The Spy Who Threat Modeled

About Me

Currently: Security Engineer at PACCAR

Formerly: Security engineer across several industries

Education: Cyberspace Operations, AFIT; MBA, Washington State

Focus Areas: Vulnerability management, awareness and training, program development

*Disclaimer: Opinions my own

Vehicles Are Complicated

Concept

Requirements

Design & Architecture

Development & Implementation

Integration

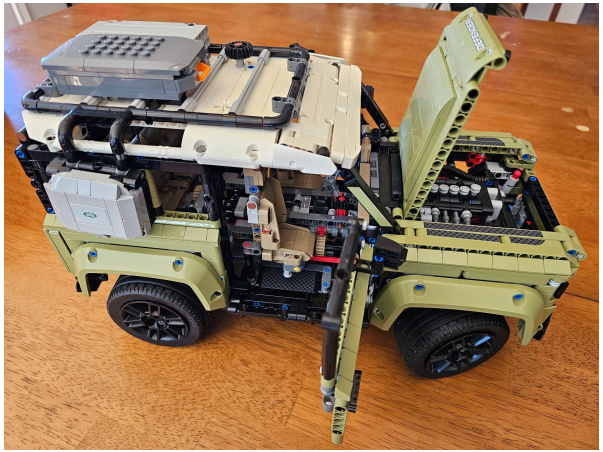
Testing

Validation

You Are Here

A Brief History

- 1885: Invented the car
- 1908: Ford Model-T
- 1975-1979: Engine Management Systems
- 2011: ISO 26262, Functional Safety of Road Vehicles
- 2015: Jeep Hack
- 2020: ISO 21434, Cybersecurity Engineering of Road Vehicles
- 2021: UNECE 155, Cybersecurity and Cyber Security Management Systems



Practical Damage Scenarios

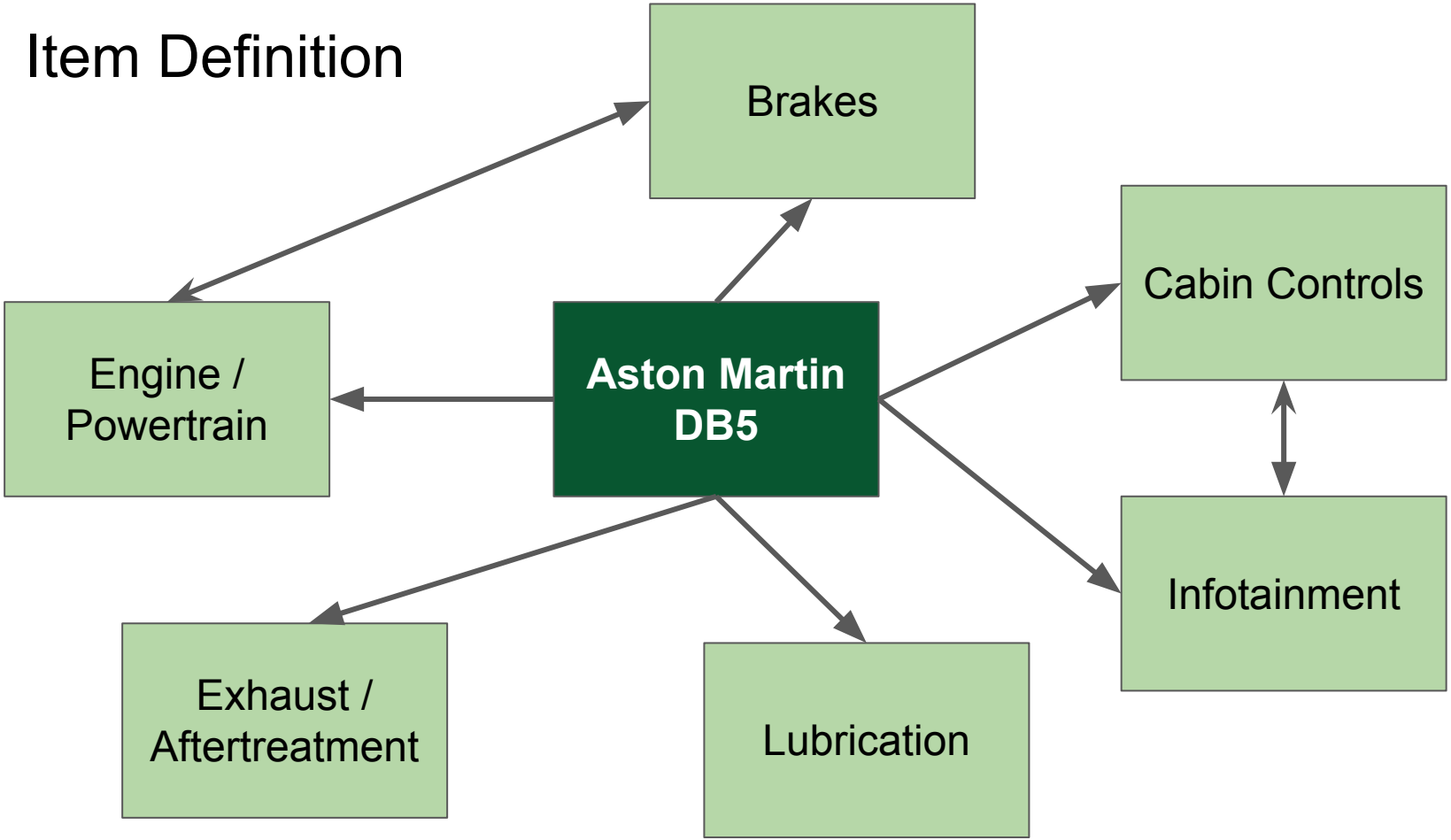
- Basic functionality: Go, stop, steer.
- Functional safety: Don’t crash. Have appropriate lights. Fail safe.
- Threat intelligence: Theft. Remote takeover. Abuse of driver privacy.

Damage Scenario: *Users*

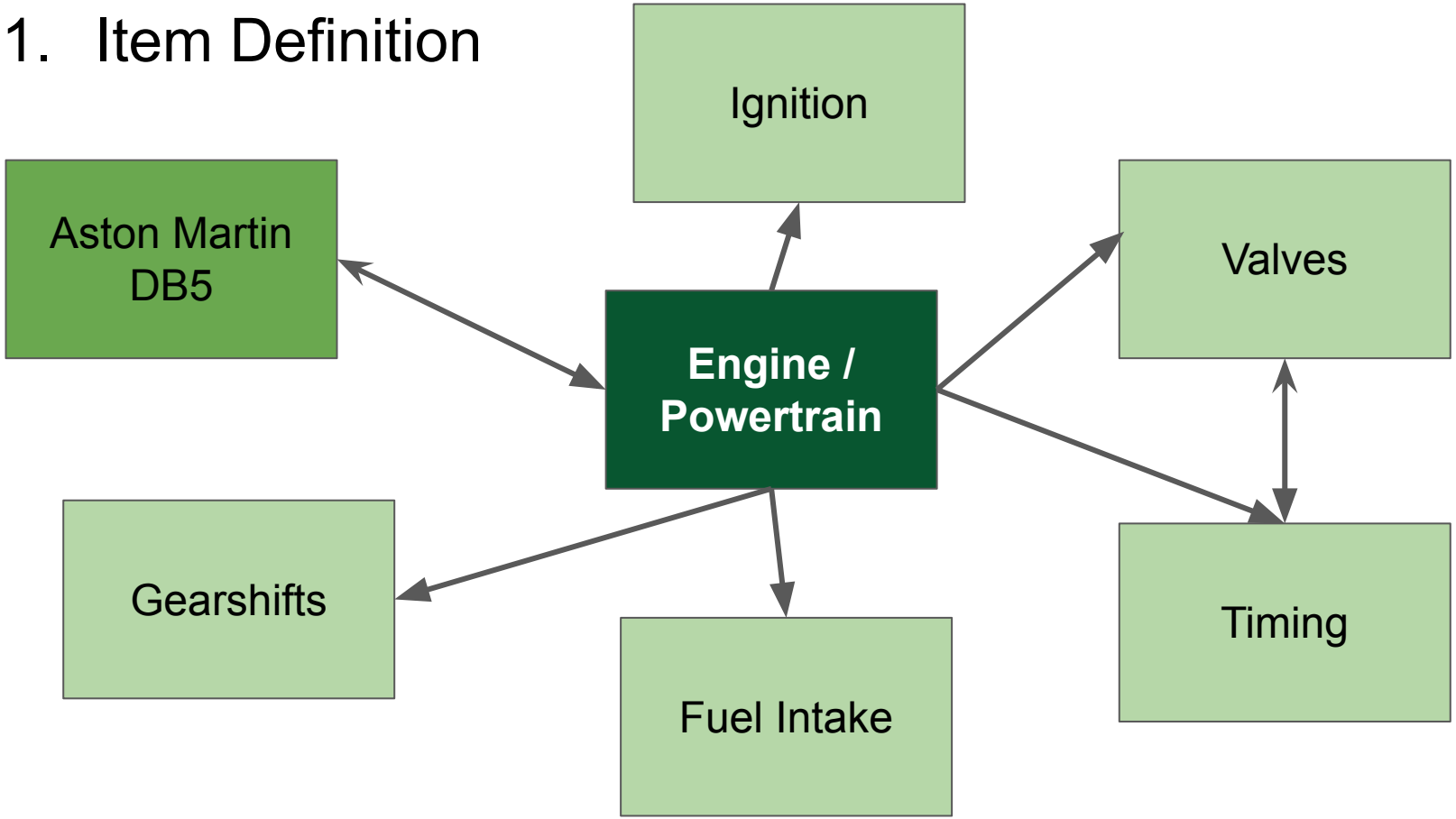
An Easy 8 Step Process

1. **Item Definition**
2. **Identify Damage Scenarios**
3. **Identify Threat Scenarios**
4. **Identify Impact Ratings**
5. **Attack Path Analysis**
6. **Attack Path Feasibility Ratings**
7. **Risk Analysis**
8. **Risk Treatment**

1. Item Definition

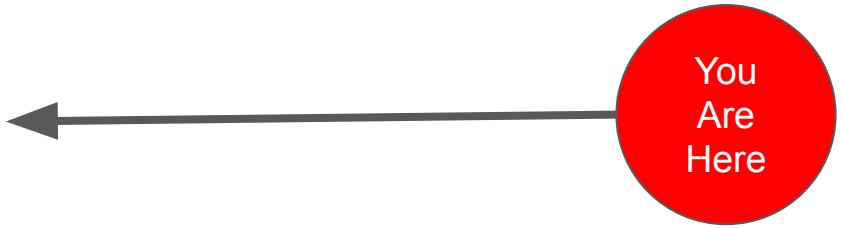


1. Item Definition



An Easy 8 Step Process

1. **Item Definition**
2. **Identify Damage Scenarios**
3. **Identify Threat Scenarios**
4. **Identify Impact Ratings**
5. **Attack Path Analysis**
6. **Attack Path Feasibility Ratings**
7. **Risk Analysis**
8. **Risk Treatment**



2: Identify Damage Scenarios

Getting Captured!

Resources stolen or destroyed!

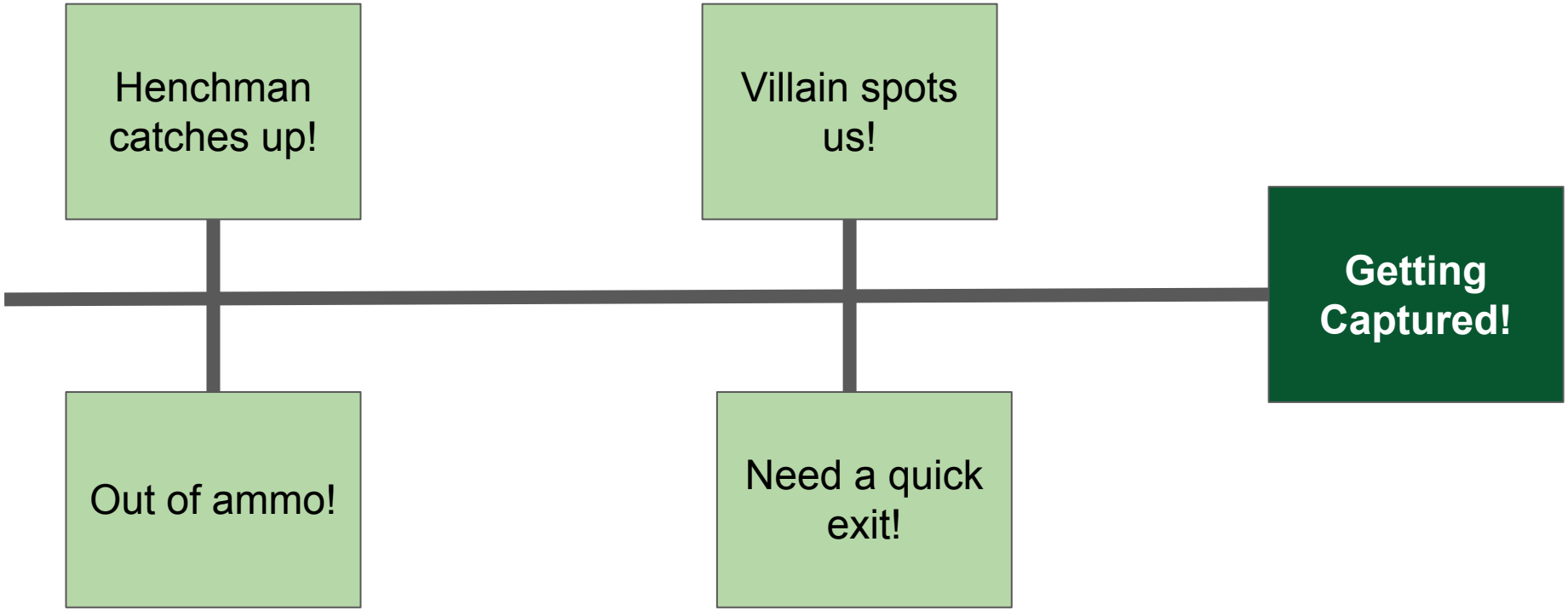
Losing the Villain's trail!

Giving information away!

An Easy 8 Step Process

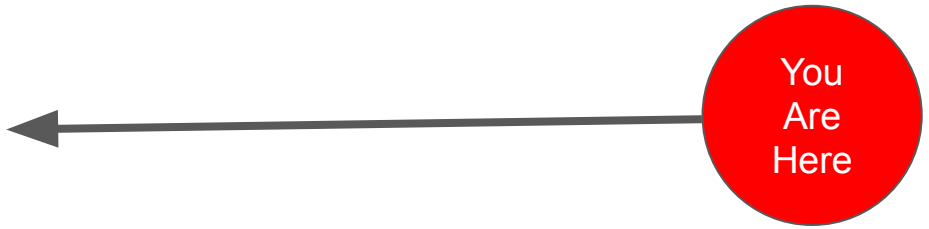
1. **Item Definition**
2. **Identify Damage Scenarios**
3. **Identify Threat Scenarios**
4. **Identify Impact Ratings**
5. **Attack Path Analysis**
6. **Attack Path Feasibility Ratings**
7. **Risk Analysis**
8. **Risk Treatment**

3: Identify Threat Scenarios



An Easy 8 Step Process

1. **Item Definition**
2. **Identify Damage Scenarios**
3. **Identify Threat Scenarios**
4. **Identify Impact Ratings**
5. **Attack Path Analysis**
6. **Attack Path Feasibility Ratings**
7. **Risk Analysis**
8. **Risk Treatment**



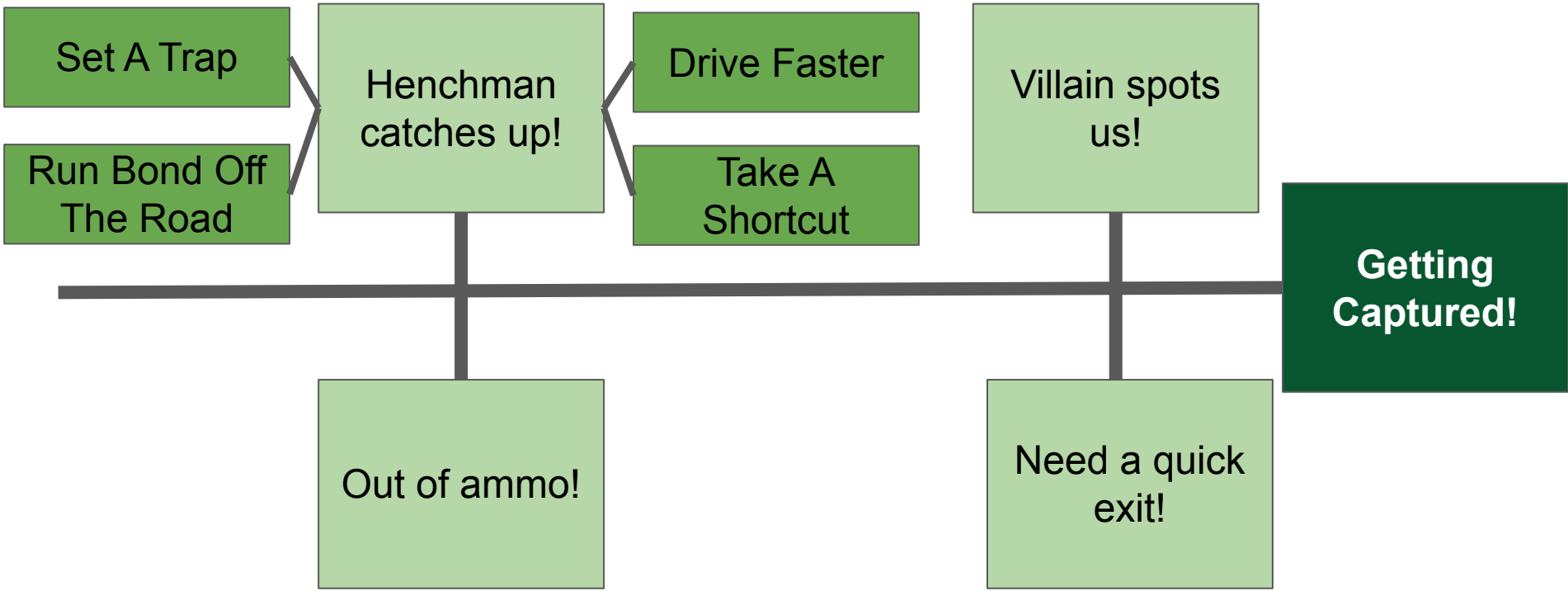
4: Identify Impact Ratings

Safety	Severe; Bond could face serious or fatal injuries!
Operation	Severe; Engines don’t like bullet holes
Privacy	Moderate; Bond’s only PII is location & plate
Financial	Moderate; Bond has significant means

An Easy 8 Step Process

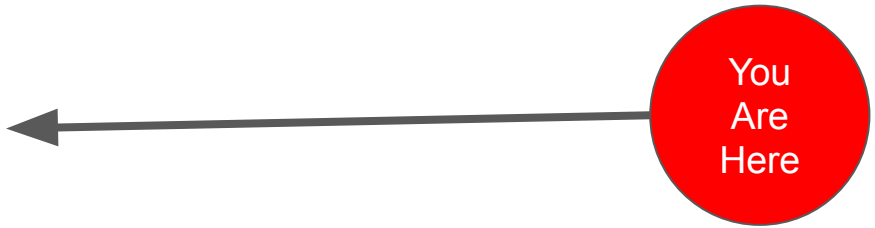
1. **Item Definition**
2. **Identify Damage Scenarios**
3. **Identify Threat Scenarios**
4. **Identify Impact Ratings**
5. **Attack Path Analysis**
6. **Attack Path Feasibility Ratings**
7. **Risk Analysis**
8. **Risk Treatment**

5: Attack Path Analysis



An Easy 8 Step Process

1. **Item Definition**
2. **Identify Damage Scenarios**
3. **Identify Threat Scenarios**
4. **Identify Impact Ratings**
5. **Attack Path Analysis**
6. **Attack Path Feasibility Ratings**
7. **Risk Analysis**
8. **Risk Treatment**



6: Attack Feasibility Analysis

	Time	Expertise	Knowledge	Window of Opportunity	**TOTAL RATING**
Take A Shortcut	Under 1 Day: 0	Proficient: 3	Restricted: 3	Moderate: 4	**10: HIGH**
Drive Faster	Under 1 Day: 0	Expert: 6	Public: 0	Unlimited: 0	**6: CRITICAL**
Set A Trap	Under 1 Month: 4	Proficient: 3	Restricted: 3	Easy: 1	**11: HIGH**
Run Bond Off The Road	Under 1 Day: 0	Expert: 6	Public: 0	Difficult: 10	**16: MEDIUM**

An Easy 8 Step Process

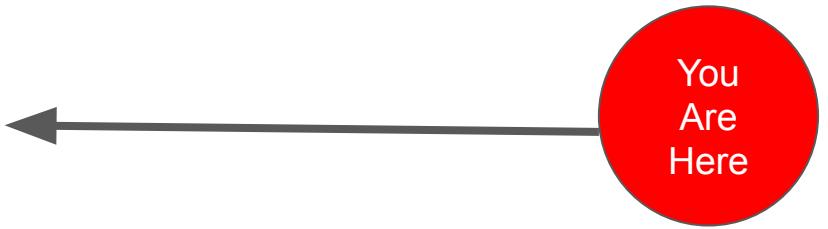
1. **Item Definition**
2. **Identify Damage Scenarios**
3. **Identify Threat Scenarios**
4. **Identify Impact Ratings**
5. **Attack Path Analysis**
6. **Attack Path Feasibility Ratings**
7. **Risk Analysis**
8. **Risk Treatment**

7: Risk Analysis

	Low	Medium	High	Critical
Critical				**Drive Faster**
High		**Take A Shortcut**	**Set A Trap**	
Medium				
Low		**Run Off The Road**		

An Easy 8 Step Process

1. **Item Definition**
2. **Identify Damage Scenarios**
3. **Identify Threat Scenarios**
4. **Identify Impact Ratings**
5. **Attack Path Analysis**
6. **Attack Path Feasibility Ratings**
7. **Risk Analysis**
8. **Risk Treatment**



8: Risk Treatments

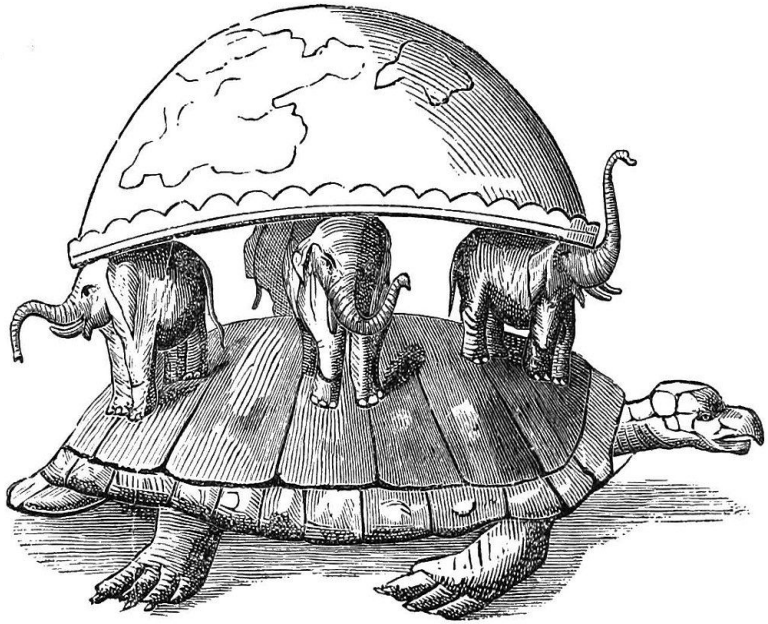
HIGH	**Henchmen take a shortcut**	• Radar scanner behind mirror • Radar screen in dash
CRITICAL	**Henchmen drive faster**	• Smoke screen from exhaust • Oil jet and caltrops
HIGH	**Henchmen set a trap**	• Radar scanner behind mirror • Radar screen in dash
MEDIUM	**Henchmen run Bond off the road**	• Tire slasher

TARAs All The Way Down

Q: What needs a TARA?

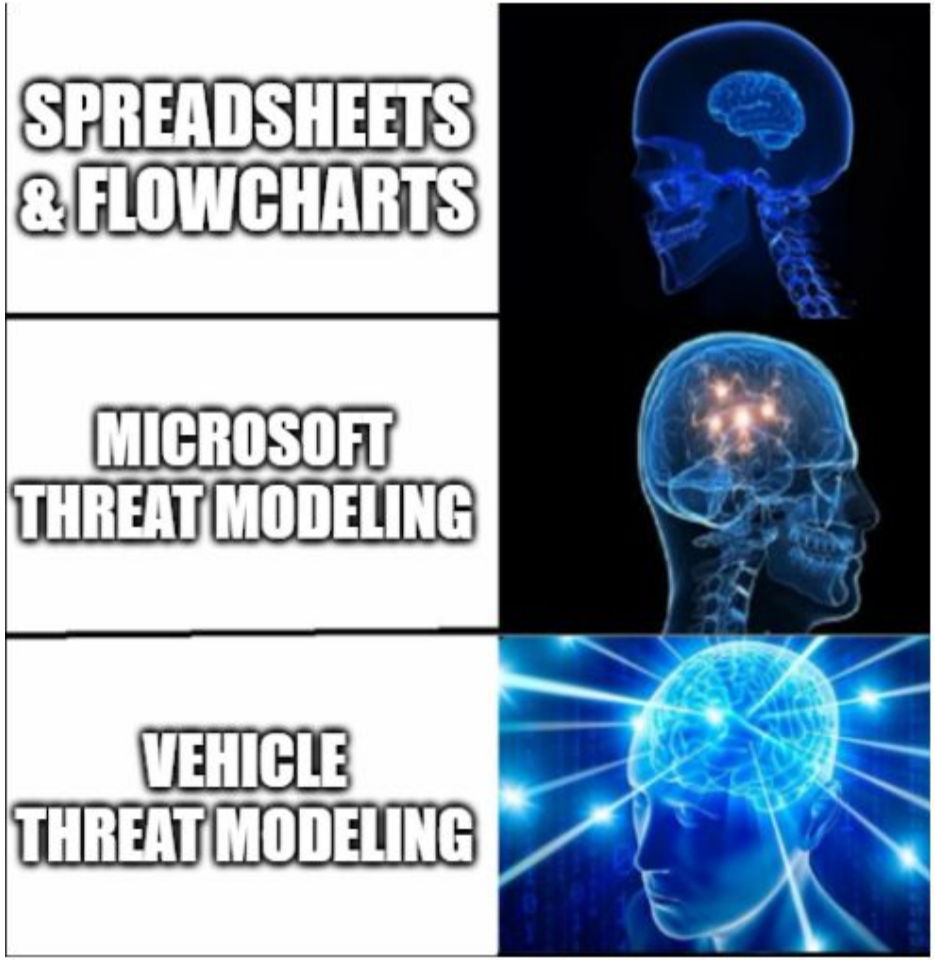
A: Any component that can impact the security risk!

Practically: ECUs are interconnected; be methodical and consistent in approach



Tooling

- Pros
  - Automation
  - Consistency
  - Repeatability
- Cons
  - Steep learning curve
  - Customization required
  - Needs extensive working knowledge



“Easy” Wins

- Disable unused interfaces
- Seperate devices of different trust levels
- Use cryptography properly
- Lock down supporting systems
- Use diagnostics and monitoring wisely

Conclusion

- Don’t try to threat model everything at once, break it down
- Don’t *overthink* it
- Get help from different disciplines
- Threat modeling is a continuous process
- Perfect is the enemy of good enough