NACM based access control for IEC/IEEE 60802 resources

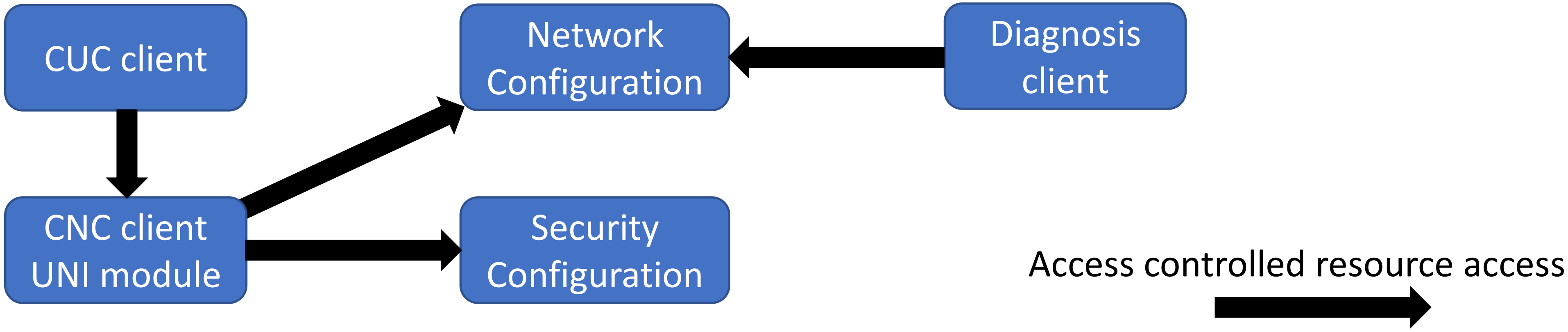
Kai Fischer, Andreas Furch, Oliver Pfaff – Siemens AG

Problem Statement

- Access control is mandatory for the resources of NETCONF/YANG servers (IETF RFC 6241 section 2.2)
- NACM (IETF RFC 8341) is the means to perform this access control
- NACM comes with syntactical and semantical structures that are to be respected when instantiating NACM-based access control to NETCONF/YANG resources
- The absence of a 60802-defined instantiation of NACM-based access control to NETCONF/YANG resources would:
  - Increase the overall workload: manufacturer and/or owner/operator would have to instantiate NACM for 60802 resources individually
  - Increase the risk for security breaches: shortcomings or errors in NACM instantiations can have severe consequences

Access Control Methodology

- Access control in general assigns rights on resources to subjects
- NACM-based access control in IEC/IEEE 60802
  - **Resources** are data nodes in YANG modules used by IEC/IEEE 60802
  - **Subjects** are CNC clients, CUC clients, diagnosis client
  - **Rights** are create, read, update, delete and execute (NACM uses the term write access as synonym for create, update and delete)



Access Control Model of IEC/IEEE 60802

- The IEC/IEEE 60802 access control mechanism is given by IETF RFC 8341 (NACM)
- IEC/IEEE 60802 resources are distinguished into security and non-security resources
- Subjects are assigned to roles that determine the access rights on IEC/IEEE 60802 resources
- Access rights of IEC/IEEE 60802 resources refer to the access control points
  - protocol operations
  - data stores
  - notifications

Scope

- NACM-based access control for IEC/IEEE 60802 YANG resources are defined in `ietf-netconf-acm`
- Already covered in IEC/IEEE 60802 D2.0 (security-related YANG modules)
  - `ietf-keystore`
  - `ietf-truststore`
  - `ietf-x509-cert-to-name`
- Now:
  - All other (non-security-related) YANG modules from IEC/IEEE 60802 D2.0 6.7.9
- Deferred to later:
  - `ietf-netconf-acm` (dynamically modifying the access control rules is postponed for complexity reasons)
- YANG modules not used in IEC/IEEE 60802 are out-of-scope

Basic Assumptions for an IA-station

- **Read access** to all IEC/IEEE 60802 YANG nodes is permitted for all authenticated subjects.
- **Create/update/delete (write) access** to any YANG node is only permitted for authenticated subjects when the access is explicitly permitted to the corresponding role (as detailed in the following slides).
- **RPC/action invocation** is only permitted for authenticated subjects when the access is explicitly permitted to the corresponding role (as detailed in the following slides).

Security-related 60802 Role Definition

- A CNC client configuring IEC/IEEE 60802 security resources may be assigned to a subset of roles from the following role catalogue (see also D2.0):
  - **TruststoreAdminRole** has write and execute access rights to YANG module **`ietf-truststore`**
  - **KeystoreAdminRole** has write and execute access rights to YANG module **`ietf-keystore`**
  - **UserMappingAdminRole** has write and execute access rights to YANG module **`ietf-x509-cert-to-name`** portion of **`ietf-netconf-server`**

Non-security-related 60802 Role Definition (1)

- A CNC client configuring IEC/IEEE 60802 non-security resources may be assigned to the following role:
  - **ConfiguratorRole** has write and execute access rights to **all YANG modules - except** those for
    - security configuration: `ietf-truststore`, `ietf-keystore`, `ietf-x509-cert-to-name` portion of `ietf-netconf-server`
    - stream configuration: `ieee802-dot1q-tsn-config`
    - subscription configuration: `ietf-subscribed-notifications` and `ietf-yang-push`

Non-security-related 60802 Role Definition (2)

- A CUC client for configuring IEC/IEEE 60802 non-security resources may be assigned to the following role:
  - **StreamConfiguratorRole** has write and execute access rights to **`ieee802-dot1q-tsn-config`**
- A diagnosis client for configuring IEC/IEEE 60802 non-security resources may be assigned to the following role:
  - **SubscriberRole** has write and execute access rights to subscribe for any notification in **`ietf-subscribed-notifications`** and **`ietf-yang-push`**

60802 Access Control for Protocol Operations

- <lock>, <unlock>: **permitted** for any IEC/IEEE 60802 defined role
- <partial-lock>, <partial-unlock>: not used in 60802 → **denied**
- <get> and <get-config>: **mapped to a "read" access operation** to the target datastore
- <edit-config>: **mapped to a particular access operation** to the target datastore
- <copy-config>: **permitted** for ConfiguratorRole
- <delete-config>: not used in 60802 → **denied**
- <commit>: **mapped to "create", "update", and "delete" access operation** to the target datastore
- <discard-changes>: **permitted** for any 60802 defined role
- <close-session>: **permitted** for any 60802 defined role
- <kill-session>: used in 60802? → **denied?**

Impact on IEC/IEEE 60802 Ed1

- *4.8.4 NETCONF/YANG access control*: Addition of some informative text for NACM
- *6.3.2.1.4 Role extension*: Addition of new roles
- *6.3.2.2 Resource access authorization*:
  - Addition of default rules
  - Addition of rules for non-security IEC/IEEE 60802 resources
  - New structure for the description of rules: role-centric description (not YANG module centric description as in D2.0)
    - Subject: Role
      - Resource: YANG module or path representing data node
      - Rights: Permitted or denied access operations

NACM Primer

- Access control is configured by ietf-netconf-acm by
  - **Global enforcement controls**, e.g. to enable/disable NACM or to define default rules for read, write and execute (if no explicit rule was found in the following rule lists)
  - **Access control rules** configuring a list of rule-list entries; per rule-list with
    - <name> Name of the rule-list
    - <group> Group for which the rule-list applies
    - Sequence of <rule> entries; per rule with
      - <name> Name of the rule
      - <module-name> Name of the to be accessed YANG module
      - <path> Optionally a specific path within the YANG module
      - <access-operation> Create, Read, Update, Delete, Exec
      - <action> Permit or deny

NACM Primer Rule Checking

- **Identification of "group" entries** that contain the role of the NETCONF client in "user-name“ entry
- **Process all rule-list entries, in the order** they appear in the configuration. If a rule-list's "group" leaf-list does not match any of the NETCONF client groups, proceed to the next rule-list entry
- For each rule-list entry found, **process all rules, in order**, until a rule that matches the requested access operation is found.
- If a **matching rule is found** in rule-lists, then the **"action" leaf is checked**.
  - If it is equal to "permit", then the protocol operation is permitted; otherwise, it is denied.
- If **no matching rule is found** in all rule-lists, then the **default-rules are checked**.
  - If it is equal to "permit", then the protocol operation is permitted; otherwise, it is denied.

NACM defaults in `ietf-netconf-acm` according to Basic Assumptions

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
       <enable-nacm>true</enable-nacm>
       <read-default>permit</read-default>
       <write-default>deny</write-default>
       <exec-default>deny</exec-default>
   …
</nacm>
```

NACM groups and 60802 defined roles in `ietf-netconf-acm`

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  ...
  <groups>
    <group> <name>TruststoreAdminGroup</name>
            <user-name>TruststoreAdminRole</user-name> </group>
    <group> <name>KeystoreAdminGroup</name>
            <user-name>KeystoreAdminRole</user-name> </group>
    <group> <name>UserMappingAdminGroup</name>
            <user-name>UserMappingAdminRole</user-name> </group>
    <group> <name>ConfiguratorGroup</name>
            <user-name>ConfiguratorRole</user-name> </group>
                <!- configuring IA-stations, e.g. CNC -->
    <group> <name>StreamConfiguratorGroup</name>
            <user-name>StreamConfiguratorRole</user-name> </group>
                <!- requesting streams at CNC entity, e.g. CUC -->
    <group> <name>SubscriberGroup</name>
            <user-name>SubscriberRole</user-name> </group>
                <!- requesting notifications from IA-stations, e.g. diagnostics station -->
  </groups>
  ...
</nacm>
```

NACM rules in `ietf-netconf-acm` for the TruststoreAdmin Group

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  ...
  <rule-list>
    <name>TruststoreAdminRule</name>
    <group>TruststoreAdminGroup</group>
    <rule> <name>deny-IDevID-write</name>
      <module-name>ietf-truststore</module-name>
      <path>/truststore/certificate-bags/certificate-bag[name=IEC60802]/
certificate[name=IDevID]</path>
      <access-operations>create update delete</access-operations>
      <action>deny</action> </rule>
    <rule> <name>permit-truststore</name>
      <module-name>ietf-truststore</module-name>
      <access-operations>*</access-operations>
      <action>permit</action> </rule>
  </rule-list>
  ...
</nacm>
```

NACM rules in `ietf-netconf-acm` for the KeystoreAdmin Group

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  ...
  <rule-list>
    <name>KeystoreAdminRule</name>
    <group>KeystoreAdminGroup</group>
    <rule> <name>deny-IDevID</name>
      <module-name>ietf-keystore</module-name>
      <path>/keystore/asymmetric-keys/asymmetric-key[name=IDevID]</path>
      <access-operations>*</access-operations>
      <action>deny</action> </rule>
    <rule> <name>permit-keystore</name>
      <module-name>ietf-keystore</module-name>
      <access-operations>*</access-operations>
      <action>permit</action> </rule>
  </rule-list>
  ...
</nacm>
```

NACM rules in `ietf-netconf-acm` for the UserMappingAdmin Group

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  ...
  <rule-list>
    <name>UserMappingAdminRule</name>
    <group>UserMappingAdminGroup</group>
    <rule> <name>permit-user-mapping</name>
      <module-name>ietf-netconf-server</module-name>
      <path>/netconf-server/listen/endpoint[transport=tls]/tls/netconf-server-parameters/client-identity-mappings/cert-to-name</path>
      <access-operations>*</access-operations>
      <action>permit</action> </rule>
    <rule> <name>permit-user-mapping-call-home</name>
      <module-name>ietf-netconf-server</module-name>
      <path>/netconf-server/call-home/netconf-client[transport=tls]/tls/netconf-server-parameters/client-identity-mappings/cert-to-name</path>
      <access-operations>*</access-operations>
      <action>permit</action> </rule>
</rule-list>
  ...
</nacm>
```

NACM rules in `ietf-netconf-acm` for the StreamConfigurator Group

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  ...
  <rule-list>
    <name>StreamConfiguratorRule</name>
    <group>StreamConfiguratorGroup</group>
    <rule>
      <name>permit-ieee802-dot1q-tsn-config</name>
      <module-name>ieee802-dot1q-tsn-config</module-name>
      <access-operations>*</access-operations>
      <action>permit</action>
      <comment>allow access to all UNI operations and data</comment> </rule>
  </rule-list>
  ...
</nacm>
```

NACM rules in `ietf-netconf-acm` for the Subscriber Group

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  ...
  <rule-list>
    <name>SubscriberRule</name>
    <group>SubscriberGroup</group>
    <rule>
      <name>permit-subscribed-notifications</name>
      <module-name>ietf-subscribed-notifications</module-name>
      <notification-name>*</notification-name>
      <access-operations>*</access-operations>
      <action>permit</action> </rule>
  </rule-list>
  ...
</nacm>
```

NACM rules in `ietf-netconf-acm` for the Configurator Group

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  ...
  <rule-list>
    <name>ConfiguratorRule</name>
    <group>ConfiguratorGroup</group>
    <rule> <!- permit rule for each YANG module according IEC/IEEE 60802 D2.0 6.7.9 except ietf-
truststore, ietf-keystore, ieee802-dot1q-tsn-config, ietf-subscribed-notifications, ietf-yang-push -->
      <name>permit-[YANG module]</name>
      <module-name>[YANG module]</module-name>
      <access-operations>*</access-operations>
      <action>permit</action> </rule>
    <rule> <!- permit rule for data nodes in ietf-netconf-server except the path to cert-to-name -->
      <name>permit-netconf-server-[PATH]</name>
      <module-name>ietf-netconf-server</module-name>
      <path>[PATH of permitted data node]</path>
      <access-operations>*</access-operations>
      <action>permit</action> </rule>
    ...
</nacm>
```