IEC/IEEE 60802

Boundary Ports and gPTP

Boundary Port Isolation
Requirements and assigned features

(Draft IEC/IEEE 60802 D1.3 already contains the port isolation use case)

Version V01 – March 2022

Günter Steindl (Siemens AG)

Recap:
Automation systems supporting Plug & Produce

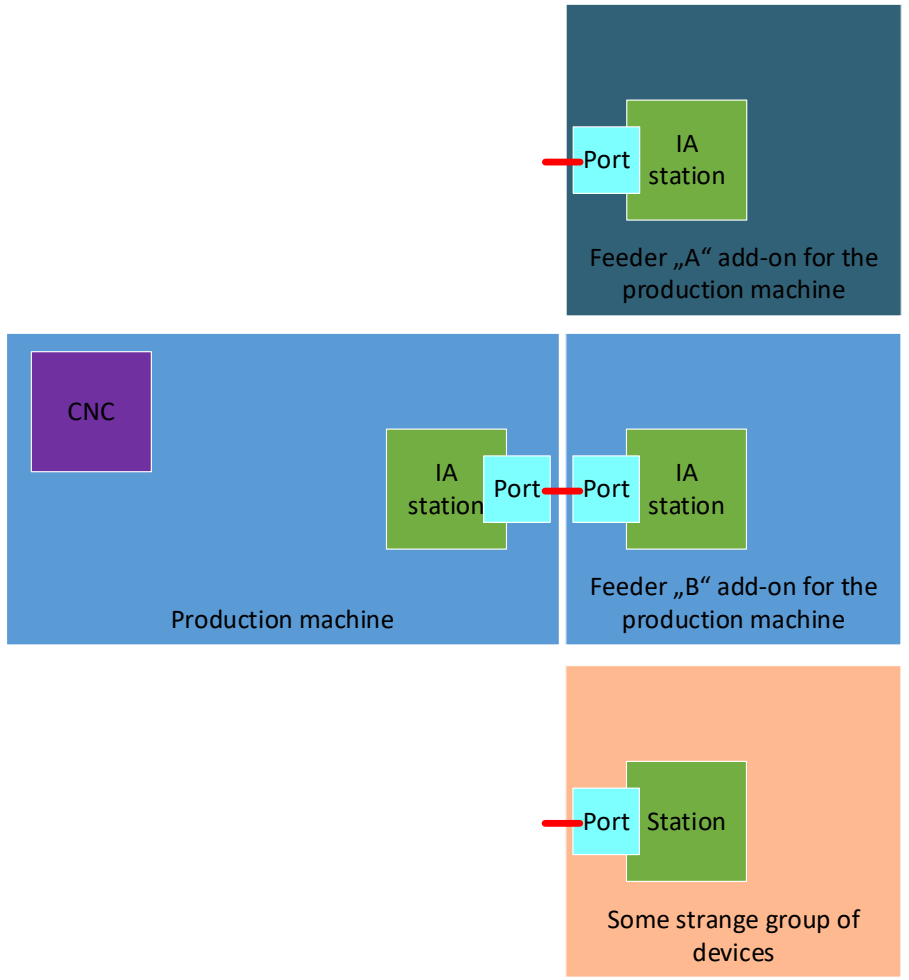
Machines are designed in a module based manner. Thus, the customer can use the base machine or the extended versions whenever needed.

In the rush of production, wrong connections happens.

Making a wrong connection shall not disturb the production machine.

Thus, any unintended use of network resource of the production machine shall be avoided.

How can we achieved this goal?



Boundary Port Isolation

How can we avoid any unintended use of network resource of the production machine?

Remote management model:

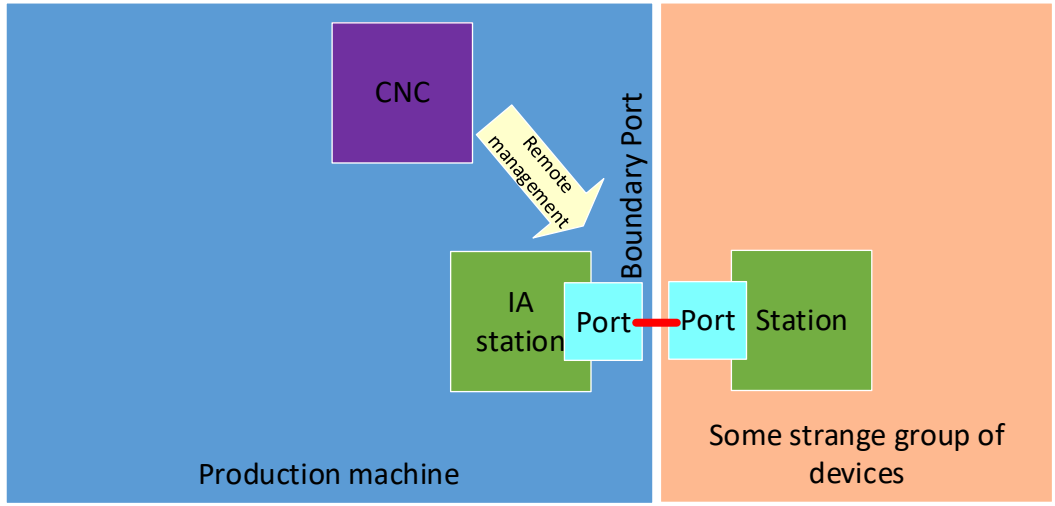
TDE / NPE entities of the CNC monitor the topology and can configure the setting at the boundary port depending on its neighborhood.

Scanning approach:

TDE scans a TSN domain with up to 1000 stations. How long will it take before the TDE discovers a change in neighborhood?

Subscription approach:

TDE uses Netconf push/Netconf subscription “on data change” to observe the port states. Any change will be indicated to the TDE and the NPE can react and change the configuration for the port to protect the network resources of the production machine.



Boundary Port Isolation Timespan

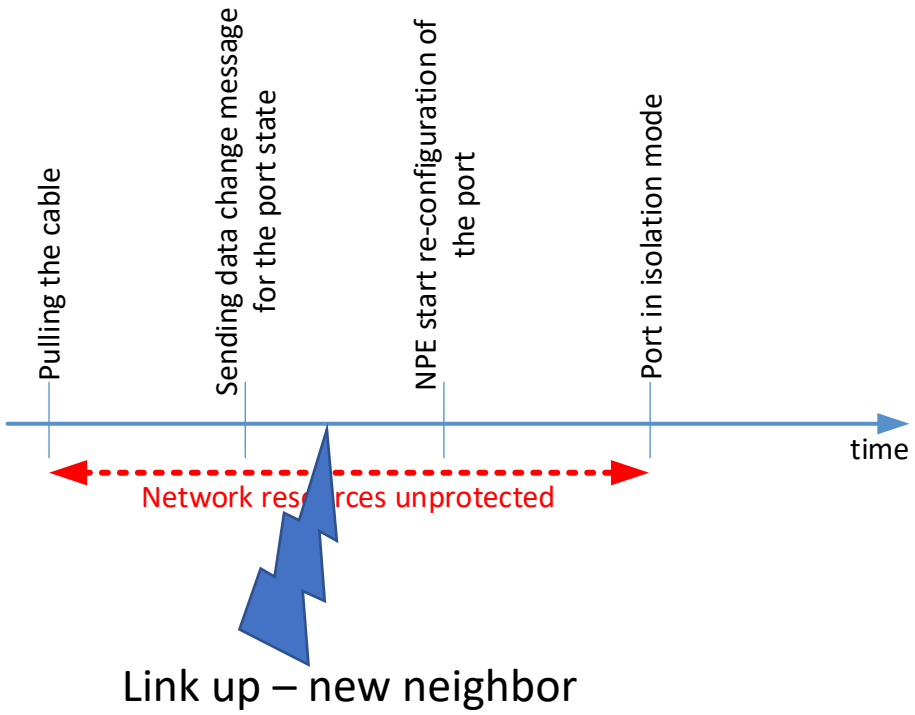
Can the subscription approach solve the problem?

The subscription approach also leaves a time gap between pulling the cable and completing the reconfiguration of the port.

How long this timespan will be is hard to state. Performance of the station, performance of the CNC, message queue size, … are influencing factors.

Thus, it seems that even the subscription approach isn't good enough.

But how can this problem be solved?



Boundary Port Isolation Protocol entity

How can we avoid any unintended use of network resource of the production machine?

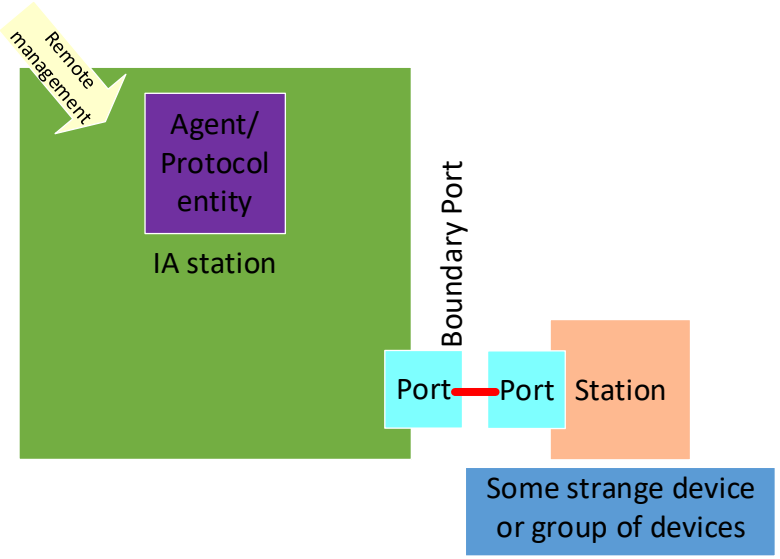
This problem can be solved by an agent/Protocol entity “sitting” in the station itself.

This agent, if active, would switch the configuration of a port into an to be defined isolation mode.

Any change of the local port state due to a new link can be delayed until the isolation mode is reached.

Remote management is used to release the isolation mode if applicable.

Now is no longer any dependency on the Netconf performance for the resource protection.



This basic principle of an agent/Protocol entity is for example used in IEEE802.1X to avoid an unprotected timespan.

gPTP

Boundary Port Isolation gPTP

gPTP is just another protocol from boundary port point of view.

Case link down:

CNC configure port for isolation mode

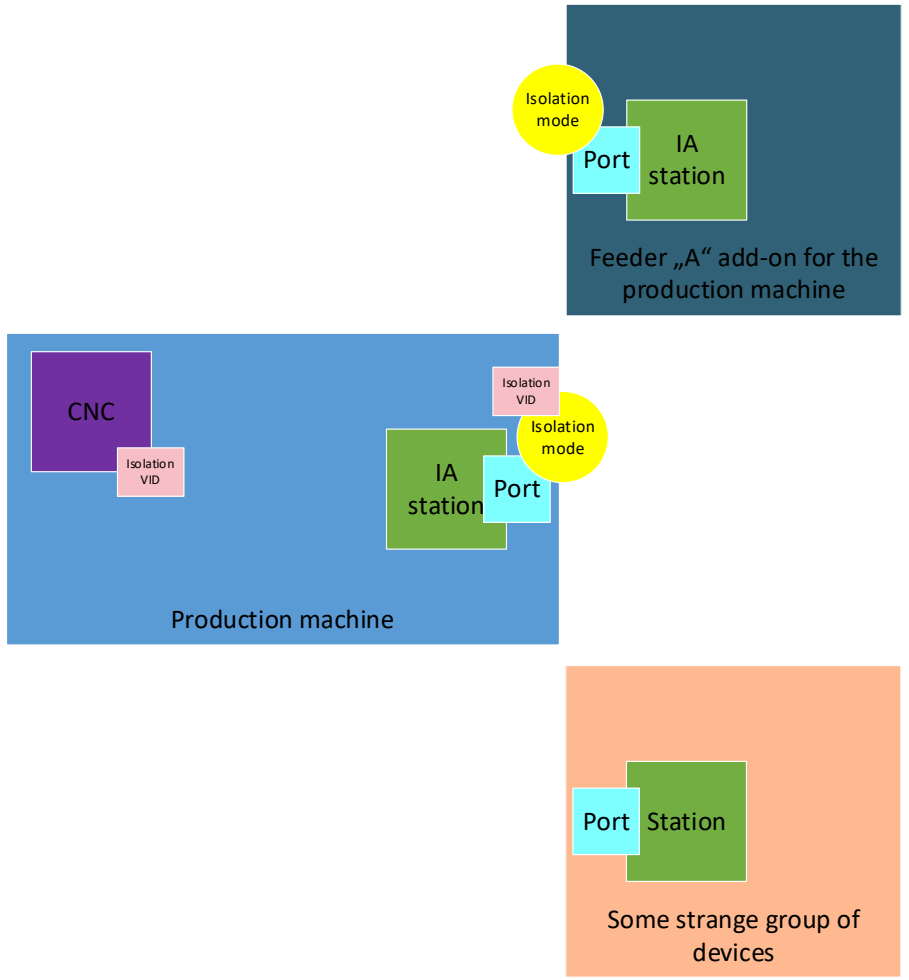
- gPTP doesn't sent sync or announce frames
- gPTP doesn't receive sync or announce frames

Case link up:

CNC checks whether isolation mode can be replaced by TSN domain internal mode

- gPTP configuration will be applied

=> Add station / remove station doesn't require a default gPTP setting at the added IA-station



Add station / remove station

Boundary Port Isolation
Add station / remove station

Add station and remove station (plug or pull a cable from a port) are cases in which link up or link down is detected.

Case link down:

CNC configure port for isolation mode

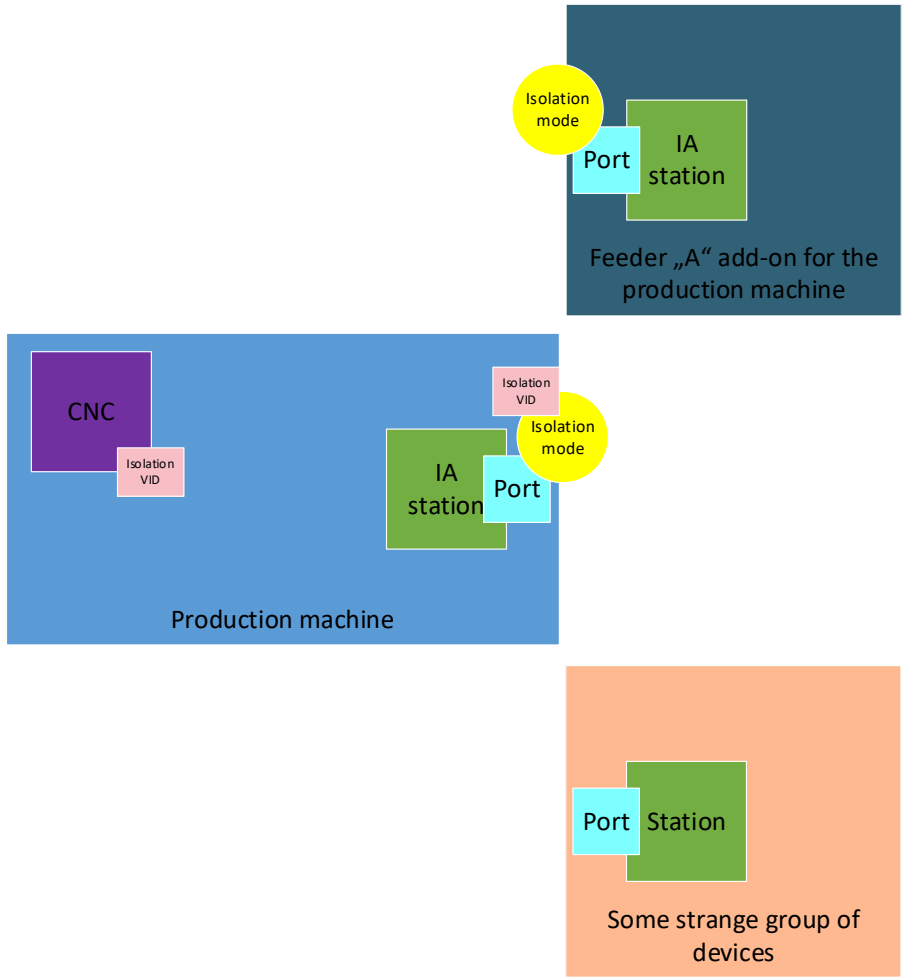
➢ Remove station

Case link up:

CNC checks whether isolation mode can be replaced by TSN domain internal mode

➢ Add station

=> Add station / remove station doesn't require a default setting at the added IA-station



Possible solution

Boundary Port Isolation

Any open port of a TSN Domain enters the isolation mode, as soon as the port state enters link-down.

Isolation mode means, that

- productive VIDs: this port in no longer part of the active topology
- isolation VID: this port is part of the active topology
- virtual port: all LLC frames are isolated, too

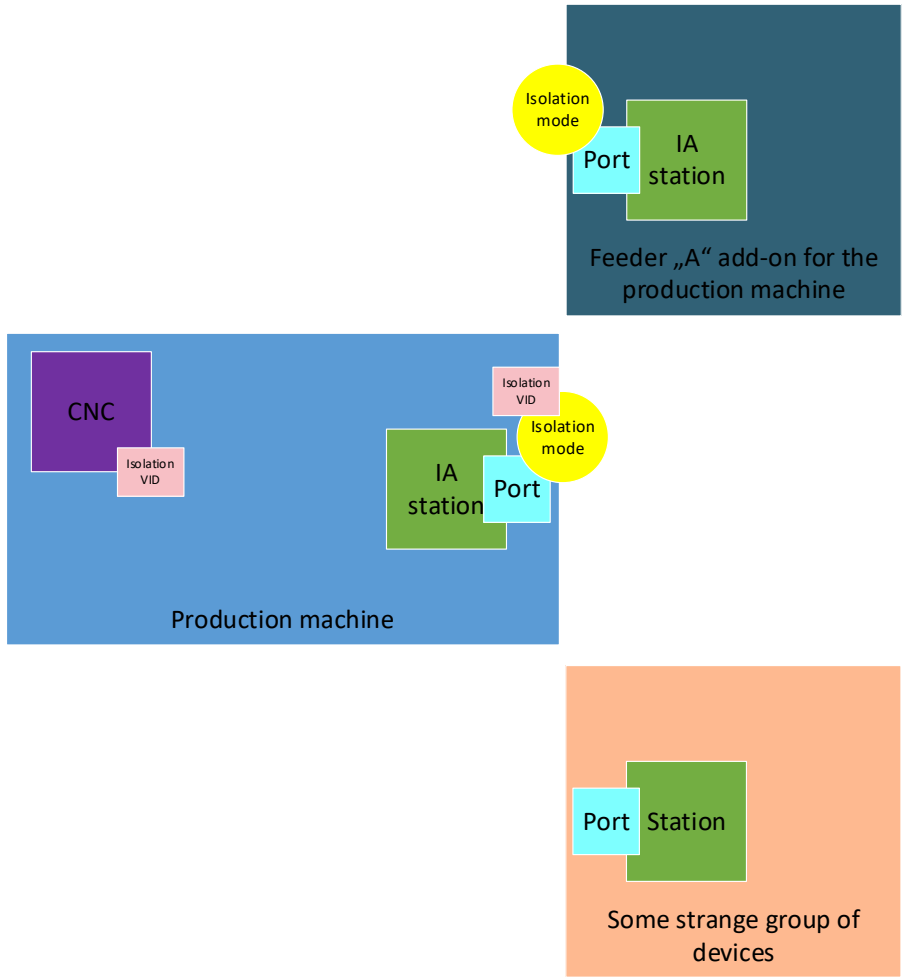
CNC / TDE gets a notification if the port state is changing and use remote management to access the station with boundary port.

It uses information received from this station to access the neighbor station using the isolation VID and address information provided by the station with boundary port.

The VLAN translation table on the boundary port in isolation mode is setup in a way that it assigns the isolation VID to any to be received non-LLC frames and strips the VLAN-TAG from any frame transmitted.

An established Netconf-over-TLS connection between CNC and neighbor station allow checking of the station.

CNC decides based on the outcome of this checking whether it configures the neighbor station and releases the isolation mode.



Fast Startup

Startup of a machine needs to be as fast as today. Thus, the two stage “release model” which includes the CNC is not fast enough.

An solution which can be handled by the stations itself is needed.

LLC protocol entity

A protocol entity using EAPOL or EAP-TLS to exchange some stored identifiers could be used to solve this problem.

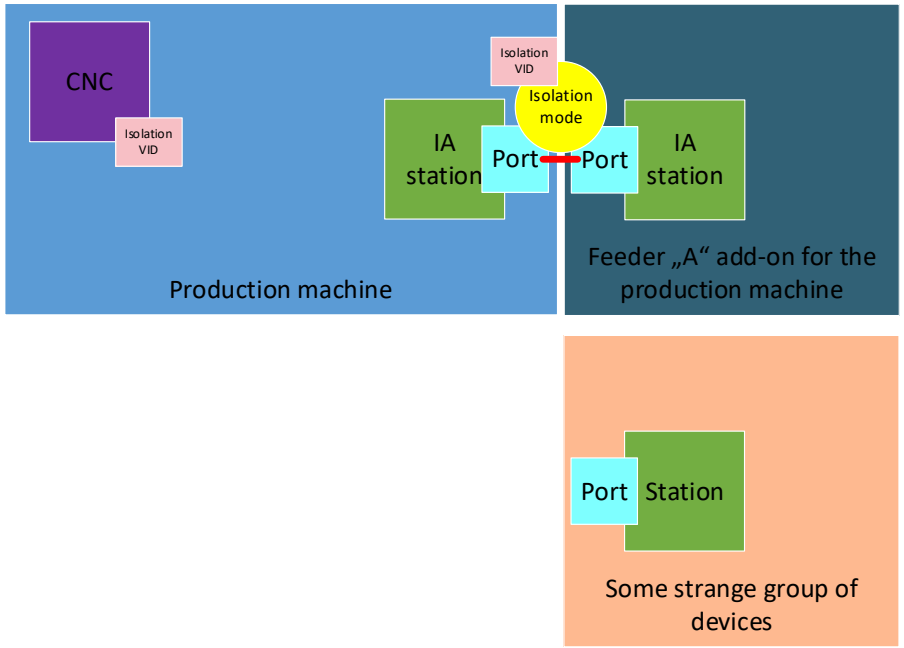
That’s very similar to use LLDP – but with adding Secure Device Identity…

Checking the exchanged identifiers allows the protocol entity to release the isolation mode without CNC support.

Netconf-over-TLS

IP address issues; runtime issues; isolation VID; isolation mode…

LLC protocol entity seems to suit better to solve the problem.



Conclusion

Conclusion

Protecting the network resource of a TSN domain requires a fitting configuration of the boundary ports.

Any port of a station of a TSN domain can be at some time a boundary port due to the modular machine / dynamic machine setup principle.

Remote management can not guarantee the “fitting configuration” at any time.

A protocol entity residing in the stations can avoid unprotected timespans.

- Shall IEC/IEEE60802 directly move to IEEE 802.1X for port isolation?
  - Lets aim for it in version 2 of the TSN-IA profile
- Does IEEE 802.1X fit for “connecting machine parts”?
  - If not, a new project may be needed

Questions ?