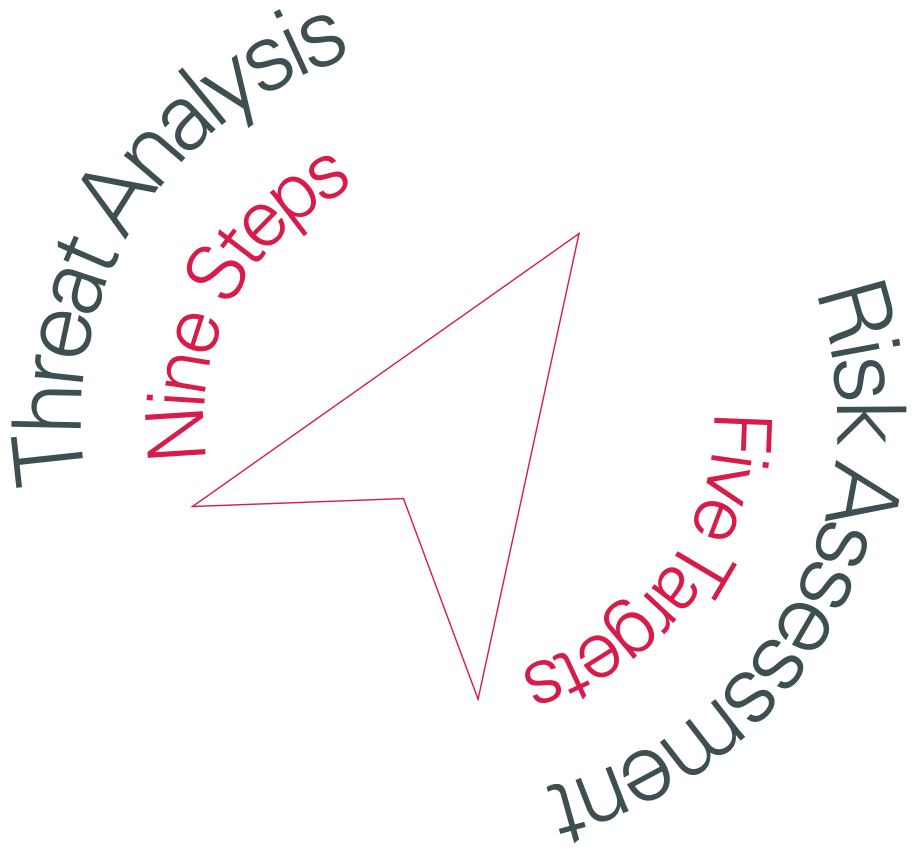
TARA in Practice.

How to perform your first Threat Analysis and Risk Assessment

by Thomas Liedtke, PhD



Automotive Cybersecurity
Step by Step

KUGLER MAAG CIE
besser mit uns

Thomas Liedtke, PhD

I'm a computer scientist by background. I'm a family man and father of several children. After completing my PhD at the University of Stuttgart I entered the telecommunications industry. At Alcatel-Lucent I rose to a role of responsibility and over the course of 14 years I successfully spearheaded a variety of projects, also managing different departments.

I entered the field of consulting more than a decade ago and has been offering my wealth of experience to clients in a variety of industries ever since, primarily in the areas of safety, security, privacy and project management.

Beyond my responsibilities as a principal at Kugler Maag Cie, I'm involved in a number of committees, particularly the working group for Automotive Cybersecurity at the German Electrical and and the VDA Cybersecurity Work Group organised by the (DIN standard NA052-00-32-11AK and ISO standard TC22/SC32/WG11).

About this White Paper

Hello folks, this white paper contains the same information I've covered in my Automotive Cybersecurity for beginners video on YouTube.

Both the YouTube tutorial and this document cover the core concepts of performing risk assessments in general and a TARA in particular. They are not complete by any means. This publication has been prepared for general guidance only. Please do not act according to any information given in this document without receiving specific professional consultancy. The publisher, KUGLER MAAG CIE GmbH, shall not be liable for any damages resulting from any use of the information contained in this report.

If you want to learn more about Automotive Cybersecurity and become a Automotive Cybersecurity expert, check out our trainings:

www.kuglermaag.com/cybersecurity-classes

Special classroom training is available for aspiring TARA practitioners:

www.kuglermaag.com/tara-training

The Nine2Five TARA-Navigator

The name says it all: The Nine2Five TARA-Navigator consists of nine analysis steps and five targets for cybersecurity.

The TARA Navigator is a proven procedure for conducting structured Threat Analyses and Risk Assessments in the concept phase.

It prepares the process steps from ISO/SAE DIS 21434 for use in practice.

In addition, the TARA Navigator provides you with information on which methods are particularly helpful.

S1-9 Analytical steps
T1-5 TARA targets
ISO/SAE 21434 reference
Methods we recommend
Target

Risk assessments are the centerpiece of Automotive Cybersecurity. Therefore Clause 8 of the coming ISO/SAE 21434 industry standard outlines the basic elements of a risk analysis. In the concept phase, a comprehensive risk assessment is expected, the so-called TARA – Threat Analyses and Risk Assessment.

With the Nine2Five TARA navigator I present a practice-proofed approach how you can perform your first risk analysis in a smart and structured manner.

The connected car and its components must be safe and secure during its entire lifetime. For this, you must protect your products against cyberattacks. Otherwise, you accept that your stakeholders will suffer losses in terms of safety, finance, operations, or privacy terms. That is not a good option.

ISO/SAE 21434
Road vehicles – cybersecurity engineering

But do you really know all the potential threat scenarios that your vehicle project will be exposed to? You can neither foresee the motivation nor the abilities of an attacker in future.

To cope with this challenge, you must continuously find out if, where and how
_your product is vulnerable.
_what harm is associated with the threat, and
_how you intend to manage the impact of the threats.

A risk analysis is a procedure in which findings are checked and related to each other in a structured and step-by-step manner. The Nine2Five TARA Navigator includes nine steps and five targets.

I will now explain this procedure to you. Think of the TARA procedure like a string of pearls: Like another pearl, we always add another analysis or identification step to the previous, from the very left to the right of the string. With each step you only must think about one topic.

Item Definition
Before you can start with your TARA, you must define your item first. This is a sub-system or a set of syb-systems, for example a function or a control unit. Describe the environment of this system, its functions, interactions, and what interfaces there are.

Step 1
Asset Identification
Then we come to our first analytical step, the so-called asset identification.

An asset belongs to your item– and it is worth protecting! It defines a property crucial for functionality. Take for example the internet communication channel – hardly any electronic system is conceivable without this asset. Encryption keys or safety goals are further examples.

However, the asset is very interesting for two parties: for your stakeholder, who thus gets the required functionality, as well as for an attacker to compromise your system.

Therefore, the primary step is to enumerate all your assets.

What can go wrong?

Systematically question each of the assets in terms of
_confidentiality,
_integrity, and
_availability

as well as
_non-repudiation,
_authenticity, and
_authorization.

The ISO/SAE 21434 standard describes these attributes as cybersecurity properties.

You identify a damage scenario by checking what happens if one of the cybersecurity properties is compromised.
This was the asset identification in short.

Step 2
Impact Rating
We continue on our string of pearls with the impact rating.

Here we evaluate the damage scenarios according to what consequences they may have for your stakeholders. This includes functional safety, finance, operations, and privacy. Tables help to determine the damage effect. The catch here is that not every stakeholder is equally affected by every damage scenario.

By the way, we have also achieved our first target: we've rated the impact of damage.

T1 Impact of Damage

Step 3
Threat Scenario Identification
In the first step we have spoken about the potential damage caused by a compromised cybersecurity property. Now we look at the selected assets again and ask what threat scenario may arise.

To make this clear we take a defective switch as an example. This damage scenario results in a possible threat scenario, namely the compromising of the CAN bus by spoofing or flooding.

Step 4
Attack Path Identification
The defect switch from our example is somewhere in the middle of the vehicle. In order to compromise the CAN bus, an attacker has to find a way through the system. The ISO standard now thinks backwards: What path must a potential attacker follow for the threat scenario to occur? This hike is called attack path.

You'll find a list of samples of vulnerabilities provided by UNECE regulations. So, see if these vulnerabilities are levant in your system. If yes, then check if they can support you to identify further threat scenarios.

Theory is fine. But is this attack realistic?

Step 5
Attack Feasibility Rating
In practice, not every attack can be conducted. Maybe encryption makes it unlikely. Therefore, we now look at the actual attack potential.

There are five key parameters for your evaluation:
_elapsed time
_the required expertise and
_product know-how as well as
_equipment and
_the window of opportunity.

Once we know whether an attacker can conduct an attack successfully, we have achieved target number two: Rating of the feasibility of an attack.

Step 6
Risk Value Determination
For this step we combine the results of both targets – impact rating (1. target) and attack feasibility rating (2. target).

$$Value_{Risk} = Impact_{Damage} \times Feasibility_{Attack}$$

We therefore have two ratings that determine the risk value:
_the impact of the associated damage scenario and
_the attack feasibility of the attack paths.

However, we usually have different stakeholders. Some of them assess the risks very differently. That makes things tricky – we may have to apply a different risk value for each stakeholder.

In any case, we have achieved the third target: we know the risk value.

Step 7
Risk Treatment Decision
Once the risks are on the table, the question is how to deal with them.

There are basically a set of options for dealing with risks:
1. avoidance
2. reduction
3. sharing or transfer to third parties
4. acceptance.

Risk reduction examples are specifying a security control on both levels technical or organizational or by introducing redundancy. Risk sharing is the business model of any insurance company.

Now decide, how you want to manage the risk.

Please keep in mind: It is very tricky to judge how effective a cybersecurity control is. However, this is where every risk assessment stands and falls.

Step 8
Cybersecurity Goals
The cybersecurity goals and claims are derived from
_the results of the TARA and
_your decisions on how the risks should ultimately be dealt with.

If you decide that you want to avoid a risk, then you go back to square one – you may consider an alternative technical solution.

The cybersecurity goals form the fourth target of the TARA.

Now we are on the home stretch.

Step 9
Cybersecurity Concept
The cybersecurity concept is derived from the cybersecurity goals. It describes how to you want to put the cybersecurity goals in practice: Derive requirements from the goals and allocate them to your architecture that means to the relevant components of your systems or organization. These requirements and their allocation to the architecture are all described in the cybersecurity concept.

The cybersecurity concepts capture all cybersecurity requirements and their allocation, this is our last target.

That takes us through all the nine steps I recommend performing. You have seen that all steps build on each other. Like a string of pearls, the next step usually refers to its predecessor and evaluates it or develops it further.

Let me conclude by summarizing the Nine2Five TARA Navigator.

Define your item or your system to prepare the TARA.

First step: Identify your assets. This includes the enumeration of your assets, the alignment with the cybersecurity properties and the identification of a damage scenario.

Secondly, rate the impact of the potential damage.
This leads you to the first objective, the impact rating.

Number 3: Identify your threat scenarios.

Fourth step: Analyze attack paths.

Fifth step: Analyze the attack feasibility.
The second objective indicates the ease of an attack.

Number 6: Determine the risk.
Objective number three names the risk level.

Step number 7: Decide how to treat the risk.

Eight: Derive the cybersecurity goals.
These goals are our target number 4.

Step number nine: Allocate the cybersecurity requirements to your components.
They lead directly to our fifth target, the cybersecurity concept.

So, now you know how you can perform a Threat analysis and risk assessment according to the ISO/SAE 21434. Please keep in mind that the international standard expects you to perform a risk assessment not only once but on a regular basis.

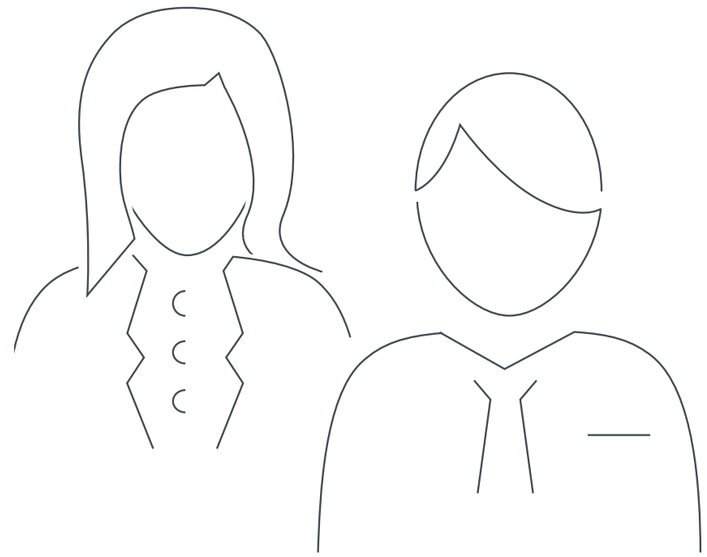
If you would like to read all of this at your leisure or perhaps integrate it into your company training programme, then use the link below to download the corresponding white paper. If you liked the video and are interested in further specialist topics, please subscribe to this Kugler Maag and Company YouTube channel and watch more videos. And maybe you will recommend our videos to your colleagues. See you soon.

KUGLER MAAG CIE GmbH
Leibnizstr. 11
70806 Kornwestheim
Germany

kuglermaag.com
information@kuglermaag.com

Management Consulting
Improvement Programs

- Automotive SPICE
- Automotive Security
- Functional Safety
- Agile Automotive



Driving the automotive industry forward.

www.kuglermaag.com

KUGLER MAAG CIE
besser mit uns