



ENCO SOFTWARE GMBH | Lortzingstr. 9 | D-81241 MÜNCHEN

SOX Feature Releases

Security Beta Version 3.3
Version 3.3 (09 / 2020)
Version 3.4 (11 / 2020)

Author: Rustam Achundov

Seite 1 / 3

EnCo Software GmbH
Lortzingstraße 9
81241 München
Germany

Tel.: +49 [0] 89 716 775 890
Fax: +49 [0] 89 716 775 899
info@enco-software.com
www.enco-software.com

Kontoverbindung:
Bremer Sparkasse
IBAN DE44290501010082531211
BIC: SBREDE22XXX

USt. ID: DE259 706 146
HR-Nr.: HRB 222055
DUNS-Nr.: 340 780 781
Geschäftsführer: Marcus Heine

SOX Version 3.3 Beta Security Release: 28th of August

- TARA – SAE J3061
 - Threat Definition and its column
 - Description columns at Impact Level
 - Description columns at Threat Level
- TARA - ISO 21434
 - Complete new TARA
 - Layout from TARA SAE J3061
 - Define Damage Scenario as Freetext
 - Define Threat Scenario as Freetext
- Create Security Goal with SAE J3061 as Guideline
- Create Security Goal with ISO 21434 as Norm
- Threat Definition in Security Goal View
- ATA
 - Select only Security Goals when creating an Attack Tree
 - Select Threat when creating an Attack Tree
 - Creating an Attack Tree after FTA Standards
 - Connect Gate with Element Category Type (EVITA Method)

Security Features in SOX Version 3.3 Release (09/2020)

- System Modeler
 - Definition of an Asset in the system model (SysML/UML)
 - Connect Cybersecurity Properties with Asset
- TARA
 - Derive Attack Tree out of TARA (Threat)
 - Enhancement of Threat Categories
 - Derive Requirements out of Security Goal
- ATA
 - When creating an Attack Tree and choosing a Threat, Threat will be created as the Top-Level Gate in Attack Tree
 - Select different Norms and Guidelines when creating an Attack Tree (SAE J3061 and ISO 21434)
 - Calculate Threat Level/Attack Feasibility Level at every Element in Attack Tree
 - Filterfunctionality in Overview Gates and Events

Security Features in SOX Version 3.4 Release (11/2020)

- TARA
 - Threat and Asset Overview
 - Definition of Damage Scenarios according to ISO 21434
 - Definition of Threat Scenarios according to ISO 21434
- Individualization of TARA
 - Create your own Definition for Impact and Threat/Attack Feasibility Level Parameters
 - Parameter Weighting
 - Parameter Value Assignment
 - Calculation Rules
 - Create your own Calculation Rules for the Security Level
- ATA
 - Propagation of Threat Level/Attack Feasibility Level
 - Transfer Threat Level/Attack Feasibility Level from ATA into TARA
 - Create Vulnerability Catalogs
 - Connect Asset Attacks with Vulnerabilities
- Reports
 - TARA Report
 - ATA Report