





# Security Analyst 21.2

## Release Notes

### CVSS Support

From now on it is possible to perform ISO 21434 compliant CVSS/AV based Security Analyses. This can be done in mixed-mode. Mixed-mode means, you may start with less knowledge about your system and could just use Attack Vectors (AV) to rate your attack steps.

	Feasibility Categories				AFL
	AV	AC	PR	UI	
<b>Local</b>	AV2				Low
<b>Accumulated</b>	<ul style="list-style-type: none"> <li> AV3: Physical CVSS 3.0</li> <li> AV2: Local CVSS 3.0</li> <li> AV1: Adjacent Network CVSS 3.0</li> <li> AV0: Network CVSS 3.0</li> </ul>				


When building up more knowledge you can easily migrate to the complete feasibility related set, including:

- Attack Vector (AV)
- Attack Complexity (AC)
- Privileges Required (PR)
- User Interaction (UI)

	Feasibility Categories				AFL
	AV	AC	PR	UI	
<b>Local</b>	AV2	AC0	PR1	UI1	Low
<b>Accumulated</b>	AV2	AC0	PR1	UI1	Low

### Reference External Elements

In the inspector of each element you can add an external link and directly navigate to it via the button to the left of the URL.

**External Link**  
 <https://external.link>

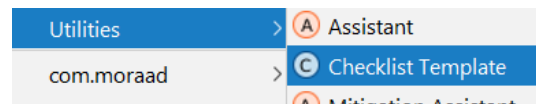
# WP.29 / UN Reg.155 Checklist

There is now a WP.29 Checklist in the ISO 21434 template. Items can be marked as “Relevant” or “Not-Relevant” and can have a Rationale. Of course, your checklists can be used in your reports using the corresponding report item “checklist”.

Threats regarding back-end servers related to vehicles in the field	Relevant	Not Relevant	Rationale
<b>1 Back-end servers used as a means to attack a vehicle or extract data</b>			
Abuse of privileges by staff (insider attack)	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Add rationale</a>
Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Add rationale</a>
Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Add rationale</a>

## Custom Checklists

Checklist Templates allow you to define your own Checklists. A Checklist can be instantiated via Right-Click in the Security Analyst View in “Utilities/Checklist Template”.



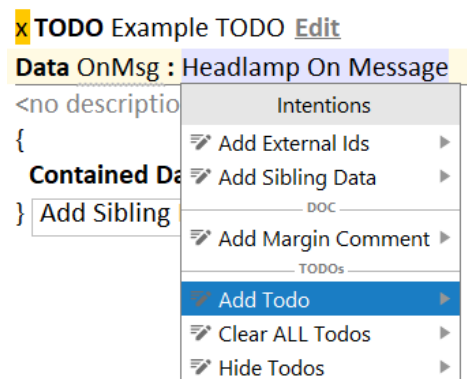
There are Checklist-Headers and -Items, which are arranged in Groups. Items can be marked as “Relevant” or “Not-Relevant” and can have a Rationale.

Group 1	Relevant	Not Relevant	Rationale
<b>Head 1.</b>			
Item 1	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Add rationale .</a>
Item 2	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Add rationale .</a>

## Improved TODOs

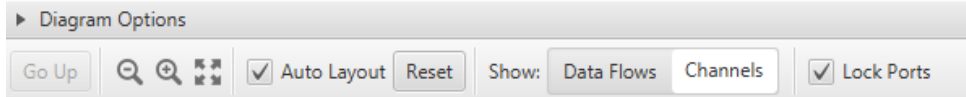
TODOs are now visible by default. Furthermore, you have more control using the revamped intentions.

You can add multiple TODOs to the same element now and toggle the visibility of TODOs with intentions. (<alt>+<enter>)

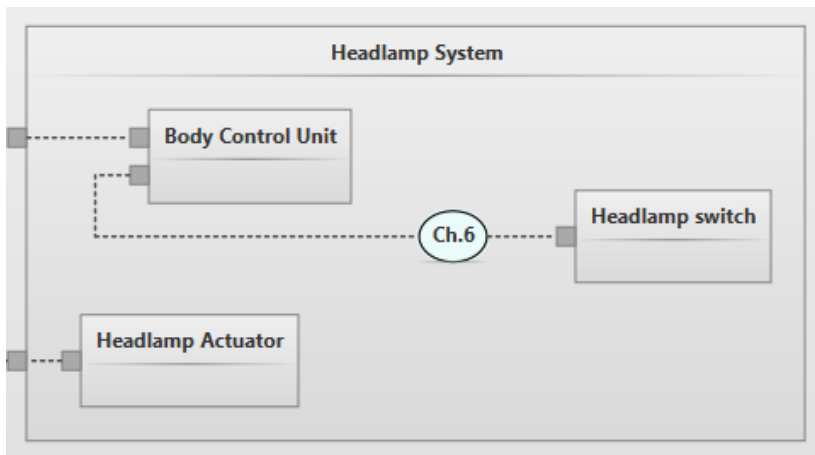


# Channel Visualization

In addition to visualizing Data Flows in the System Diagram, you may switch to showing channels, instead. The option can be found in the System Diagram tool bar:



Channels will be displayed as follows. All endpoints of the channel will be displayed and connected to the channel. Furthermore, you can create new Channels graphically, rename Channels and when creating new Data Flows, it is possible to decide for a target Channel.



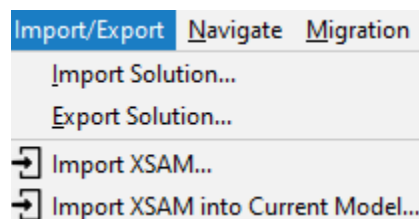
**Note:** The style and layouting is subject to change.

## Various fixes and improvements

- Damage Scenarios may contain “Normal Behavior” and “Operational Situation”
- Fixed and streamlined some icons and buttons
- New default style (e.g. having “clickable” Elements only underlined when hovered)
- Sort report elements by name
- Closing projects or changing project settings is no longer provoking error messages
- Improved description field behavior
- Performance improvement when changing titles
- Performance improvement when changing names
- Performance improvement in Assistants
- Minor fixes in several report items
- Sort risks in risk treatment by name
- Improve “Undo” in System Diagram
- Fixed “Lock Ports” in System Diagram
- “Security Analyst” project view is now active by default

# Open initiative for an exchange format

You might already know our exchange format XSAM. Starting from this, we are launching an initiative to form an open community which aims at establishing a cross-vendor, cross-tool XML-based format for eXchanging Security Analysis Models. We call it [openxsam.io](https://openxsam.io) and recently [talked about it at ASRG](#). If you are interested in joining the initiative, please contact us at [security-analyst@itemis.de](mailto:security-analyst@itemis.de).



Additionally, we still have the knowledge base at <https://www.security-analyst.org> about general security analysis processes and norms.

# Version Mapping

The following table can be used to determine the Security Analyst version based of the internal plugin version “com.moraad.core” that is stored in the .msd file of every solution:

```
<language slang="1:2bca1aa3-c113-4542-8ac2-2a6a30636981:com.moraad.core" version="<com-moraad-core-version>" />
```

com.moraad.core version	Security Analyst version
73	21.2
72	21.1.1
71	21.1
64	20.4
63	20.3.1
61	20.3
59	20.2.1
58	20.2
55	20.1.1
54	20.2.1
49	19.4.1
48	19.4
46	19.3.1
44	19.3
41	19.2
37	2.5.1