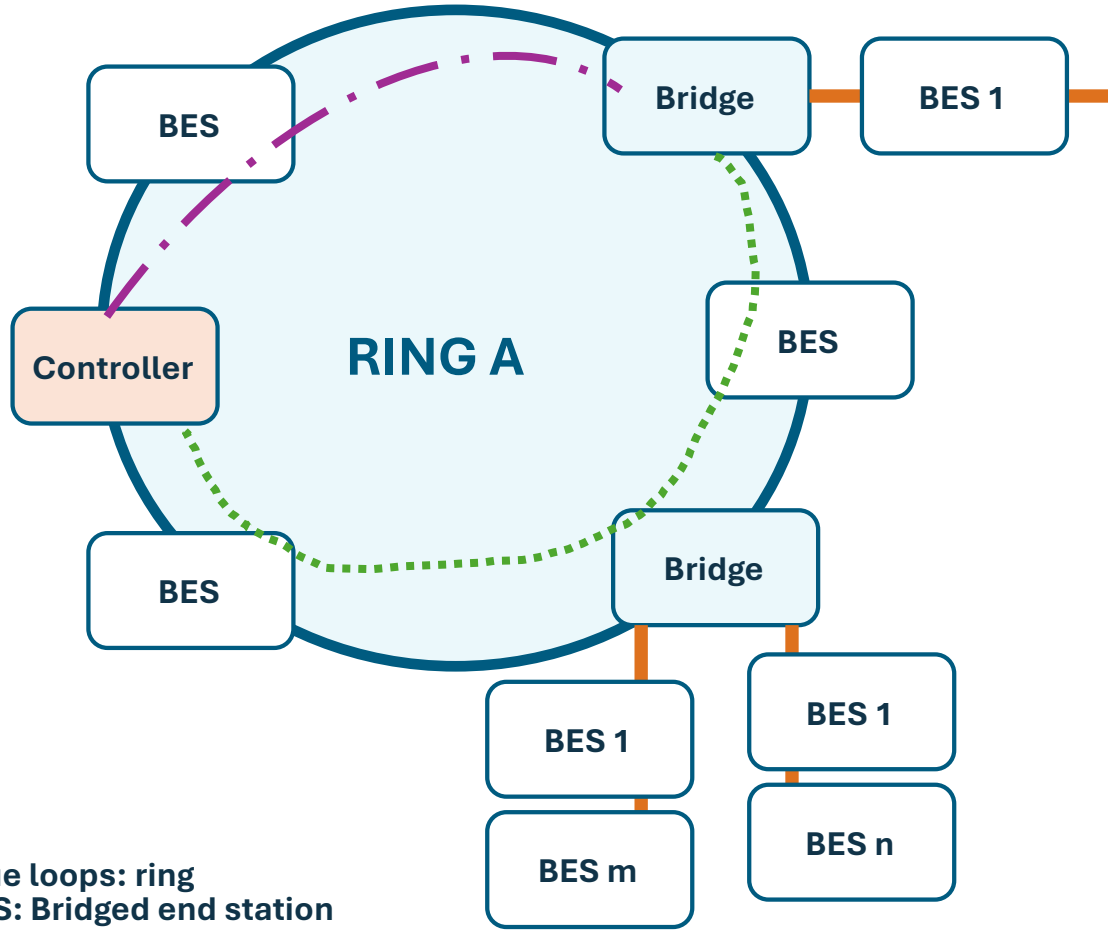
Maximum hops due to synchronization

128

Stations connected to the spurs of a Bridge of a ring

A single controller can control up to 999 stations. Therefore, all real-time traffic within a Configuration Domain may converge at the controller or at the bridge connecting the controller to the network.

Example
Controller as endpoint



Blue loops: ring
BES: Bridged end station
Orange: spurs

- Propagation delay between the lilac and the green path may be 4ms (or more)
- A controller may handle 999 real-time connections with seamless redundancy
- A controller may handle additional connections with seamless redundancy

Dynamic Automation Requires Dynamic Communication

- Automation cells form and change during operation
- AGVs and modular production dynamically change the topology
- Static communication paths cannot be assumed
- Offline traffic engineering is not feasible
- Seamless redundancy shall not depend on pre-engineered paths or schedules

- Time-Aware Shaping relies on pre-engineered paths and schedules, which conflicts with dynamic automation

Profiling FRER for the IEC/IEEE 60802

Dynamic traffic identification

- Cover eligible unicast, multicast, and broadcast traffic without configuring every communicating pair.
- Keep sequence/recovery contexts distinct when multiple sources use the same group destination address.

FRER in bridge components

- Support replication and elimination in ccA bridge components.
- Ordinary attached stations must not need FRER themselves.
- Eligible traffic entering a ring shall be identified, sequenced and replicated onto its redundant ring paths.
- Copies leaving the ring shall be recovered and eliminated before a single frame is delivered to an internal station or spur.
- Redundant coupled rings (inter-ring couplings) shall be possible.

Dynamic automation lifecycle

- Automatically establish, update, and retire identification, sequence, and recovery state as stations join, move, restart, or leave.
- Specify a measurable time until protection becomes effective.

Cover capacity

- Dimension the controller-side convergence point (for replication and elimination) for up to 999 sending stations and a ring bridge for 128 stations on its spurs.
- Specify concurrent context count, throughput, and sequence-history depth separately.

Ring-local single-fault protection

- The profile shall maintain seamless delivery of eligible traffic between surviving nodes of each ring after the failure of any one ring link or ring node.
- It shall support one such failure per ring concurrently in multiple rings.
- Failures of spur links, including inter-ring couplings, are excluded.
- Delivery to a failed node or to devices reachable only through it is not guaranteed; neither is inter-ring connectivity if the failed node terminates the only coupling.

Coexistence with per-port protocols and their redundancy mechanisms

- FRER shall not replicate gPTP, LLDP, or other per-port control traffic, including MACsec/MKA link traffic.
- It shall operate concurrently with MACsec on each applicable link.
- It shall not interfere with the independent redundancy and failover mechanisms of per-port protocols, including IEEE 802.1AS hot-standby time synchronization.

Questions?

Thank you!