Risk Management for Automotive Cybersecurity

Bill Mazzara – Global Vehicle Cybersecurity Technical Fellow – FCA US LLC

Contents :

November 7, 2018

The Auto Industry continues to add connectivity to vehicles to satisfy the customer's insatiable appetite for technology, but cars are not just insecure endpoints on some computer network as some have portrayed. Vehicle Cybersecurity is forging a new field of Product Cybersecurity. The underlying challenges of forging this new field is to choose adequate Cybersecurity. Unlike enterprises Product Cybersecurity must fit into smaller spaces on tiny budgets.

The SAE is at the forefront of this new field working proactively to develop standards of Risk based methodology to meet the growing demands. Working collaborative with ISO, best processes are being established for industry wide preparedness for the inevitable. Risk policies must be established for processes of a Risk Based Methodology based on Risk Assessment.

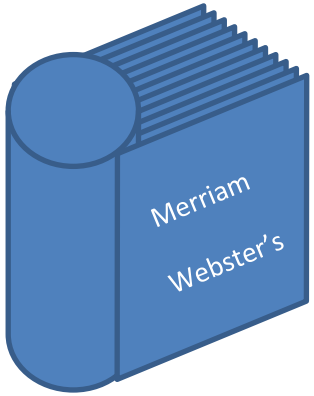
In order to achieve Product Cybersecurity Risk Assessment, Enterprise Cybersecurity Risk Assessment Methods must be reworked and used in a consistent manner across the Industry. ISO21434 proposes common interpretations of Methods leveraging the existing wealth of knowledge in Asset Categorization and assessment of Impact and Attack Potential in order to estimate Risk presented to products.

Bill Mazzara, the technical fellow of global vehicle cybersecurity regulatory compliance at FCA US LLC, serves on the SAE/ISO joint Working Group for automotive security. He is also the SAE Vehicle Electrical System Hardware Security Subcommittee Chair.

Having begun his career as a test engineer during the infancy of the connected car, Mazzara has witnessed and been a driving force in the evolution of the field being granted 27 related patents in the process. As it became apparent that the lack of cybersecurity was an unfortunate oversight of the connected car, Bill became part of the solution. Mazzara served on the response team charged with addressing what is widely considered one of the automotive industry's first cybersecurity incidents against a passenger vehicle, the incident chronicled in 2010 study by researchers from the Universities of California San Diego and Washington.

A Certified Information Systems Security Professional(CISSP), Mazzara holds a bachelor's degree in Electrical Engineering from the University of Notre Dame in addition to advanced degrees in wireless communications and business administration.

This presentation sets forth a proposed application of SAE/ISO21434



RISK - **possibility of loss or injury : Peril.**

Cybersecurity - **measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack**

Product Cybersecurity is the protection of digital information systems within a product from malicious use or access.

So, What is a Product?

A product is defined as something that is mass produced.
. millions of copies, only one or a few users per copy

This is distinct from an Enterprise

For Enterprise Cybersecurity the administrators is managing the one copy.
An Enterprise is a multiuser environment.

One Copy millions of users

Adequate Cybersecurity

- **efficient use of the right Cybersecurity mechanisms**
- **within a limited budget**
- **minimizing impacts on usability.**
- **But not Excessive**

Adequate Cybersecurity is achieved by developing a risk based methodology of product design.

Risk Based Methodology

- **A Generic reusable method of Risk Assessment**
- **Used at all phases of development**
- **Used to for maintenance over a Product's Lifecyle**
- **Must Judge Risk questions a within or above tolerance**

Risk Tolerance: a description of Risk above which action is mandatory by policy to mitigate the risk.

Risk Caution: a description of Risk less than Risk Tolerance but above which policy requires monitoring to be established to ensure assumptions made as a part of the assessment hold true.

Organization sets policy to …

a) Define and scope the risks associated with Cybersecurity threats of interest to their products and
b) Outline the basic principles management will follow and will expect to be followed to manage the risks associated with Cybersecurity of their products.

Policies

- **proactive**
- **clear objective decisions**
- **cohesive strategy of Cybersecurity**
- **creates a yardstick by which the quality of a solution may be measured**

Written to meet the needs of each product uniquely and cannot be standardized.

Established policies allow an organization to make decisions without the pressures and influences of any particular situations.

Objectives

Universal

A Universal method of risk assessment is necessary for the industry

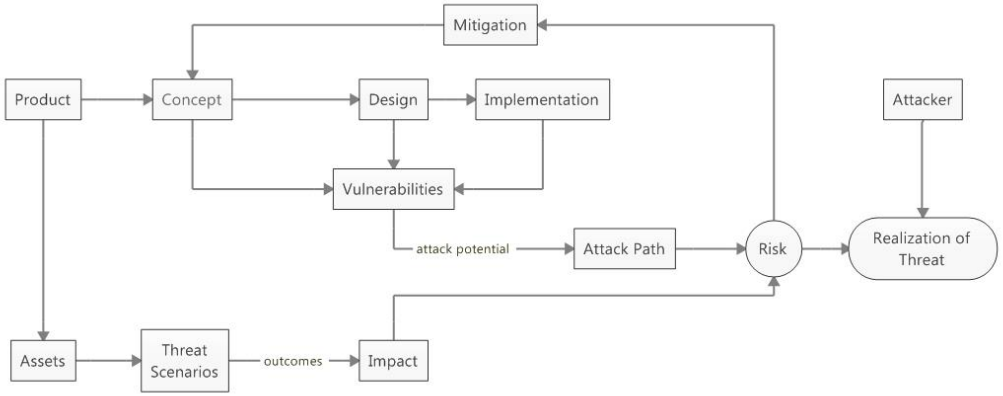
- Information Sharing across the industry
- Reuse of solutions and strategies

Extensible

Universal does not mean uniform.

The intricate details of the method will need to vary to accommodate distinctions in :

- Risk tolerance of use cases
- Purpose of products
- Environment of operation



Common Scales throughout the method

- Singular and objective in nature
- Facilitating a rating of only one attribute of the risk assessment.
- Independent and uncorrelated to any other scale used within the Risk Assessment.

utilize numerical scales

a common range (i.e. 0 to 5) of comparable distributions.

"Lower the Better" for the customer.

favorable outcomes for Customers at the lower end of the value range specified for the scale.

At times can require a rephrasing of the question asked by the rating dimension

Allows for flexibility in the number of dimensions used

New (uncorrelated) dimensions may be added to an assessor's method of assessment without modification of past assessments or redistribution of other rating scales.

Weighting of dimensions is achieved in the selection of scales.

The eliminating property of Zero must be preserved.

example : a Vulnerability which requires a high level of expertise to exploit should receive a low numerical rating because such is a "better" situation for the customer. So instead the dimension should be described as Ease of which a Vulnerability is exploitable resulting in a sensibly low rating.

example : if the proximity of attack necessary to conduct an exploit is "weighted" more than the expertise necessary, a low (better) rating of proximity might be "within the vehicle" while a low (better) rating might be "average technical expertise". Under this example any distance of remote access even of short range would score a higher attack potential than a vulnerability that requires average technical expertise to exploit. A vulnerability must exhibit aspects which would require some specialized expertise to exploit to compare to a remote exploit of even short range.

In mathematics, a geometric progression, also known as a geometric sequence, is a sequence of numbers where each term after the first is found by multiplying the previous one by a fixed, non-zero number called the common ratio.

For example, the sequence 2, 6, 18, 54, ... is a geometric progression with common ratio 3.

– [Wikipedia – Geometric Sequence]

> *example :* if the equipment cost necessary to exploit a vulnerability is rated according to a scale {<$100, <$10,000, <$1,000,000} the expertise necessary to exploit a vulnerability should be rated in terms of weeks of study necessary but on a similar distribution e.g. {10wks (a self study), 100wks (a certificate or degree program), 1000wks (a career expert)} *Note :* remember scales should be rated lower the better for the customer so each of these example distributions are listed in descending ranking (i.e. 3.2,1) Higher cost and increased skill necessary to exploit a vulnerability are both "better" for the customer.

Geometric Progression diminishes the weight of an incremental difference at each progressive level of the scale

Examples : , a hundred dollar difference in a tool, a month of study to learn certain expertise, minor scratches compared to complete destruction.

Comparative examples

Product Failure Risk – i.e. Instances per thousand vehicles, or Parts per Million

Investment Risk- i.e. rates of return

Geometric Mean

Use a geometric mean for all calculations of averages.

Geometric Mean is the Nth Root of a product of N numbers

$$\sqrt[N]{\prod_{n=1}^{N} d_n}$$

Where: d_n is a dimension within the series of N dimensions

The Geometric Mean is calculated in Excel using the following Formula :

=POWER(PRODUCT(<<RANGE>>),1/COUNT(<<RANGE>>))

where <<RANGE>> is the range of values to be calculated e.g. "A1:A10"

- Capable of comparing ratings of disparate number of dimensions
  - Allows Risk Assessment Methods to be used only in part if availability of information is an issue
  - Allows expandability if the type of information suits the need.
- Disqualifies any item that is rated a zero on a single dimension,
  - interpreted as path that is impossible.
- Using dimensions rated along common scales of magnitude and distribution with a geometric mean the result is a similar scale of interpretation throughout the assessment system.

- ***A TARA is a Cybersecurity FMEA***

- Geometric Mean is also selected due to the similarity to FMEA
  - a familiar process to automotive engineers.
  - the product of many dimensions

A reminder : an FMEA rates failure modes through the multiplication of Severity, Occurrence, Detectability

Logical Graph Theory

The Risk Assessment Method uses logical combinations of ratings as follows:

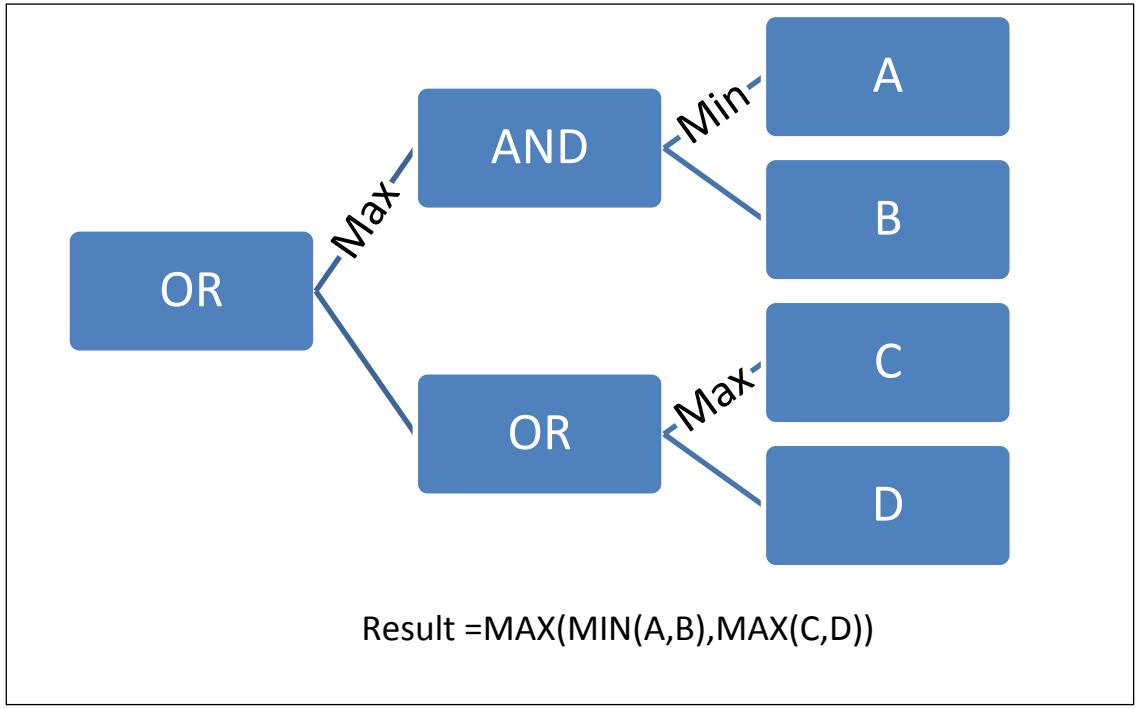
a logical AND as the minimum of the set ratings

a logical OR as the maximum of the set of ratings

Use of scales of similar direction of meaning (i.e. "Lower the better") allows this

Makes use of principles of least resistance and defense in depth.

Makes an Attack Tree and a Fault Tree very similar, leveraging familiar Engineering Concepts and skills



The classical formula for risk : Impact X Likelihood

Risk is determined as a function of (a) feasibility/likelihood (b) its impact on the road users.

Universal Definition

- At any point in a Cybersecurity Lifecycle
- during any phase of the product life cycle
- Useful in any environment or use case

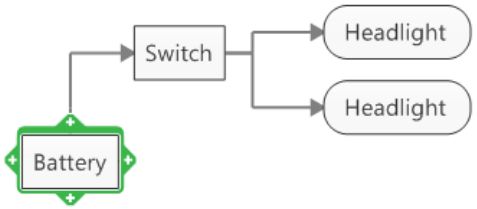
Determined from the current understanding of the risk factors.

The objective of Risk assessment is to determine where risk lies with respect to applicable Governance Policies

Risk Tolerance: a description of Risk above which action is mandatory by policy to mitigate the risk.

Risk Caution: a description of Risk less than Risk Tolerance but above which policy requires monitoring to be established to ensure assumptions made as a part of the assessment hold true.

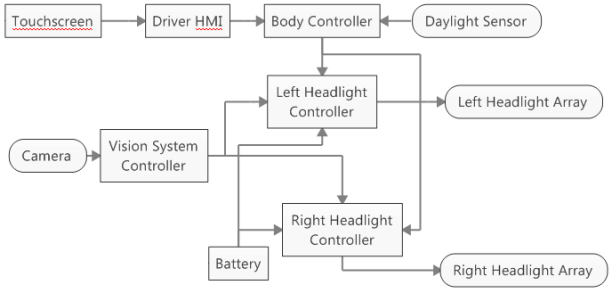
Legacy Headlight System Diagram:



Time Happens…

- Light bulbs aren't good enough anymore; demand for LEDs
  LED arrays require electronic controllers… Now its Cyber-Relevant
- Modern Headlight systems are Automatic
  - This introduces a daylight sensor and HMI
- Modern systems require a left and right controller to "balance" lighting … Complexity Increases
- Modern Headlight systems are predictive, … more sensors.
  - Steering sensors, Oncoming traffic detection … a Camera

Futuristic Headlight System Diagram :



$$I = \max(S, P, O, F, X)$$

where

S = Safety Impact(ASIL QM =1, ASIL A=2 through ASIL D = 5)

Notice the only way to score a 5 is ASIL D Impact

P = Privacy Impact (Non linkable Data = 1, Personally Linkable = 2, nonregulated/regulated = 3/4)

O = Operational Impact (Indiscernible =1 …Total Vehicle Failure = 4)

F = Financial Impact (Negligible=1…Personal Bankruptcy = 4)

X = Extended Impact as deemed appropriate by assessor(Remember to keep a similar scale)

- Analyze the impacts of the outcomes of threat scenarios irregardless of methods
- Threat Scenarios may be theorized, demonstrated, observed on other products…
- Only Threat Scenarios with quantifiable outcomes are of interest.

Threats Scenarios are:

Unintended Acceleration
Failure of Brakes
Theft of a credit card number

Threat Scenarios are not :

A Man in the Middle
Root Access
Time of Check / Time of Use

- There is no harm in proposing Threat Scenarios which cannot be realized.
  The fact that the threat cannot be realized will be wrought out in the process

Headlights

- Legacy system has safety and operation Impact (Unintentionally turning off headlights)
- Futuristic System now has potential Privacy Impact (depending on the correct use of the Camera)

- The Attack Paths of a Threat Scenario have to be decomposed into distinct vulnerabilities (vulns).
- The chain of vulns easiest to exploit to reach the goal is most interesting.
- The rating is the inverse of the attack potential needed to exploit each vuln. (Feasibility)
- Rate each vulnerability without regard for the other vulns in the Attack Path.

Use the attack potential dimensions of ISO18045: Time (Typically not relevant)
Expertise
Knowledge of Target
Window of Opportunity
Equipment

But change to geometric scales represented by 1..5. (remember Lower is better for the Road Users)
Clear examples of some awkward questions…e.g. Expertise is not higher if its harder

Allows a single attack potential score for a vuln using the Geometric Mean

$$L_v = \sqrt[n]{\prod_1^n AP_d}$$

where :
L = Likelihood — v = each vulnerability
AP = Attack Potential Rating — d = Each Attack Potential dimension based on ISO18045
n = the number of Attack Potential Dimensions(d) used by the assessor to rate the Vulnerability (v)

- Object Oriented Vulnerability Analysis
- The granularity to which an attack path may be decomposed is flexible
- In simple cases an entire attack path may be rated under a single rating of attack potential.
- Under complex scenarios detailed attack trees may be drawn.
- This system is also extensible. beyond dimensions spec'd in ISO18045
    - I like to add Proximity Required (a distinct perspective or Window of Opportunity)
        - 1 = Inside an otherwise running car
        - 2 = physical access
        - 3 = Short Range Remote
        - 4 = At least one time encountered
        - 5 = Global Range Remote
- Allows operation with incomplete knowledge
    - Remember a property of the geometric mean allows comparison of series of differing dimensions

Headlights

- Malware Driver HMI Device has unauthorized permission to turn off headlights(AP=4)
- Malware in the Vision System Controller has unauthorized permission to turn off headlights(AP=3)
- Crafted input to the Camera allows Malware to be loaded on to Vision System Controller(AP=2)
- A Malicious service tool can load malware on the Vision System
- Malware in the Headlight controller prevents the vision system from serving other needs(AP=4)
-

Review of what we have

- Threat scenarios for which the impact of each was characterized
- Vulnerabilities independently rated by attack potential needed for exploit

Develop one or more Attack Tree for each Threat Scenario

String together exploitable vulnerabilities to reach the goal of the threat scenario

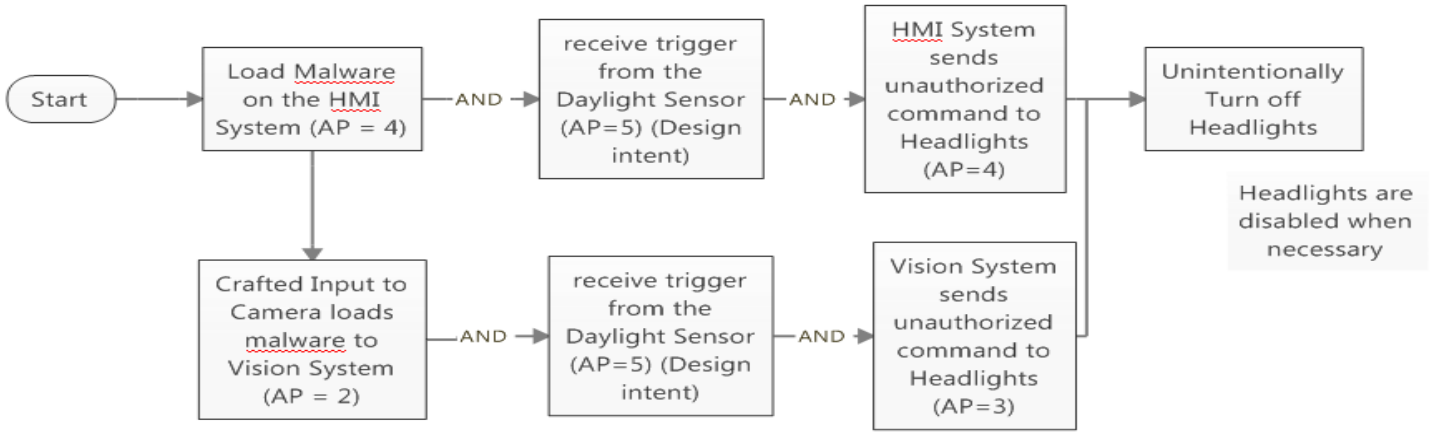
Attack Tree : a Logic string(ANDs & ORs) of exploitable vulnerabilities and/or conditions to achieve the outcome of the threat scenario.

Net Attack Potential of an attack tree can be determined using Logical Graph Theory

MAX & MIN.

A single rating of Likelihood (i.e. attack potential) for a threat scenario is the maximum (logical OR) of the net attack potential for each attack tree developed for that threat scenario.

Headlights



Ignore the Threat Source.

- Over the long life of Automotive products, we cannot know what people will do
- Every year disclosures prove just how willing attackers are to accomplish goals

Threat Source information is only relevant when analyzing a field Incident

Real Attackers are involved

Attackers are also characterized by Attack Potential (ISO18045 : Expertise, Knowledge of Target, etc.)

Note : NOT the inverse of attack potential

Remember lower is better for the Road Users

Less Capable Attackers are beneficial

A prediction of an eminent threat :

Attack Potential of Threat Source = Net Attack Potential of an Attack Tree

Note : Under these scenarios time to exploit might also be relevant in the attack potential calculations of both the threat source and the vulnerability

$$R = \sqrt[2]{I * AP}$$

Where
R= Risk
I = Impact
AP = Attack Potential

But it is mostly meaningless

Useful to rank threat scenarios developed for an assessment
Useful to compare assessments of distinct products

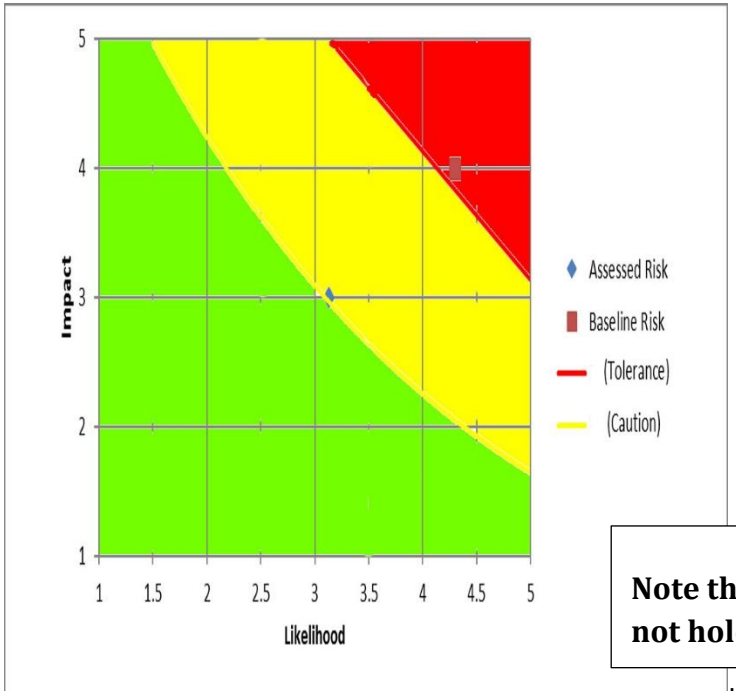
Headlights

Risk = 4

A Risk Report must

- be tailored to the risk management policies of the receiving organization
- Not universal for all audiences.
- Present the risk question which scoped the assessment
- indicate the Risk determined with respect to the Tolerances of the requesting organization.

Note the range and magnitude of the scales used are irrelevant once reported in terms of tolerance to policy



The example risk chart illustrates that the Risk was first assessed (baselined) to be above tolerance according to the governing policy which is a linear designation of tolerable risk , then upon mitigation the new assessed risk is found to be acceptable to tolerance but still within the cautionary range defined by the Governing Policy

Note that Tolerance and Caution thresholds need not hold to a strict grid pattern or linear functions.

The risk assessment is iterative in nature,

improving the understanding of risk of a threat scenario upon each iteration,

there is not specific order in which the assessment must be executed.

For illustration of the iterative nature of risk assessment the following events at distinct points in a product lifecycle are presented:

Concept Risk Assessment

1) Asset Analysis
2) Identify Failure Modes
3) Impact Analysis
4) possible attack paths that can realize proposed scenarios
5) Estimation of Attack Potential of Vulnerabilities that make up the attack paths
6) Calculation of risk

Test Result Risk Assessment

1) Vulnerabilities reported in test results
2) individually asses each for Attack Potential
3) Vulnerabilities are chained together to form attack paths which result in meaningful threat scenarios
4) Impact analysis on the outcome of the attack paths
5) Assets affected identified
6) Calculation of risk

Incident Risk Assessment

1) The Attack Path of the Incident is documented
2) Impact Analysis is performed
3) Assets affected identified
4) Attack Potential of Vulnerabilities that make up the attack path are assessed
5) Calculation of risk
6) Attack Potential of Attacker analyzed
7) Prediction of eminent threats might be made

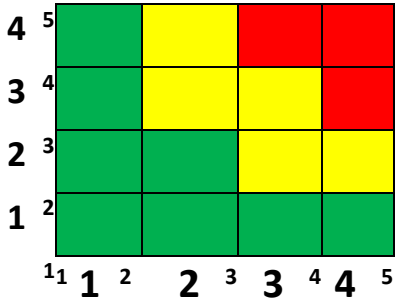
The proposed method for calculation facilitates consistency and comparison of results among the numerous parties of the Auto Industry operating in disparate environments and with various use cases

- Consistent and Comparable
- Cannot be overly simplified

The ease of a simple table look up method is desirable

Calculations and assumptions must be made on behalf of the assessor to create this

Only achievable under the context of a single organization with its respect environments and use cases in alignment with organizational policies



Some Encourage a “Heat Map” as shown above

You end up with this you can’t start with it.

Numerical Methods are superior more appropriately dealing with ratings “between the lines”

- An army of new Automotive Cybersecurity Engineers is not necessary
- This Risk Assessment Method uses concepts in common with Familiar tools
  - Failure Mode Analysis
  - Fault Tree Analysis
- The math is not hard…
- Can be accomplished at the same time as Failure Mode analysis for other reasons
- The Expertise of the product function is more important than the cybersecurity Expertise
  - No need to analyze the motivation of the attack

Build Cybersecurity Risk Assessment into the typical analysis performed by an engineer for the development of a product

Risk Assessment can be performed for every choice made at every level of abstraction

Put this tool into the tool belt of every engineer.

Asset	Confidentiality Rating	Confidentiality Notes	Integrity Rating	Integrity Notes	Availabilty Rating	Availabilty Notes	Composite Rating
	0						0

Vulnerability	Exploitability Rating	Exploitability Notes	Knowlegde of Target Rating	Knowlegde of Target Notes	Window of Opportunity Rating	Window of Opportunity Notes	Proximity Rating	Proximity Notes	Equipment Rating	Equipment Notes
	0									

Impact Analysis								Attack Pattern (1..N)		
Financial	Notes	Operational	Notes	Privacy	Notes	Safety	Notes	Impact Severity (MAX)	Summary	Attack Potential	Single Risk Level
								0		0	0

Cover Sheet | Assets | Vulns | Impact | Risk | Summary

Ready

The most Important part of a TARA is the notes

- This Presentation has been an application of SAE/ISO 21434 – Road Vehicles : Cybersecurity Engineering
- As of the publication of this presentation the document is in Committee Draft accepting comment through Nov 17, 2018

High Level Summary:

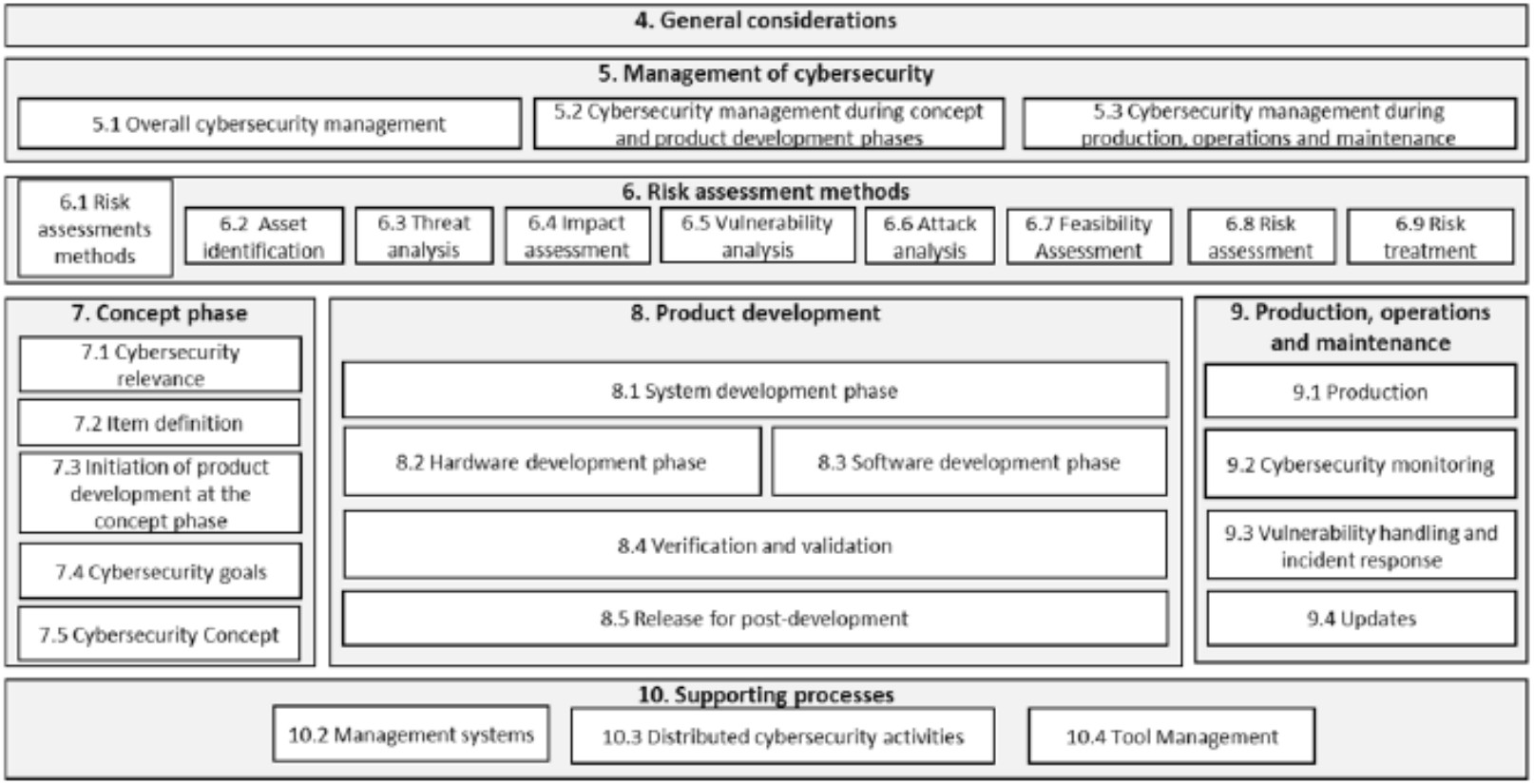


Figure 1 from SAE/ISO 21434 “CD” Draft distributed Sept 21, 2018

November 7, 2018