Brainstorming on IEC/IEEE 60802 Edition 2:

Review of potential security use cases for a potential amendment to IEC/IEEE 60802

David McCall (Intel Corporation)

Dieter Proell (Siemens AG)

Review of "Security Use Cases IEC/IEEE 60802 v0.1", contribution to IEC/IEEE 60802 by Kai Fischer, Andreas Furch, Oliver Pfaff, Thomas Pössler & Günter Steindl. April 2021.

v02 updated following group discussion on Monday 1st December 2025

Use Case Num	Use Case Name	Met in 60802?	Notes
1	Checking the equipment under control	YES	See Clause 4.8.6 in 60802. The foundations laid to meet this use case (e.g. IDevID) can be used to secure other traffic (e.g Timesync; LLDP)
2	Imprinting during bootstrapping/commissioning	Partial	Use case for Taking Posession covered in detail (trust on first use model). 60802 currently doesn't elaborate on Device Replacement or Modular Machine Assembly, both of which would probably use a lot of what was defined for Taking Possession but were regarded as out of scope for 1st Edition
3	Instructing equipment about security	Partial	Covered in detail for Configuration (NETCONF), but not for LLDP or Time Sync (all Control Plane). Data plane security is regarded as out of scope for 60802; handled via automation protocol (which may choose to leverage some aspects of Use Case 2).
4	Peer entity authentication	YES	Similar to Use Case 2. First check manufacture credentials and than operator credentials.
5	Message exchange protection	Partial	Covered in detail for Configuration (NETCONF), but not for LLDP or Time Sync (all Control Plane). Data plane security is regarded as out of scope for 60802; handled via automation protocol (which may choose to leverage some aspects of Use Case 2).
6	Proving self-asserted information	NO	Very broad. Not covered by 1st Edition. Carry forward for discussion of potential scope. Some aspects may be of interest.
7	Resource access authorization	YES	Yes for Configuration. (See Use Cases 3 and 5.)
8	Credential/key update during operation	NO	Not elaborated on in Edition 1. Left up to the operator. Out of scope for 60802 1st Edition as Configuration security does not require bumpless management. May need to change for 2nd Edition if we start to secure more types of control plane data.
9	Credential/key revocation/invalidation during operation	NO	

Use Case Num	Use Case Name	Met in 60802?	Notes
10	Crypto algorithm-expiry/agility	Partial	One cipher suite is mandatory, may not the best, but okay. Some further (and better) are optional. Interesting for future, Quantum computers forces the need for better cipher suites. Carry forward to potential Edition 2 use cases for discussion.
11	Robust supply of security core function	NO	Out of scope, but 60802 does rely on robust supply of security core functions. Don't need details, but may be good to add some references on how to do it (e.g. IEC 62443). Carry forward for that reason.

Questions, Discussion, …

Thank you