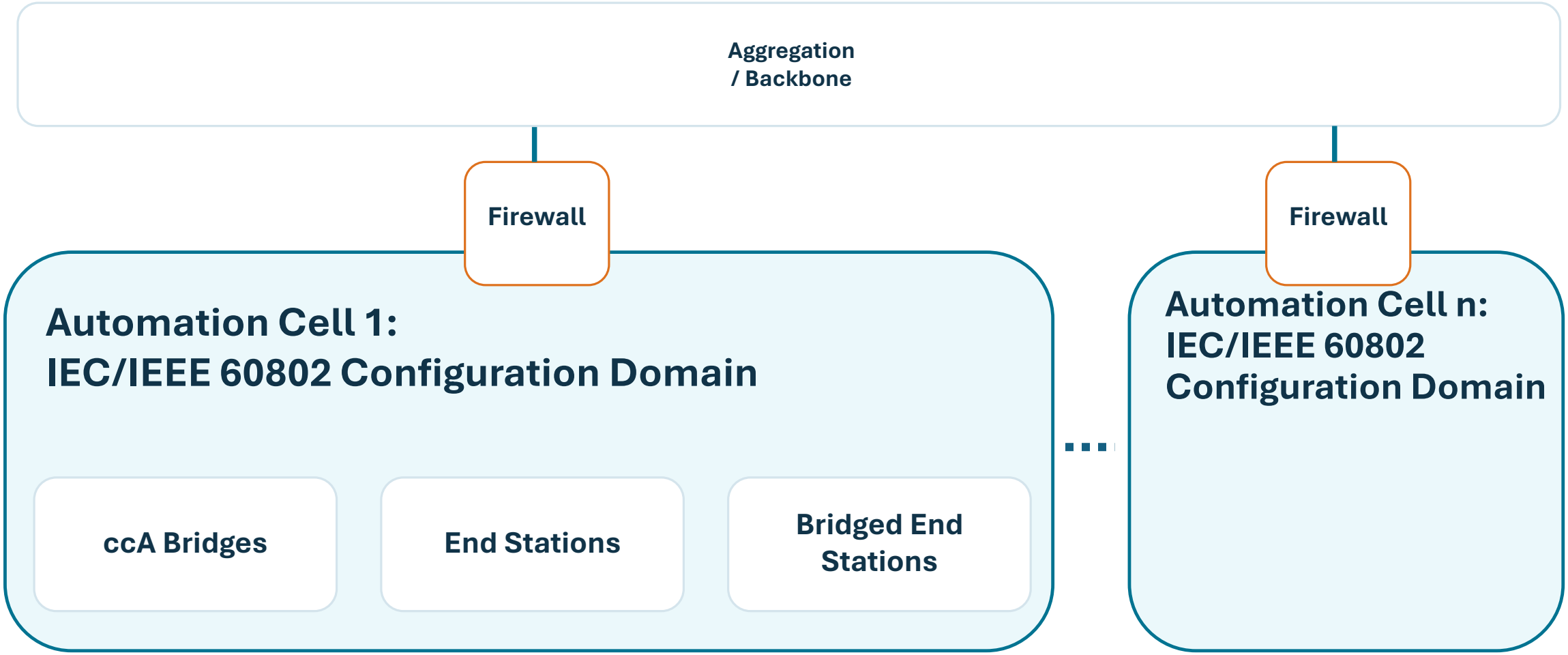
Seamless Redundancy in IEC/IEEE 60802 Configuration Domains

Architectural Requirements, Design Principles, and Constraints

V02

Günter Steindl (SIEMENS AG)

Plant automation is structured into automation cells



Customer Requirements

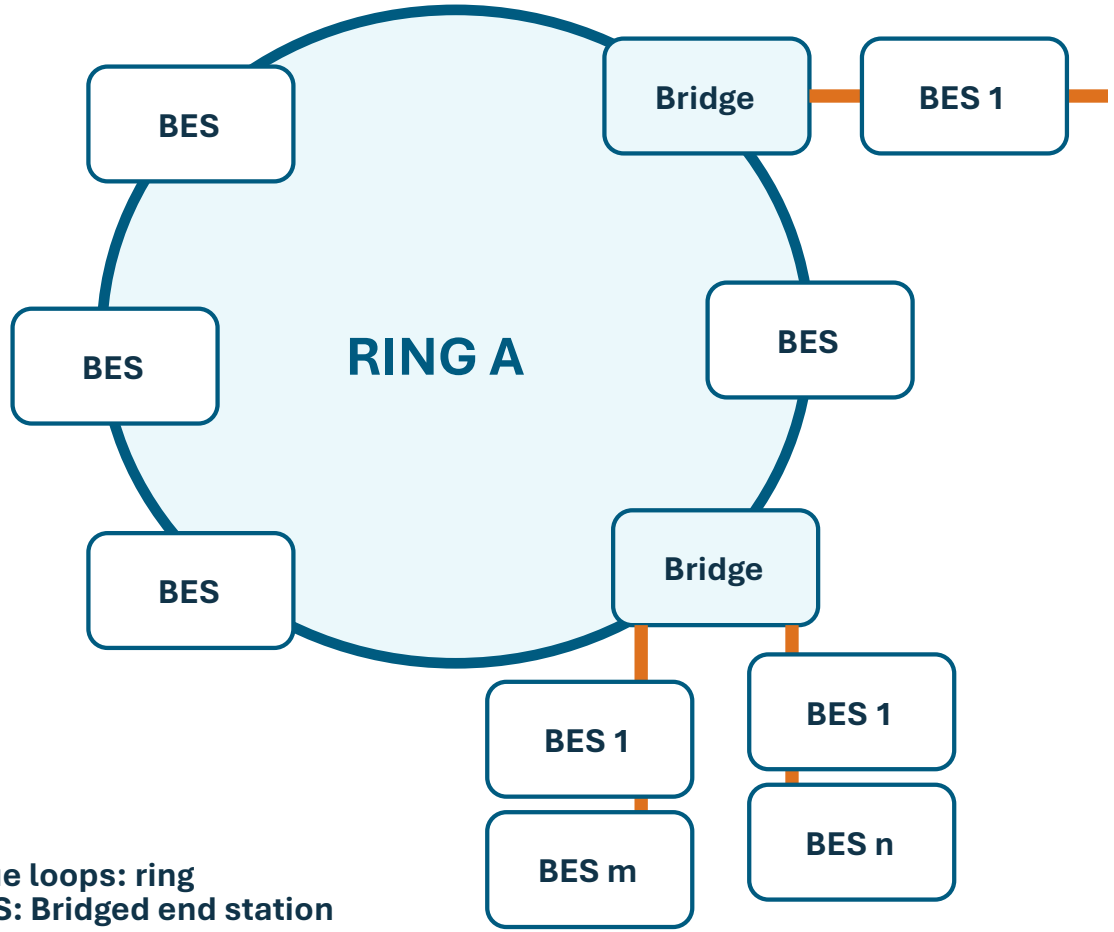
Protect any application traffic within the designated protection scope of the Configuration Domain

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

Support concurrent operation with other network functions

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

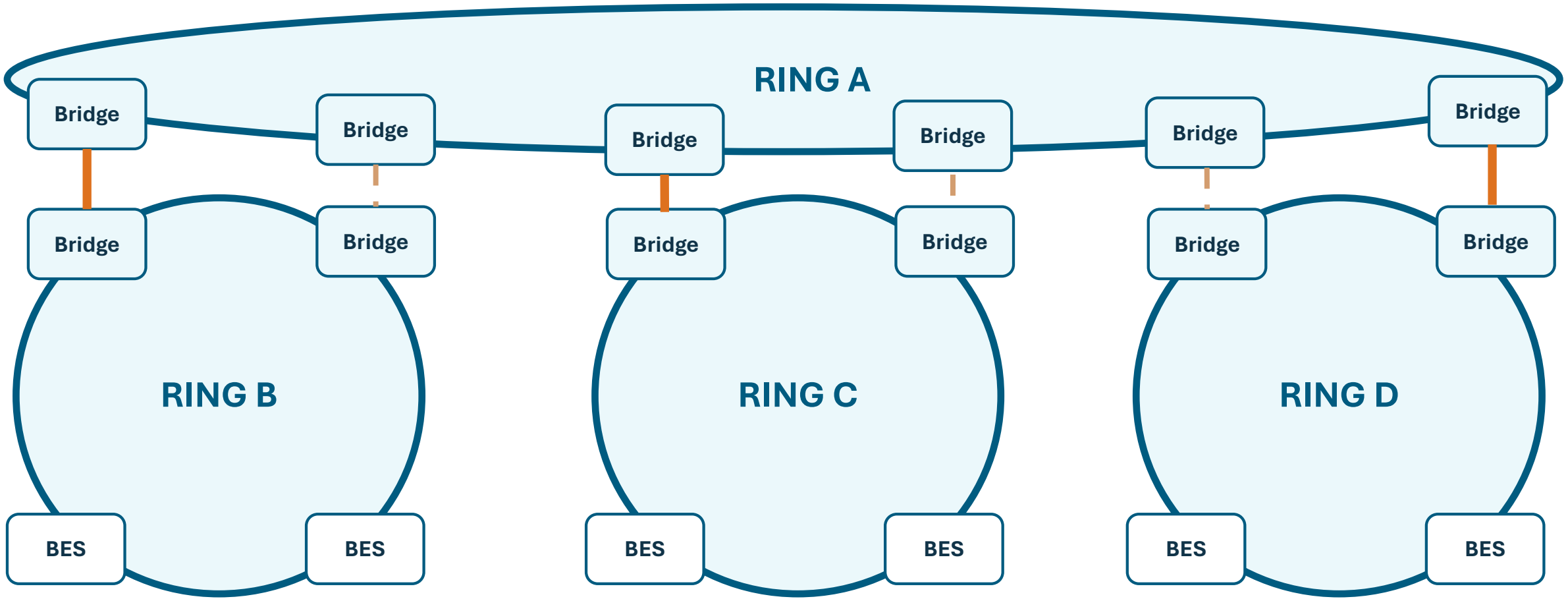
Bridged end stations and topologies



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

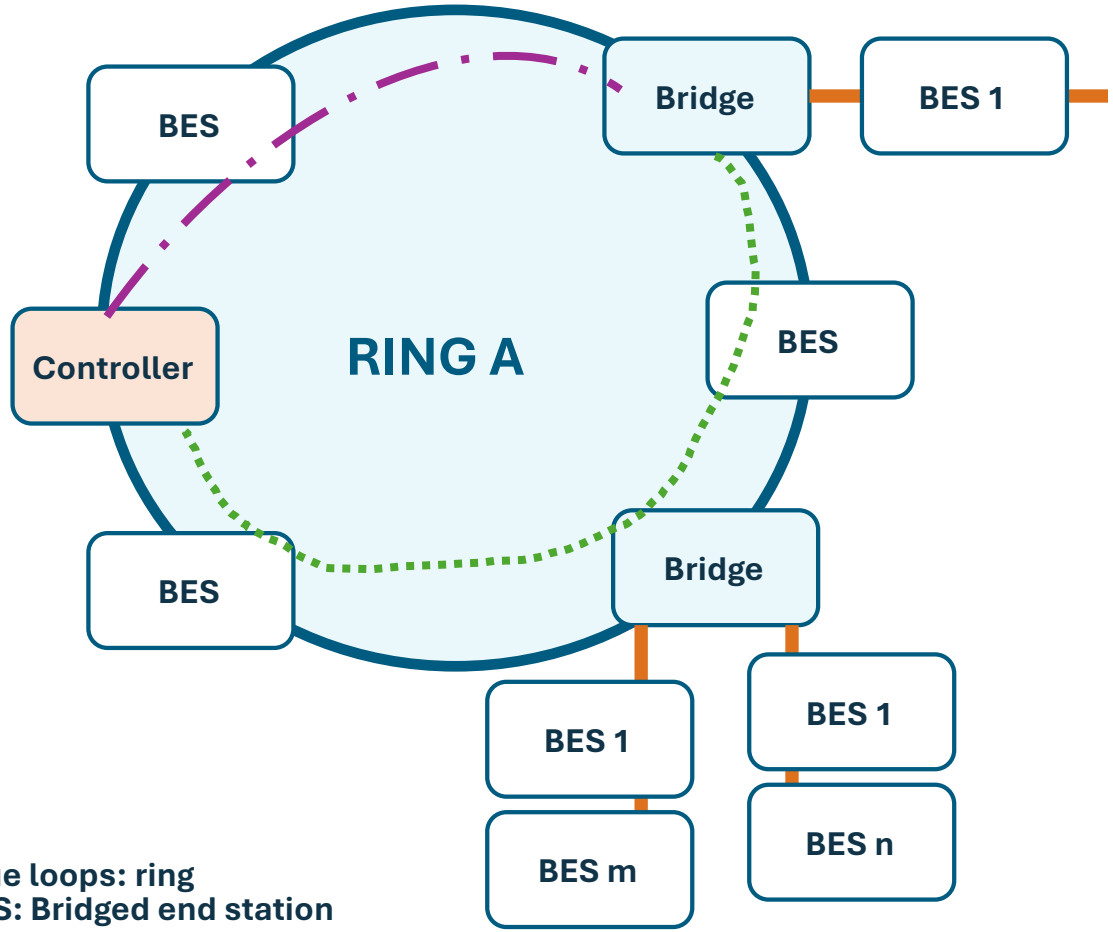
Maximum hops due to synchronization

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

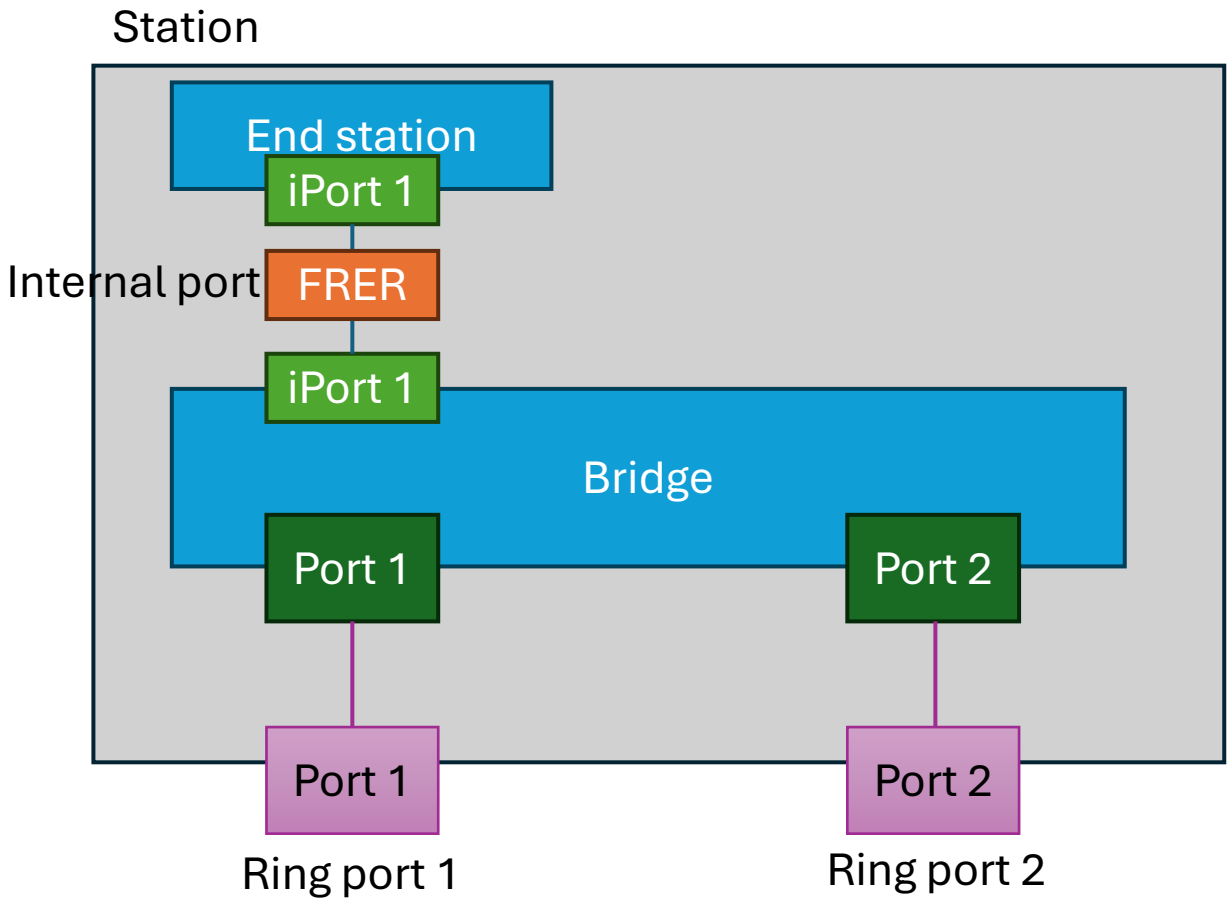
- Automation cells form and change during operation
- AGVs and modular production dynamically change the topology
- Static communication paths cannot be assumed
- Offline traffic engineering is not feasible
- Seamless redundancy shall not depend on pre-engineered paths or schedules

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

Examples

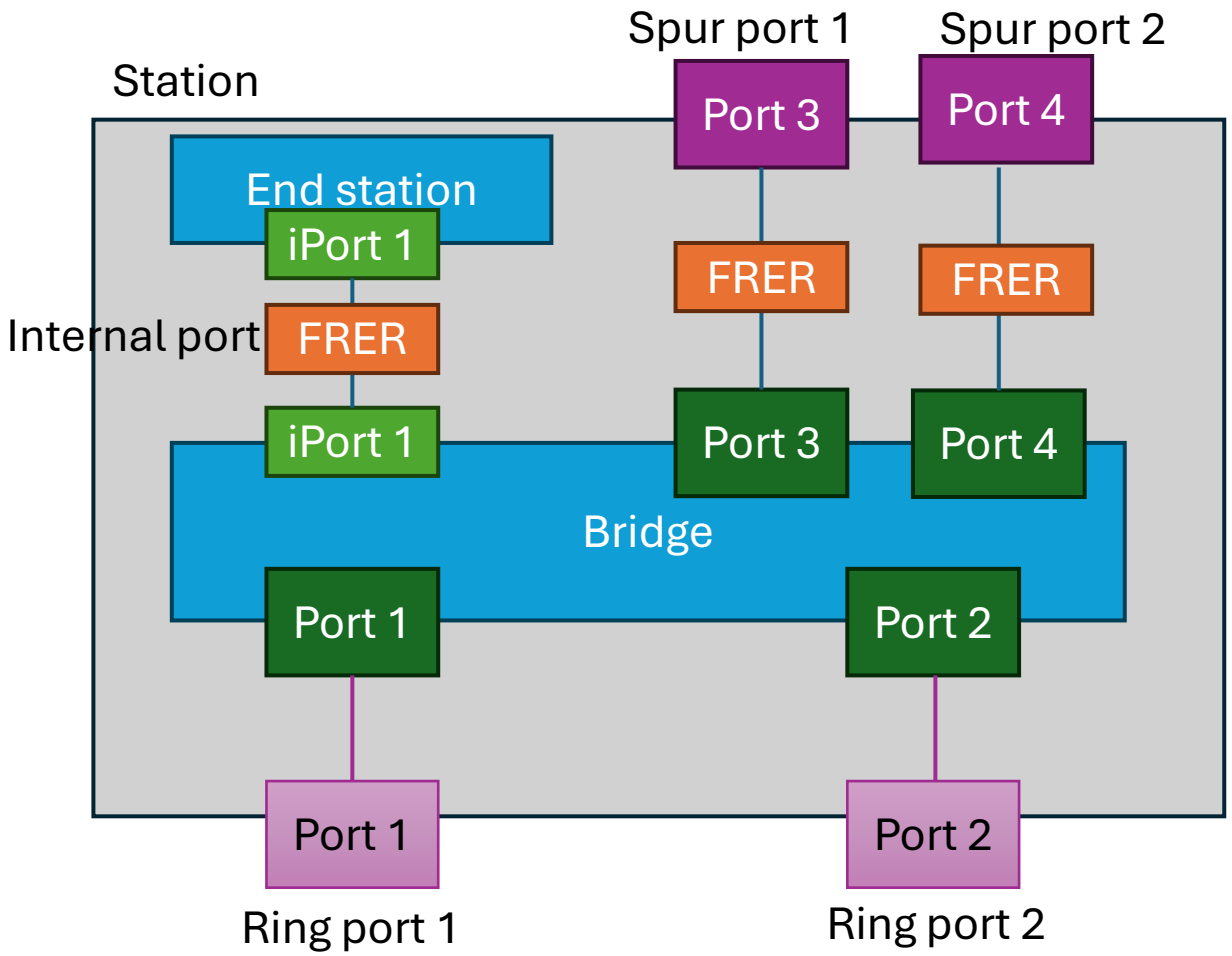
FRER usage examples

Example 1
FRER entity inside Bridge



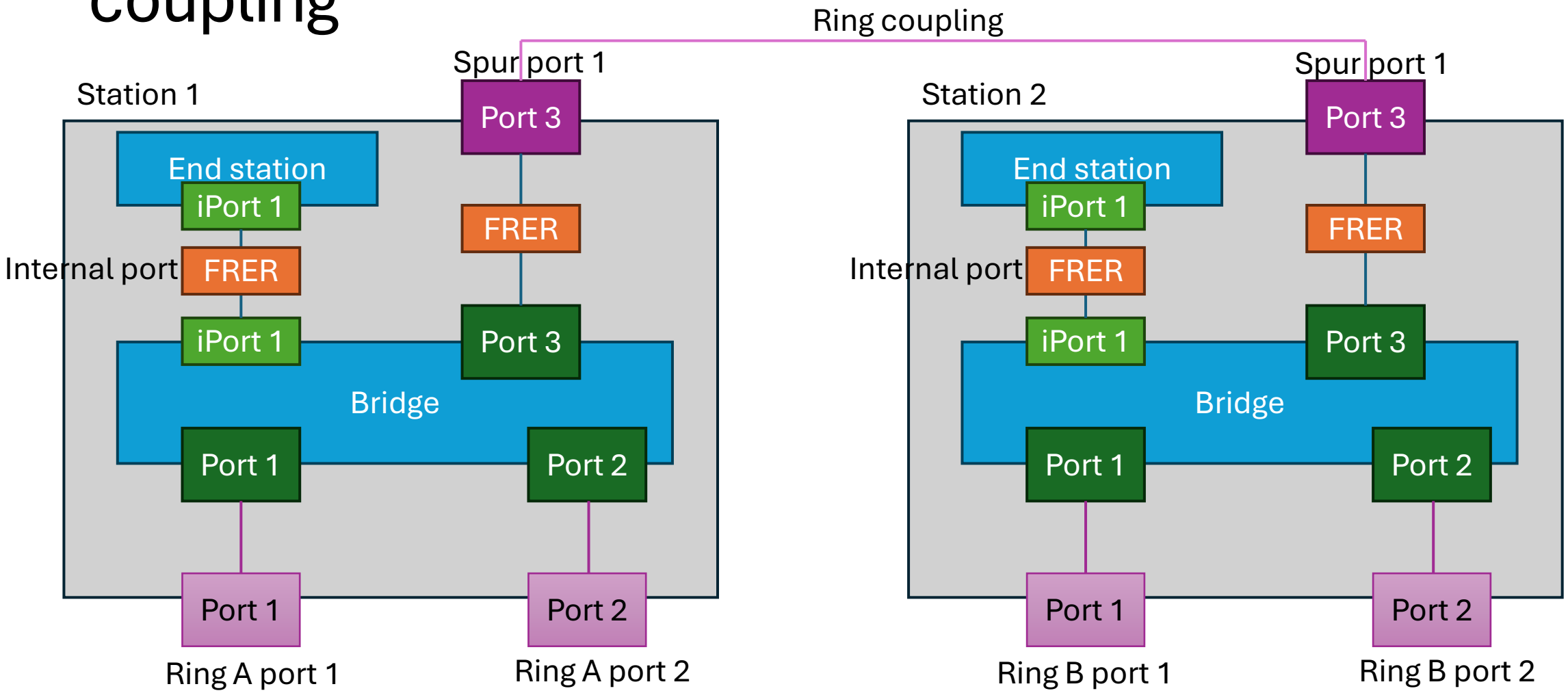
- Replication an elimination is done at the FRER stage
- Stream identification may be based on SA, DA, VID (and PCP)
- Forwarding of the replicated frames is done by the bridge
- Enabling of FRER is an engineered decision

Example 2
FRER entity inside Bridge with spurs



- Replication an elimination is done at the FRER stage
- Stream identification may be based on SA, DA, VID (and PCP)
- Forwarding of the replicated frames is done by the bridge
- Spur and internal port uses the same principle according FRER
- Ring, spur and internal ports are engineered ports
- Redundant couplings between rings may require another kind of port type

Example 3
FRER entity inside Bridge with spur used for ring coupling



Profiling FRER for Automation Cells

Protocol-independent FRER identification

- Identify every eligible data frame “presented to FRER” through the applicable 802.1AC MAC Service interface — including unicast, unknown unicast, multicast and broadcast — without a rule for each EtherType, application or communicating pair.
  - Provide a fitting stream identification function, e.g. per DA, SA, VID and PCP tuple
- Distinguish independent sequence generators even when their frames have the same destination address and VLAN.
  - Sequence Recovery Functions should support streams identified by a DA, SA, VID and PCP tuple
- Establish and retire the required identification state as sources appear or disappear; do not require a manually configured FRER entry for each source.
  - Any new stream shall be handled by FRER, e.g. at a spur or internal port, automatically

Recovery behavior and management

- Define safe initialization, reset and aging of generation/recovery state when a source appears, moves, restarts or becomes inactive.
  - Any new stream shall be handled by FRER, e.g. at a spur or internal port, automatically
- Specify recovery behavior as a function of “concurrent sequence contexts”, peak frames and bursts “per context”, and maximum differential arrival time. Test reordering, sequence wrap and reset.
  - Behavior in case of missing resources, e.g. available Sequence Recovery Functions
- Expose configured limits, active contexts and recovery/duplicate counters through a YANG model consistent with 802.1CBcv.
  - Specify managed objects for supported number of Sequence Recovery Functions, History Length and Burst/Rate as a consistent set

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.
- FRER shall support one such failure per ring concurrently in multiple rings.
- Failures of spur links, including non-redundant inter-ring couplings, are excluded.
- Where redundant inter-ring coupling is provided, the failure of one coupling link shall be tolerated.

- NOTE - 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.
  - Provide a fitting stream identification function

- It shall not interfere with the independent redundancy and failover mechanisms of per-port protocols, including IEEE 802.1AS hot-standby time synchronization.

Bibliography

- IEC 62439-3:2021, Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)

- IEC 62439-3, Edition 5.0 (under development), Industrial communication networks – High availability automation networks – Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR)

Questions?

Thank you!