

# AN INTRODUCTION TO THREAT MODELING IN PRACTICE

Thorsten Tarrach, Christoph Schmittner



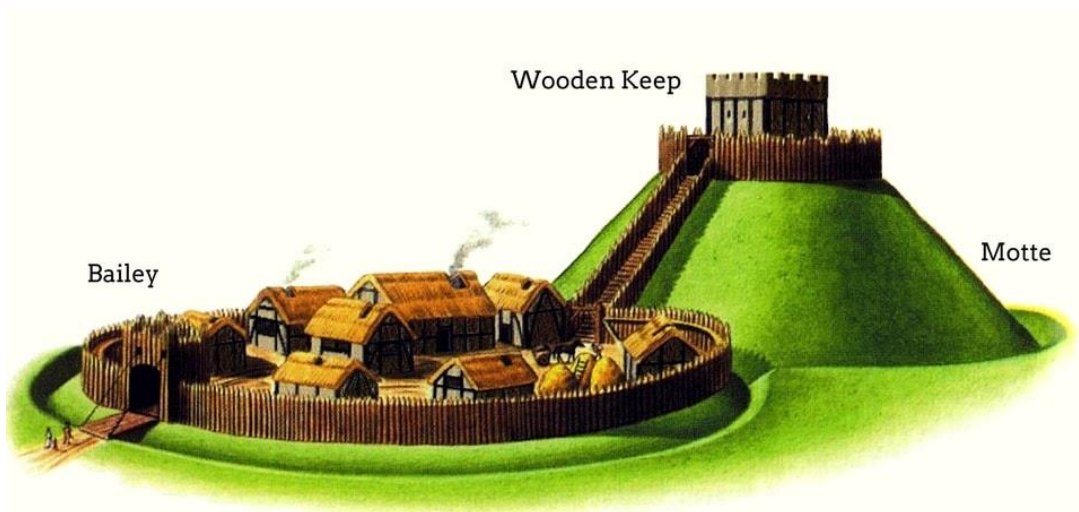
# WHAT IS THREAT MODELING

## Introduction



# WHAT IS THREAT MODELING

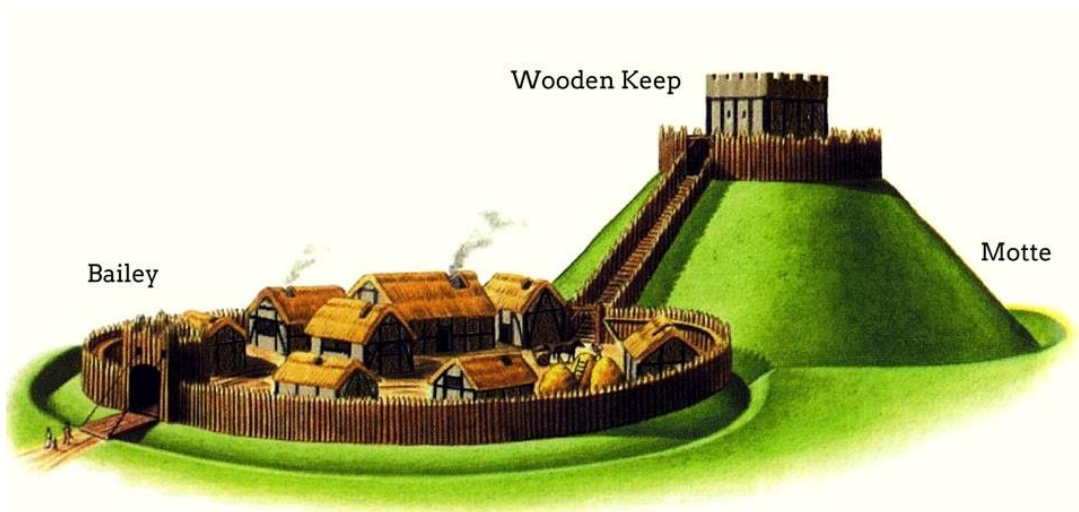
- **Structured Process**
  - Examination of a system for potential weaknesses



<https://www.castlesworld.com/tools/motte-and-bailey-castles.php>

# WHAT IS THREAT MODELING

- **Structured Process**
  - Examination of a system for potential weaknesses
- **Systematic approach**
  - Based on a conceptual model of weaknesses and threats



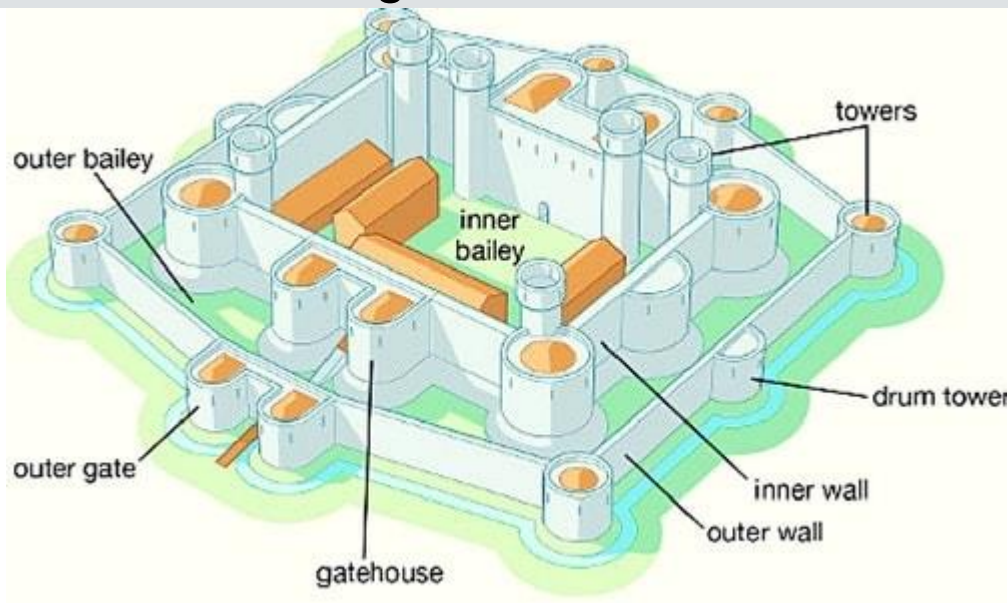
<https://www.castlesworld.com/tools/motte-and-bailey-castles.php>



[https://deadliestwarrior.fandom.com/wiki/Huo\\_Chien](https://deadliestwarrior.fandom.com/wiki/Huo_Chien)

# WHAT IS THREAT MODELING

- **Structured Process**
  - Examination of a system for potential weaknesses
  - Resolving identified weaknesses
- **Systematic approach**
  - Based on a conceptual model of weaknesses and threats



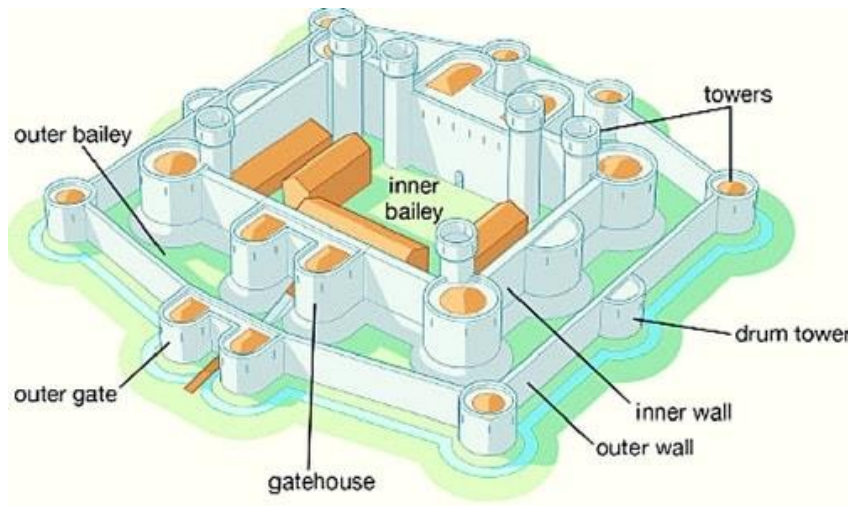
<https://www.castlesworld.com/tools/concentric-castles.php>



[https://deadliestwarrior.fandom.com/wiki/Huo\\_Chien](https://deadliestwarrior.fandom.com/wiki/Huo_Chien)

# WHAT IS THREAT MODELING

- **Structured Process**
  - Examination of a system for potential weaknesses
  - Resolving identified weaknesses
- **Systematic approach**
  - Based on a conceptual model of weaknesses and threats
  - Keeping the model of weaknesses and threats current



<https://www.castlesworld.com/tools/concentric-castles.php>



<https://www.pbs.org/video/1812-niagara-frontier-fort-george-cannon-firing/>

# THREAT MODEL

STRIDE

# STRIDE

- **Spoofing**
  - Person or program successfully impersonate someone else



<https://www.amazon.com/Moustache-Sailor-Fancy-Costume-Outfit/dp/B07QXT3C26>

# STRIDE

- **Tampering**
  - Modify something in a way which is not desired by the considered stakeholder



<https://www.pinterest.at/pin/477311260477998586/>

# STRIDE

- **Repudiation**
  - Actions cannot be assigned to a person or program



# STRIDE

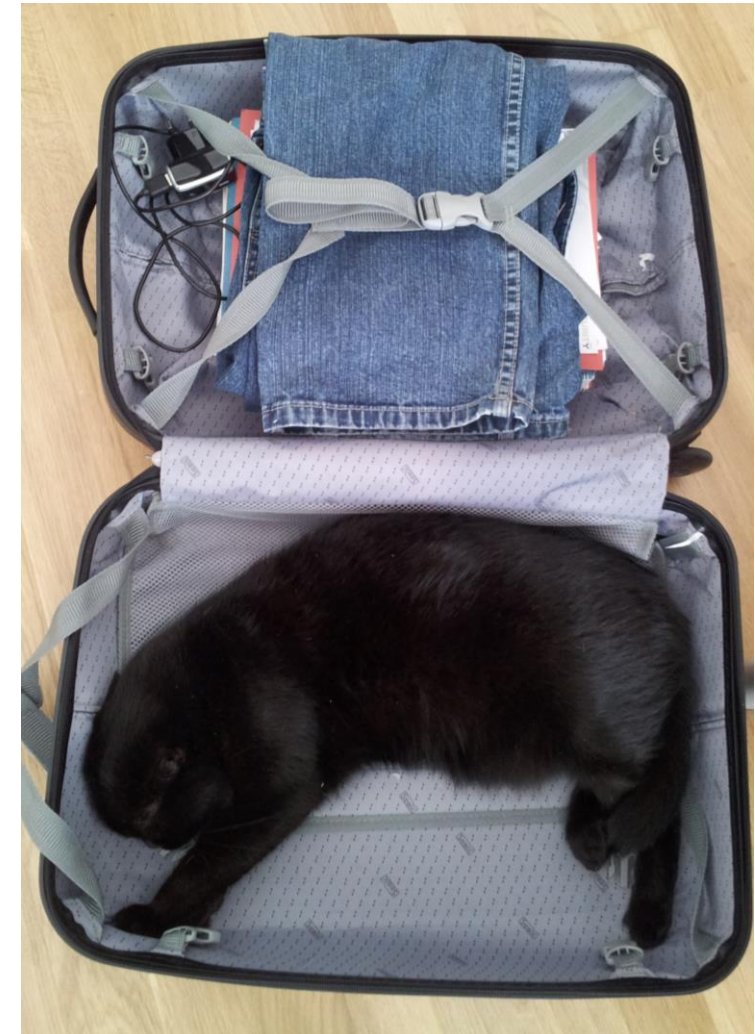
- **Information disclosure**
  - Sensitive information becomes known to people who should not know it



<https://www.tarses.com/blog/%EF%BB%BFlandlords-do-not-have-x-ray-vision-like-superman/>

# STRIDE

- **Denial of Service**
  - Resource or service is made temporarily or indefinitely unavailable



# STRIDE

- **Elevation of Privilege**
  - Gain elevated privileges



<https://tvtropes.org/pmwiki/pmwiki.php/Main/TotemPoleTrench>

# APPLY THIS TO IT – STANDARD WAY

- We model the system as a dataflow diagram
  - Processes, data stores, external elements communicate with each other over dataflows
- And we define susceptibilities for the elements based on STRIDE

	S	T	R	I	D	E
Process	X	X	X	X	X	X
Data flow		X		X	X	
External element	X		X			
Data store		X		X	X	

# ISSUES

- Works for a rough system draft
  - Less suited for systems modeled in more details
    - There is a connection, but no intended data flow
- Also challenging if the threat model is more concrete
  - How to describe known issues or weaknesses
    - If there is no time stamp or version number in an update an attacker could cause a downgrade
- Difficult for certification, missing traceability

# AIT APPROACH FOR THREAT MODELING

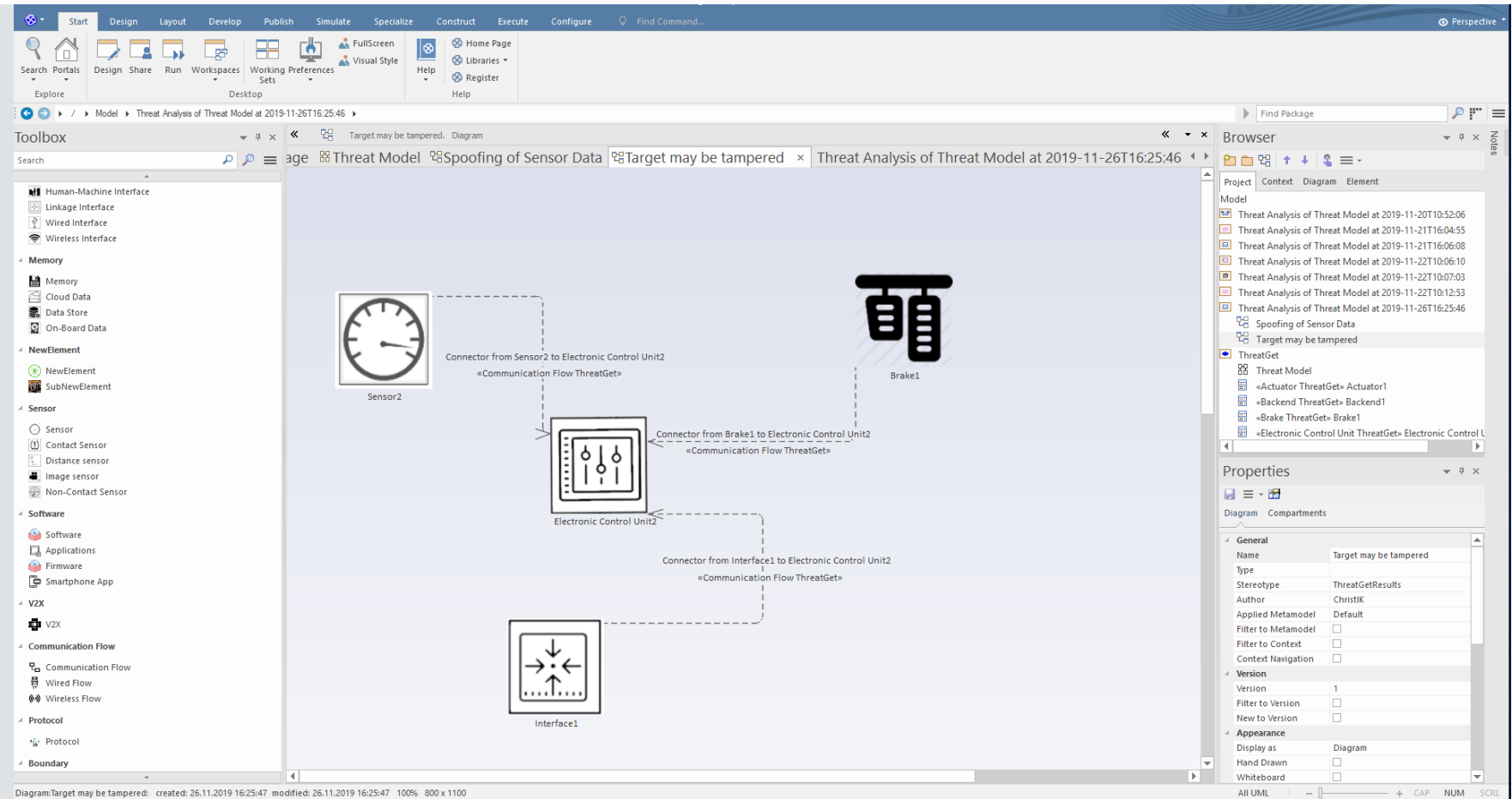
Developed for embedded systems and integrated in model-based engineering



# MODEL-BASED ENGINEERING

## Security Model

- **ThreatGet is integrated into Enterprise Architect**
- **Extensive model library with security properties and common domain elements**



# DOMAIN ELEMENTS

## Domain Elements

- Set of common elements for a domain
- Inheritance and Refinement
- Customizable

ThreatGet

RULESELEMENTS

admin

Actuator (Shapes)

Electric Actuator

Hydraulic actuator

Pneumatic actuator

+

Backend (Shapes)

Third Party Server

Update Server

+

Communication Element (Shapes)

Wired Bus Communication Element

Wired Communication Element

Wireless Bus Communication Element

Wireless Communication Element

+

Electronic Control Unit (Shapes)


Communication-ECU

High-Performance ECU

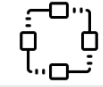
Low-Performance ECU

Element: Communication Element

























Description: ThreatGet Communication Element

Icon: 

Change

Image: 

Change


No.	Name	Default	Fixed	Inherited	Actions
1	Bandwidth	undefined	<input type="checkbox"/>	<input checked="" type="checkbox"/>	  
2	Communication Latency	undefined	<input type="checkbox"/>	<input checked="" type="checkbox"/>	  
3	Communication Reliability	undefined	<input type="checkbox"/>	<input checked="" type="checkbox"/>	  
4	Error Rate	undefined	<input type="checkbox"/>	<input checked="" type="checkbox"/>	  
5	Protocol version	Default	<input type="checkbox"/>	<input checked="" type="checkbox"/>	  
6	Protocols	undefined	<input type="checkbox"/>	<input checked="" type="checkbox"/>	  
7	Range	undefined	<input type="checkbox"/>	<input checked="" type="checkbox"/>	  
8	Troughput	undefined	<input type="checkbox"/>	<input checked="" type="checkbox"/>	  

ADD VALUE

# SECURITY PROPERTIES



## Security Properties



- Relevant security properties
- Assignable to elements
- Customizable

 ThreatGet
 

RULES

ELEMENTS


 admin

Name:

Secure Boot

Description:

Does the hardware element support secure boot

Default:

undefined

No.	Value	Default	Action
1	yes	<input type="checkbox"/>	×
2	no	<input type="checkbox"/>	×
3	undefined	<input checked="" type="checkbox"/>	

ADD VALUE

# AUTOMATED SECURITY ASSESSMENT

## Rule Engine

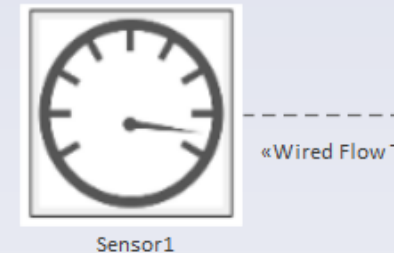
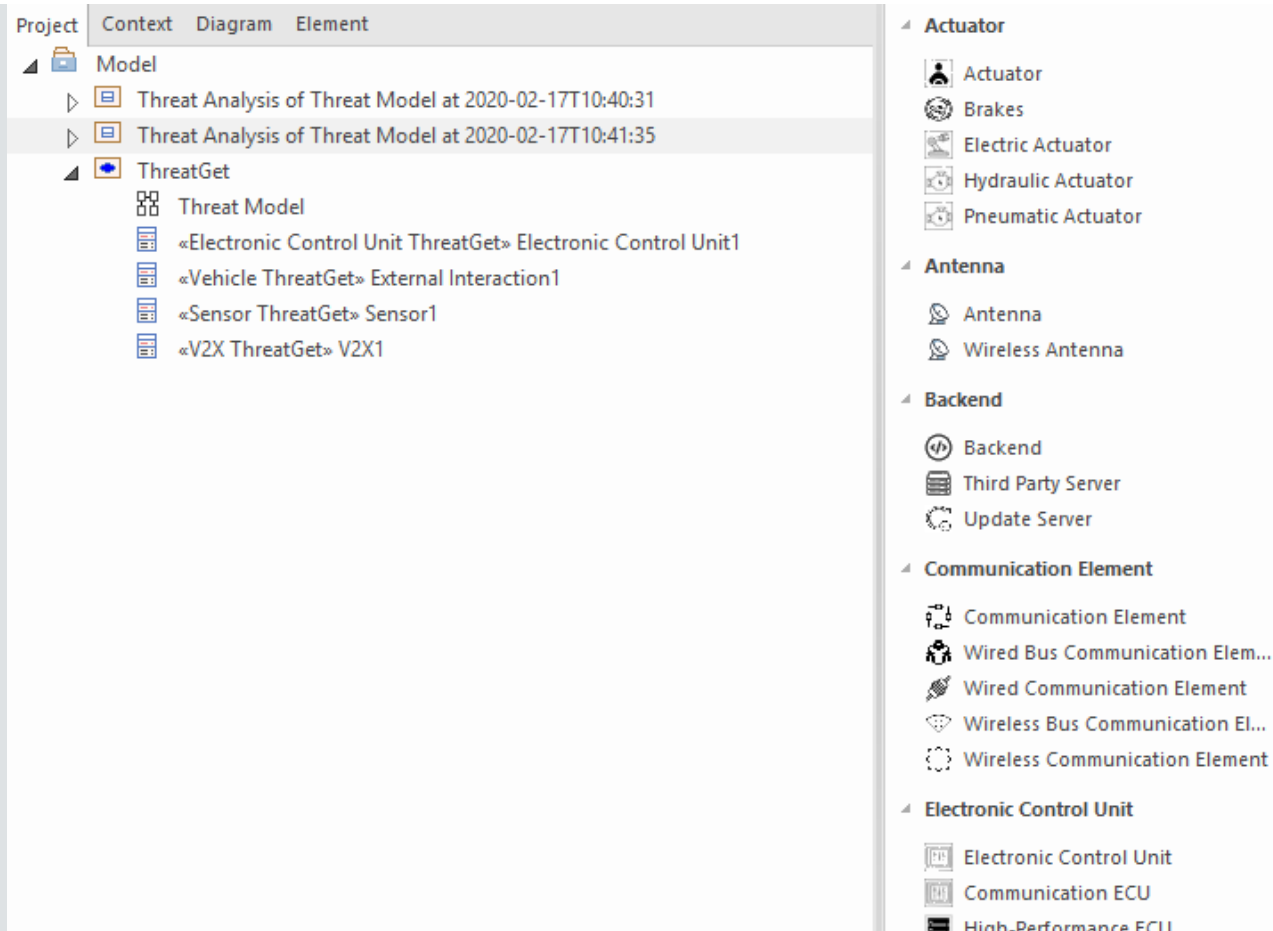
- Rules describe potential weaknesses
- Custom made Grammar
- Multi-hops attacks
- Usage of multiple databases

ThreatGet		RULES		ELEMENTS		admin	
		Search Rules					
#	Title	Description	ThreatType	Owner	Activated	Actions	
1	Compromised Target via a physical interface	Include: source is [USB] or source is [OBD 2]	Tampering	AIT	<input checked="" type="checkbox"/>		
2	Manipulate the Map Data on the Target Prior to it Being Delivered to the Car	Include: source is [Map Update Server] Exclude: flow,[Provides Integrity ...	Tampering	AIT	<input checked="" type="checkbox"/>		
3	Server is used to attack vehicle	Include: source is [Web Server] or source is [Update Server] or source is ...	Elevation of Privilege	AIT	<input checked="" type="checkbox"/>		
4	Jamming of Sensor or V2X Data	Include: flow,[Physical Network] is 'Local Area Wireless Network' and tar ...	Denial of Service	AIT	<input checked="" type="checkbox"/>		
5	Compromise by external apps	Include: source is [Infotainment System] or target is [Infotainment Syst ...	Elevation of Privilege	AIT	<input checked="" type="checkbox"/>		
6	Spoof messages in the vehicle network	Include: target is [Control Unit] or target is [Data Store] and flow,[Phy ...	Spoofing	AIT	<input checked="" type="checkbox"/>		
7	Use USB devices to attack Target	Include: target is [USB] or source is [USB] and target,[Stores Personal ...	Tampering	AIT	<input checked="" type="checkbox"/>		
8	Data Flow Sniffing	Include: flow is [Communication_flow] and flow crosses [Boundary] or flo ...	Information Disclosure	AIT	<input checked="" type="checkbox"/>		
9	Gaining unauthorised access to files or data on Source	Include: source is [Data Store] or source is [Control Unit] or source,[S ...	Information Disclosure	AIT	<input checked="" type="checkbox"/>		
10	Extract Data / Code from Control Unit	Include: source is [Control Unit] or source is [Data Store] Exclude: sou ...	Information Disclosure	AIT	<input checked="" type="checkbox"/>		
11	Message replay attacks in Target	Include: source is [Control Unit] and target is [Control Unit] Exclude: ...	Repudiation	AIT	<input checked="" type="checkbox"/>		
12	Attempt to Flash the Target With Custom Firmware	Elevation of privileges in order to gain complete control of Electronic Co ...	Elevation of Privilege	AIT	<input checked="" type="checkbox"/>		
13	Cause the Target to Crash or Stop or disabling functions	Include: source is [Electronic Control Unit] or source [Interface] and ...	Denial of Service	AIT	<input checked="" type="checkbox"/>		
14	Services from back-end server disrupted	Include: source is [Web Server] or source is [Update Server] or source is ...	Elevation of Privilege	AIT	<input checked="" type="checkbox"/>		
15	Spoofing the Source	Include: target is [Control Unit] or target is [Data Store] or target is ...	Spoofing	AIT	<input checked="" type="checkbox"/>		
16	Spoofing of Sensor Data	Include: source is [Sensor] and flow,[Physical Network] is 'Local Area W ...	Spoofing	AIT	<input checked="" type="checkbox"/>		
17	Impersonate Source	Include: target is [V2X ] or target is [V2X Gateway] Exclude: flow,[Sou ...	Spoofing	AIT	<input checked="" type="checkbox"/>		
18	Remote Attack Against Vehicle over the Internet	Include: target is [Infotainment System] and source is [WiFi Access Point ...	Spoofing	AIT	<input checked="" type="checkbox"/>		

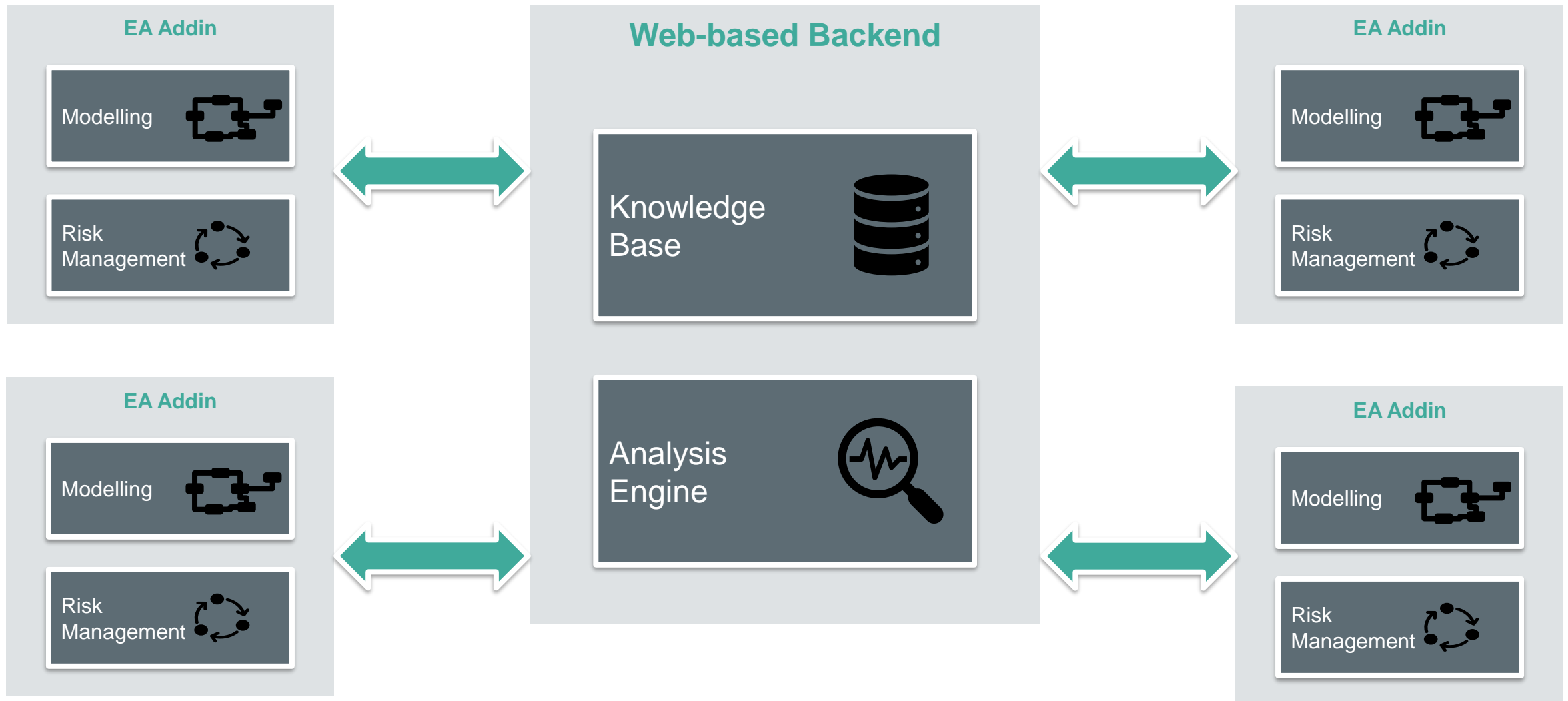
# VERSIONING

## Traceability of Analysis

- For each analysis a snapshot of the model is generated
- Snapshot + analysis reports is marked with date and time
- Stored in the model

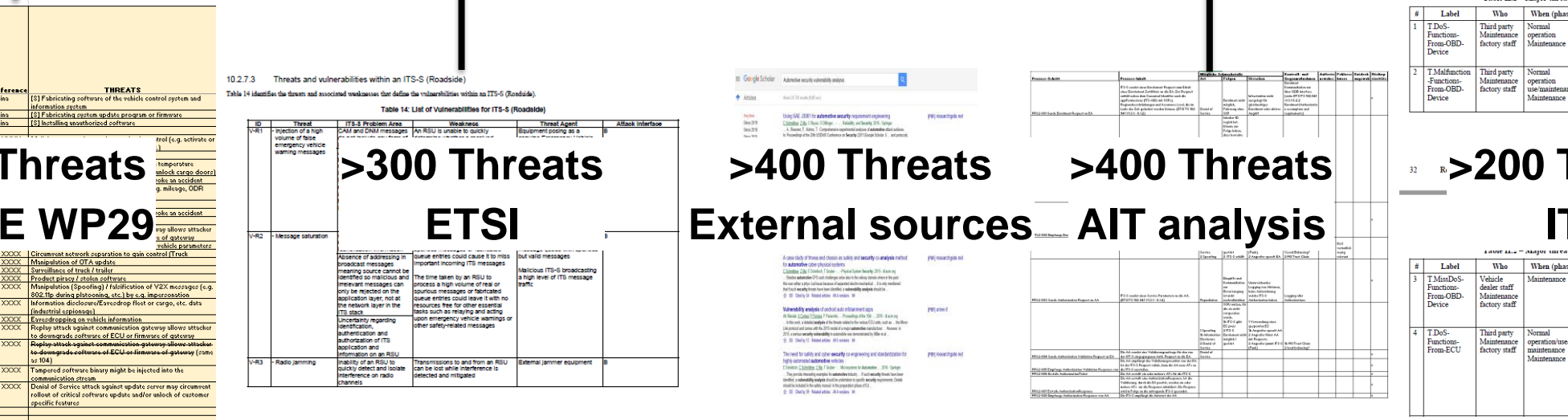


# THREATGET – COOPERATIVE THREATMODELING



**AIT** AUSTRIAN INSTITUTE  
LieberLieber 





24

# THREATGET

## Example



# THREATGET

## Summary



# THREATGET - THREAT ANALYSIS AND RISK MANAGEMENT

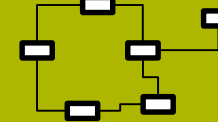
## Domain knowledge



## Cybersecurity expertise



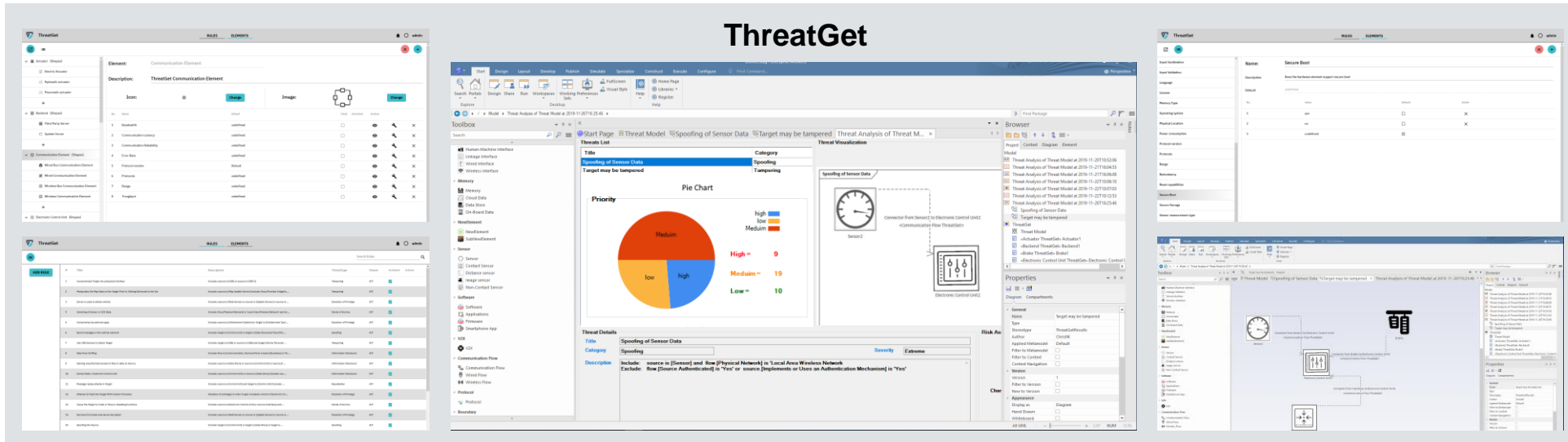
## Modeling knowhow



## Benefits



## ThreatGet



- **Automated** threat analysis based on current threat intelligence
- **Traceability** from threats to requirements
- **Continuous** process, integrated with model-based engineering

<https://www.threatget.com/>

# THANK YOU!

Thorsten Tarrach, Christoph Schmittner

