TITLE : Cyber Security

AUTHOR : 정재우 / Jaewoo Joung / 郑在祐/ (A.K.A.)海绵宝宝

DATE : 2023. 01. 27

TARGET AUDIENCE : Who wants to CyberSecurity engineering

ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering(8月 version) Explnation

Definition

Term	meaning
Archtectural design	Representation that allows for identification of the components, their boundaries, interfaces and interactions
asset	object that has value, or contributes to value
atack feasibility	attribute of an attack path describing the ease of sucessfully carrying out the corresponding set of actions
attack path	set of deliberate actions to realize a threat scenario
attacker	person, group, or organization that carries out an attack path
audit	examination of a process to determine the extent to which the process objectives are achieved
customer	person or organization that recieves a service or product
cybersecurity	Road vehicle cybersecurity condition in which assets are sufficiently protected against threat scenarios to items of road vehicles,their functions and their electrical or electronic components
cycbersecurity assessment	judgementof cybersecurity
cybersecurity concept	cybersecurity requirements of the item and requirements on the operational environment, with associated information on cybersecurity controls
cybersecurity control	measure that is modifying risk
cybersecurity event	cs-information that is relevant for an item or component
cybersecurity goal	Concept-level cybersecurity requirement associated with one or more threat scenarios
cybersecurity incident	situation in the field that can involve vernerability exploitation
cybersecurity information	information with regard to cybersecurity for wich relevance is not yet detemined
cybersecurity interface agreement	agreement between customer and supplier concerning distributed cs-activities
cybersecurity property	attribute that can be worth protecting
cybersecurity specification	cs-requirements and corresponding architectural design
damage scenario	adverse consquence involving a vehicle or vehicle function and affecting a road user
distributed cybersecurity activities	cybersecurity activities for the item or component whose responsibilities are distributed between customer and supplier
impact	estimate of magnitude of damage or physical harm from a damage scenario
item	component or set of components that implements a function

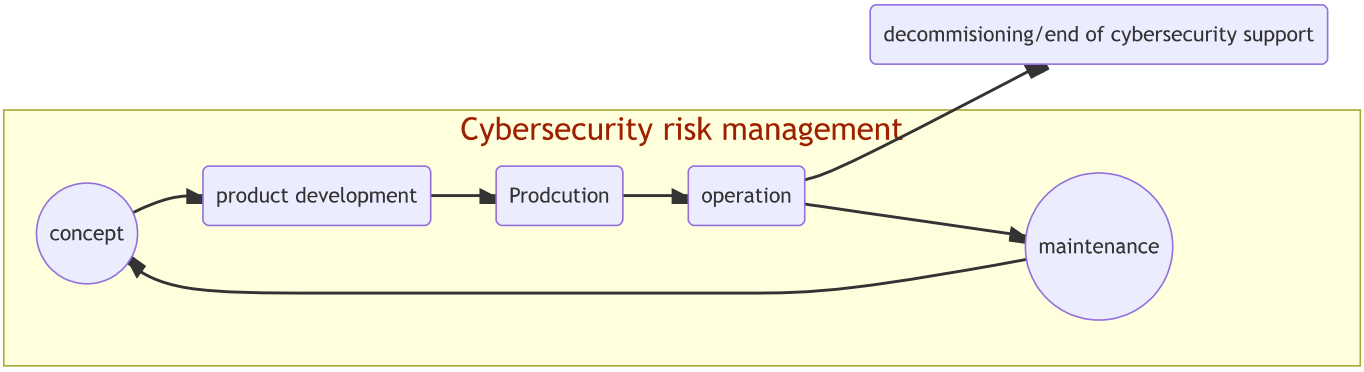
Term	meaning
operational environment	contect considering interactions in operational use
out-of-context	not developed in the context of a specific item
penetraton testing	cybersecurity testing in which real-world attacks are mimicked to indentify ways to compromise cybersecurity goals
risk	cybersecurity risk:effect of uncertainty on the road vehicle cybersecurity expressed in terms of attack feasibility and impact
risk management	coordinated activities to direct and control an organization with regard to risk
road user	person who uses a road
tailor	to omit or perform an activity in a different manner compared to its description in this document
threat scenario	potential cause of compromise of cybersecurity properties of one or more assets in order to realize a damage scenario
triage	analysis to detemine the relevance of cybersecurity information to an item or component
trigger	criterion for triage
validation	confirmation, through the provision of bjective evicence, that the cybersecurity goals of the item are adequate and are archieved
verification	confirmation, through the provision of objective evidence, that specified requirements have been fullfilled
vernerability	weakness that can be exploited as part of an attack path
vulnerability analysis	systematic identification and evaluation of vernerabilities
weakness	defect or characteristic that can lead to undesirable behaviour

Abbreviated terms

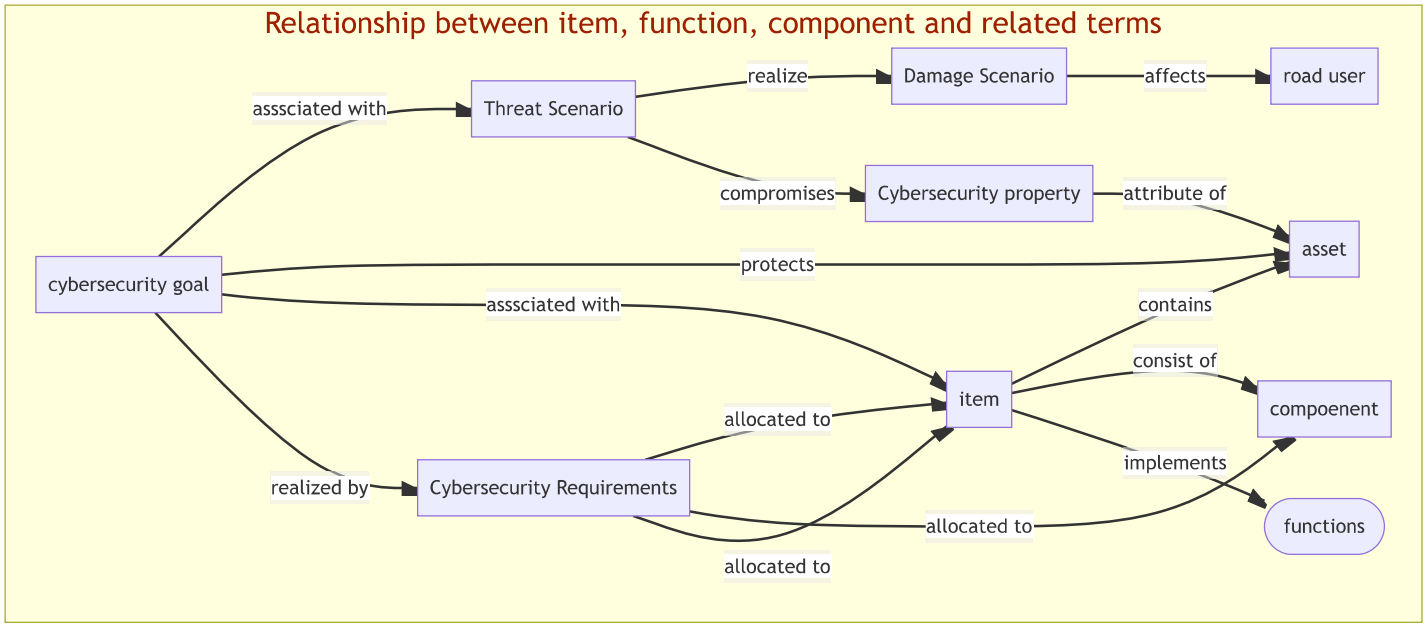
Abbreviation	meaning
CAL	Cybersecurity Assurance Level
CVSS	Common Vulnerability Scoring System
E/E	Electrical and electronic
ECU	Electrical Control Unit
OBD	On-Board Diagnostic
OEM	Original Equipment Manufacturer
PM	Permission
RC	Recommendation
RQ	Requirement
RASIC	Responsible, Accountable, Supporting, Informed, Consulted
TARA	Threat Analysis & Risk Analysis
WP	Work Product

Diagrams

Risk Management



Relationship Management



Questions to supplier

The following diagram to see the Supplier's Cyber security capability will help the person understand how to measure objectively.

Mainclause	Requirement ID	Subclause	Work Package ID	What are the output	what point we should ask	What we expect	point
Organizational cybersecurity management	5.4.1	Cybersecurity governance	[WP-05-01]	Cybersecurity policy, rules and processes	Could you tell us about your Cybersecurity policy and organizational rules and processes?	Cybersecurity Policy exist	2

Mainclause	Requirement ID	Subclause	Work Package ID	What are the output	what point we should ask	What we expect	point
Organizational cybersecurity management	5.4.2	Cybersecurity culture	[WP-05-01]	Cybersecurity policy, rules and processes	Could you tell us about your Cybersecurity policy and organizational rules and processes?	Rule exist	2
Organizational cybersecurity management	5.4.2	Cybersecurity culture	[WP-05-02]	Evidence of competence management, awareness management and continous imrpovement	May we see the evidence of the management of competency, awareness and Countinous imrpovement?	Continous improvement plan exist	2
Organizational cybersecurity management	5.4.3	Information sharing	[WP-05-01]	Cybersecurity policy, rules and processes	Could you tell us about your Cybersecurity policy and organizational rules and processes?	Process exist	2
Organizational cybersecurity management	5.4.4	Management Systems	[WP-05-03]	Evidence of the organization's management systems	Could we see your management system? And see how it is worked?	Evidence of management shown	2
Organizational cybersecurity management	5.4.5	Tool Management	[WP-05-04]	Evidence of tool management	Is there specific tool for Cybersecurity?	there is tool for cybersecurity	2
Organizational cybersecurity management	5.4.6	Informtion Security management	[WP-05-03]	Evidence of the organization's management systems	Could we see your management system? And see how it is worked?	management system exist	2
Organizational cybersecurity management	5.4.7	Organizational cybersecurity audit	[WP-05-05]	Organizational cybersecurity audit report	could we see your audit report?	there is internal periodic audit report	2
Project dependent cybersecurity management	6.4.1	Cybersecurity responsibilities	[WP-06-01]	Cybersecurity plan	May we see the Cybersecurity plan?	responsibility is written for human resource	2
Project dependent cybersecurity management	6.4.2	Cybersecurity planning	[WP-06-01]	Cybersecurity plan	May we see the Cybersecurity plan?	activities are distributed to people	2
Project dependent cybersecurity management	6.4.3	Tailoring	[WP-06-01]	Cybersecurity plan	May we see the Cybersecurity plan?	Tell us the story of how it was tailored	2
Project dependent cybersecurity management	6.4.4	Reuse	[WP-06-01]	Cybersecurity plan	May we see the Cybersecurity plan?	There is plan to reuse	2
Project dependent	6.4.5	Component out-of-context	[WP-06-01]	Cybersecurity plan	May we see the Cybersecurity plan?	There is plan for component out-of-context	2

Mainclause	Requirement ID	Subclause	Work Package ID	What are the output	what point we should ask	What we expect	point
cybersecurity management							
Project dependent cybersecurity management	6.4.6	off-the-shelf component	[WP-06-01]	Cybersecurity plan	May we see the Cybersecurity plan?	If there is off-the-shelf component, this should be shown	2
Project dependent cybersecurity management	6.4.7	Cybersecuirty case	[WP-06-02]	Cybersecurity case	May we see the Cybersecurity cases?	how many cases are created? >100 =5, >50 = 2, >20 = 1	5
Project dependent cybersecurity management	6.4.8	Cybersecurity assessment	[WP-06-03]	Cybersecurity assessment report	May we see the Cybersecurity assessment report?	There is Cybersecurity assessment report	1
Project dependent cybersecurity management	6.4.9	Release for post-development	[WP-06-04]	Release for post-development report	May we see the Release for post-development report?	We can see all the post release reports	1
Distributed cybersecurity activities	7.4.1	Supplier capability	None	N/A	Have we finished supplier capability with delievery?	SW capability Check done	5
Distributed cybersecurity activities	7.4.2	Request for quotation	None	N/A	Do we have RFQ?	RFQ exist	1
Distributed cybersecurity activities	7.4.3	Alignment of responsibilities	[WP-07-01]	Cybersecurity interface agreement	May we see the Cybersecurity interface agreement?	Is there Cybersecurity interface agreement	1
Continual cybersecurity activities	8.3	Cybersecurity monitoring	[WP-08-01]	Sources for cybersecurity infromation	May we see the Sources for cybersecurity infromation?	Internal and/or external sources was shown	1
Continual cybersecurity activities	8.3	Cybersecurity monitoring	[WP-08-02]	Triggers	May we see the Triggers?	Triggers are defined	1
Continual cybersecurity activities	8.3	Cybersecurity monitoring	[WP-08-03]	Cybersecurity event	May we see the Cybersecurity event?	The project's Cybersecurity event is explained	1
Continual cybersecurity activities	8.4	Cybersecurity event evaluation	[WP-08-04]	Weakness from cybersecurity event	May we see the Weakness from cybersecurity event?	weaknesses found during product development exist	1
Continual cybersecurity activities	8.5	Vulnerability analysis	[WP-08-05]	Velnerability analysis	May we see the Velnerability analysis?	past vernerability analysis includes attack path	1
Continual cybersecurity activities	8.6	Vernerability management	[WP-08-06]	Eveidence of managed vulnerabilities	May we see the Eveidence of managed vulnerabilities?	documented vernarability analysis	1
Concept phase	9.3	Item definition	[WP-09-01]	Item definition	May we see the Item definition?	items boundary and function and	1

Mainclause	Requirement ID	Subclause	Work Package ID	What are the output	what point we should ask	What we expect	point
						architecture is defined	
Concept phase	9.4	Cybersecurity goals	[WP-09-02]	TARA	May we see the TARA?	TARA(Threat Analysis and Risk Assessment) is writtendown	5
Concept phase	9.4	Cybersecurity goals	[WP-09-03]	Cybersecurity goals	May we see the Cybersecurity goals?	TARA Goal is defined	5
Concept phase	9.4	Cybersecurity goals	[WP-09-04]	Cybersecurity claims	May we see the Cybersecurity claims?	risk value determined and calculated	5
Concept phase	9.4	Cybersecurity goals	[WP-09-05]	Verification report for cybersecurity goals	May we see the Verification report for cybersecurity goals?	Verification report finished	1
Concept phase	9.5	Cybersecuirty concept	[WP-09-06]	Cybersecurity concept	May we see the Cybersecurity concept?	Cybersecurity concept exist and match with later	2
Concept phase	9.5	Cybersecuirty concept	[WP-09-07]	verification report for cbersecurity concept	May we see the verification report for cybersecurity concept?	complete requirements and CAL(Cybersecurity Assurance Level) is defined	2
Product development phase	10.4.1	Design	[WP-10-01]	Cybersecurity specifications	May we see the Cybersecurity specifications?	Cybersecurity specification is writen down	2
Product development phase	10.4.1	Design	[WP-10-02]	Cybersecurity requirements for post-development	May we see the Cybersecurity requirements for post-development?	Cybersecurity Requirement exist	2
Product development phase	10.4.1	Design	[WP-10-03]	Documentation of the modelling, design, or programming languages and coding quidelines	May we see the Documentation of the modelling, design, or programming languages and coding quidelines?	Documentation of the modelling, design, or programming languages and coding quideline exist	5
Product development phase	10.4.1	Design	[WP-10-04]	Verification report for the cybersecurity specifications	May we see the Verification report for the cybersecurity specifications?	Verification report for the cybersecurity specifications exist	1
Product development phase	10.4.1	Design	[WP-10-05]	Weaknesses found during product development	May we see the Weaknesses found during product development?	Weaknesses found during product Design exist	1
Product development phase	10.4.2	Integration and verification	[WP-10-05]	Weaknesses found during product development	May we see the Weaknesses found during product development?	Weaknesses found during product integration exist	1
Product development phase	10.4.2	Integration and verification	[WP-10-06]	Integration and verification specification	May we see the Integration and verification specification?	Integration and verification specification exist	1

Mainclause	Requirement ID	Subclause	Work Package ID	What are the output	what point we should ask	What we expect	point
Product development phase	10.4.2	Integration and verification	[WP-10-07]	Intergration and verification report	May we see the Intergration and verification report?	Intergration and verification report exist	3
Product development phase	Clause 11	Cybersecuirty validation	[WP-11-01]	Validation report	May we see the Validation report?	Validation report exist	1
Post-development phases	Clause 12	Production	[WP-12-01]	Production control plan	May we see the Production control plan?	Cybersecurity Production control plan exist	1
Post-development phases	13.3	Cybersecurity incident response	[WP-13-01]	Cybersecurity incident response plan	May we see the Cybersecurity incident response plan?	Cybersecurity incident response plan exist	1
Post-development phases	13.4	Updates	None	N/A	Could we see your Updates status?	Updates Status exist	1
Post-development phases	14.3	End of Cybersecurity support	[WP-14-01]	procedures to communicate the end of cybersecurity support	May we see the procedures to communicate the end of cybersecurity support?	end of cybersecurity support plan exist	2
Post-development phases	14.4	decommissioning	None	N/A	If your company is in anyways decommissioned, what are the key points for us to follow	If you company is decommissioned, what may happen?	1
Threat analysis and risk assessment methods	15.3	Asset identification	[WP-15-01]	Damage scenarios	May we see the Damage scenarios?	damage scenarios exist	1
Threat analysis and risk assessment methods	15.3	Asset identification	[WP-15-02]	Assets with cybersecurity properties	May we see the Assets with cybersecurity properties?	Asset definition defined	1
Threat analysis and risk assessment methods	15.4	Threat scenario identification	[WP-15-03]	Threat scenarios	May we see the Threat scenarios?	threat scenarios exist	1
Threat analysis and risk assessment methods	15.5	Impact rating	[WP-15-04]	Impact ratings with associated impact catagories	May we see the Impact ratings with associated impact catagories?	Impact rating exist	1
Threat analysis and risk assessment methods	15.6	attack path analysis	[WP-15-05]	Attack paths	May we see the Attack paths?	attack paths exist	1
Threat analysis and risk assessment methods	15.7	attack feasibility rating	[WP-15-06]	Attack feasibility ratings	May we see the Attack feasibility ratings?	Attack feasibility ratings exist	1

Mainclause	Requirement ID	Subclause	Work Package ID	What are the output	what point we should ask	What we expect	point
Threat analysis and risk assessment methods	15.8	Risk value determination	[WP-15-07]	Risk values	May we see the Risk values?	risk values exist	1
Threat analysis and risk assessment methods	15.9	Risk treatment decision	[WP-15-08]	Risktreatment decisions	May we see the Risk treatment decisions?	risktreatment decisions exist	1
						Total Score	100

Although; Score system is not in the ISO, for a company to measure and deliver better cyber security, it would be necessary to have a standard. Thus, the following system is proposed.