Problem Statement

- Provide a **deep-dive** for **NETCONF security** (*as-is*) from the perspective of industrial automation esp. IA devices/controllers
- Report the **fitness** of NETCONF security for **industrial automation**
- Use **specification documents** for this analysis (implementations are not considered herein)
- See the accompanying overview slide-deck for the **abstractions/terms** etc. considered herein

**Note**: deep-dives (according the same scheme) will be made for all short-listed candidates
# Fitness of As-Is NETCONF Security for Industrial Automation

<table>
<thead>
<tr>
<th>Security fulfilment disciplines*</th>
<th>Message exchange protection</th>
<th>Resource access authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect shared resources on IA devices/controllers</td>
<td><strong>Assessment</strong>: covered (NETCONF-over-TLS or SSH) but has many options and is not yet profiled for industrial automation</td>
<td><strong>Assessment</strong>: addressed with respect to DAC (NACM) but not yet incarnated for industrial automation</td>
</tr>
<tr>
<td>Establish security associations with endpoints on IA devices/controllers</td>
<td><strong>Action item</strong>: <strong>profiling</strong> for IEC/IEEE 60802</td>
<td><strong>Action item</strong>: <strong>profiling</strong> for IEC/IEEE 60802</td>
</tr>
<tr>
<td>Manage initial credentials and overall security configuration at IA devices/controllers</td>
<td><strong>Assessment</strong>: addressed (SZTP) but comes with many specifics and has white spots</td>
<td><strong>Assessment</strong>: NACM comes with a chicken-and-egg problem which is not elaborated in NACM RFCs</td>
</tr>
</tbody>
</table>

* should wait for other deep-dive results
** can be started without waiting for other deep-dive results
*** should wait for other deep-dive results

*: see background slide for details
Profiling Action Items Include

• **Security for shared resources:**
  • Message exchange protection:
    • Select TLS and/or SSH
    • Profile scheme-specific details e.g. version of security protocols, handling of optional features…
  • Resource access authorization (NACM - if DAC is the preferred model):
    • Model authorization-controlled resources and actions
    • Assign NETCONF ‘users’ to groups

• **Shared security means:** compile a catalogue of cryptographic algorithms

• **Securing-the-security:**
  • Select SZTP with and/or without ‘call home’ feature (RFC 8071, RFC 8366)
  • Profile SZTP-specific sources and details of bootstrapping data e.g. sources of bootstrapping data, nonceless vouchers, revocation means
  • Select supported ‘user’ population: implicit (mapping from TLS/SSH), local and/or remote repositories
Action Items Possibly Beyond Profiling Include

- **Security for shared resources:**
  - Message exchange protection: n.a.
  - Resource access authorization: reconfirm authorization model DAC vs. MAC/ABAC/RBAC…

- **Shared security means:** n.a.

- **Securing-the-security:**
  - Supply of own (private keys and) EE certificates to NETCONF servers
  - SZTP bootstrapping/credentialing of network components without any initial credentials
  - Supply credentials/trust anchors to NETCONF clients
  - Push support for credential/trust anchor management
  - Elaborate the assignment/management/identification of the NACM root-of-authority
  - Cover equipment originality checks
  - Enforce overall security configuration, e.g. allow only protected access
NETCONF Security Mind-Map

- Copy the markdown source from the grey text field on the left (don't worry about the tiny font size)
- Paste this text into an interpreter e.g. https://markmap.js.org/repl
- Adjust the page zoom and browse the shown mind-map
- This map provides the NETCONF security essentials
Next Steps

1. Kicking-off - Done

2. Establish goals and constraints, agree on use cases (automation and security-specific)

3. Perform deep-dives for the security technology candidates
   i. NETCONF security – Largely done
   ii. SNMP security
   iii. DNS security
   iv. 802.1AE/X/AR
   v. 802.1AS security
   vi. NN, decide about items from the longlist

4. Identify cross-relation/common interests with middleware/application-specific security
   • Shortlist: security for IEC 61158 technologies, OPC-UA security, Web security…

5. Create the blueprint of an overarching security architecture (more details are tbd)
## Abbreviations*

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABAC</td>
<td>Attribute-Based Access Control</td>
</tr>
<tr>
<td>DASA</td>
<td>Delegated Authorized Signing Authority</td>
</tr>
<tr>
<td>MAC</td>
<td>Mandatory Access Control</td>
</tr>
<tr>
<td>MASA</td>
<td>Manufacturer Authorized Signing Authority</td>
</tr>
<tr>
<td>NACM</td>
<td>NETCONF Access Control Model</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-Based Access Control</td>
</tr>
<tr>
<td>SZTP</td>
<td>Secure Zero Touch Provisioning</td>
</tr>
<tr>
<td>XACML</td>
<td>eXtensible Access Control Markup Language</td>
</tr>
</tbody>
</table>

* see the accompanying overview slide-deck for further abbreviations
References, Chronologically Ordered

2. IETF RFC 4742: Using the NETCONF Protocol over Secure Shell (SSH), 2006
3. IETF RFC 5539: NETCONF over Transport Layer Security (TLS), 2009
4. IETF RFC 6187: X.509v3 Certificates for Secure Shell Authentication, 2011
5. IETF RFC 6241: Network Configuration Protocol (NETCONF), 2011
6. IETF RFC 6242: Using the NETCONF Protocol over Secure Shell (SSH), 2011
9. IETF RFC 8071: NETCONF Call Home and RESTCONF Call Home, 2017
10. IETF RFC 8341: Network Configuration Access Control Model, 2018
11. IETF RFC 8366: A Voucher Artifact for Bootstrapping Protocols, 2018
12. IETF RFC 8572: Secure Zero Touch Provisioning (SZTP), 2019
Authors

Kai Fischer, Siemens AG, T RDA CST SES-DE,
kai.fischer@siemens.com

Andreas Furch, Siemens AG, T RDA CST SES-DE,
andreas.furch@siemens.com

Lars Lindemann, Siemens AG, DI FA CTR ICO ARC,
lars.Lindemann@siemens.com

Oliver Pfaff, Siemens AG, T RDA CST,
oliver.pfaff@siemens.com

Thomas Pössler, Siemens AG, RC-AT DI FA DH-GRAZ SAS,
thomas.poessler@siemens.com

Günter Steindl, Siemens AG, DI FA TI ART EA,
guenter.steindl@siemens.com
## Security Fulfilment Disciplines Explained

<table>
<thead>
<tr>
<th>Security fulfilment disciplines</th>
<th>Meaning</th>
<th>Example for Web security*</th>
</tr>
</thead>
</table>
| Protect shared resources on IA devices/controllers                   | Exercise **message exchange protection** and **resource access authorization** for shared resources on IA devices/controllers | *Message exchange protection*: send HTTP requests/responses with TLS record layer protection  
*Resource access authorization*: enforce write/read access control to specific folders (paths) etc. |
| Establish security associations with endpoints on IA devices/controllers | Establish **(authenticated) keys** and further security settings **between communicating partners** | Prepare the TLS record layer(s) for operation by doing a TLS handshake                   |
| Manage initial credentials and overall security configuration at IA devices/controllers | Supply **(initial) credential/trust anchor(s)** to a **dedicate entity** | Prepare the TLS handshake layer(s) for operation by supplying credentials, trust anchors and other security configuration e.g. cipher suite preferences |

*: not actually part of the shared resources but used for illustration - as Web security is familiar to all
Authorization Management Pattern: NACM

- **NACM pattern**: authorization management and authorization controlled operations *use* the *same channel*

- **Default pattern in IT**: authorization management and authorization controlled operations *use different channels*
Bootstrapping Pattern: SZTP

- **1 main event:** booting in **factory-default state**
- **2 main actors:** network device, SZTP bootstrap server (alternatives: removable storage, DNS/DHCP)
- **2 main security strategies:** `deprotect_with_current` or `subsequent` (an indirection → uses vouchers)
- **4 main supplies:** {redirection or onboarding} and opt. {**owner certificate and ownership voucher**}

**Diagram:**

- **1a (2a…) Bootstrap request**
- **1b (2b…) Voucher request**
- **1c (2c…) Voucher response (alternative: pre-coined, nonceless vouchers)**
- **1d (2d…) Bootstrap response**

**Network device**

- **Redirection:** server host/port/trust anchor OR
- **Onboarding:** boot image, config, scripts AND (opt.)
- **Owner certificate:** signed EE certification path (3rd party) AND
- **Ownership voucher:** signed owner info, trust anchor