NETCONF-over-TLS 1.3

Kai Fischer, Andreas Furch, Oliver Pfaff – Siemens AG

Problem Statement

- IEC/IEEE 60802 D2.0 supports NETCONF-over-TLS 1.2 based on IETF RFC 7589
- The NETCONF WG in the IETF elaborates a support of NETCONF-over-TLS 1.3, see https://datatracker.ietf.org/doc/draft-ietf-netconf-over-tls13/
- The latest WG draft 02 (2023-03-10) supports NETCONF-over-TLS 1.2 and NETCONF-over-TLS 1.3. This work item aims at updating IETF RFC 7589
- IEC/IEEE 60802 needs to consider when and how to add NETCONF-over-TLS 1.3 – without creating unwanted risks for the publication schedule of IEC/IEEE 60802
- Important: TLS 1.3 is a full redesign of TLS 1.2 → adopting NETCONF-over-TLS 1.3 requires more than editorial changes; additions to the IEC/IEEE 60802 text body are needed to reflect the design changes between TLS 1.2 and 1.3

Proposal

- Step 1 (editor): create a document update that covers the D2.0 comment resolution and normative wording changes for security
- Step 2 (security contributors): use the step 1 document to provide an update that identifies the text changes for an adoption of NETCONF-over-TLS 1.3 (in addition to NETCONF-over-TLS 1.2)
- Step 3 (working group): use the step 2 update to determine a timeline for an adoption of NETCONF-over-TLS 1.3 (in addition to NETCONF-over-TLS 1.2)

Caveats

- For the time being NETCONF-over-TLS 1.3 is documented on the level of an IETF WG draft (https://datatracker.ietf.org/doc/draft-ietf-netconf-over-tls13/). When this draft will become an IETF RFC document is hard to predict.