2025 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE
MUNICH, GERMANY
OCTOBER 14-15, 2025

A pragmatic Approach to apply HEAVENS Threat-Level for Attack Feasibility Determination as per ISO/SAE 21434 Recommendations RC-15-11 and RC-15-12

Clemens Röttgermann, *exida.com GmbH*, Munich, Germany (clemens.roettgermann@exida.com)

Frauke Blossey, *exida.com GmbH*, Munich, Germany (frauke.blossey@exida.com)

Tanja Schülting, *exida.com GmbH*, Munich, Germany (tanja.schuelting@exida.com)

Abstract - Security Analysis for Electrical/Electronic (E/E)-Systems, their sub-systems and components started to become common practice. This includes analysis of TIER2 products such as System on Chips (SoC's), complex Soft IP and Software. We were confronted with the challenge to assess the adequacy of a variety of Threat-Modelling approaches when running ISO/SAE 21434 assessments [1]. We observed as common practice that organizations apply Healing Vulnerabilities to Enhance Software Security and Safety (HEAVENS) [2] for Component Security-Analysis (C-SA) or Threat-Analysis and Risk-Assessment (TARA) in context of ISO/SAE 21434. We therefore decided to challenge the claim that the HEAVENS [2] Threat-Level (TL) can be used in equivalence with the ISO/SAE 21434 RC-15-12 Attack Potential approach to rate the Attack Feasibility (AF). This paper makes a pragmatic and empirical proposal on how to achieve this. The proposal is used to perform a systematic comparison. The results demonstrate that using HEAVENS TL in combination with proposals from this paper seems appropriate to achieve results which are comparable to Attack Potential approach as recommended in [1] RC-15-12.

Keywords – ISO/SAE 21434, Threat-Analysis and Risk Assessment, Component Security Analysis, , Attack Feasibility, HEAVENS, EVITA, Attack Potential

I. INTRODUCTION AND MOTIVATION

Security Analysis for Electrical/Electronic (E/E)-Systems, their sub-systems and components started to become common practice. This includes analysis of TIER2 products such as System on Chips (SoC's), complex Soft IP and Software. One motivation is the understanding that Security Analysis (of called threat-modeling) substantially contributes to the reduction of Cybersecurity risks. It complements other essential elements such as appropriate verification, validation, vulnerability monitoring and Cybersecurity Management Systems which ensure that Cybersecurity is considered for the relevant phases of the lifecycle from concept, development, production, operation and maintenance until decommissioning. The other motivation is driven top-down from regulations such as UNECE WP29 Nr. 155 which results in ISO/SAE 21434 process and product compliance evidence. Those get requested throughout the supply chain. The ISO/SAE 21434 requests Security Analysis by the Work-Products Threat-Analysis and Risk-Assessment (TARA) and the Vulnerability Analysis which is mostly required for ISO/SAE 21434 component development and continuously throughout the product lifecycle. TARA and Vulnerability Analysis refer to ISO/SAE 21434 clause 15 methods. Despite their different names they share a common methodology. In this paper we refer by Component-Security-Analysis (C-SA) to the Vulnerability Analysis on ISO/SAE 21434 Component level which is performed during development and/ or post-development phase.

The authors were confronted with the challenge to assess the adequacy of a variety of Threat-Modelling approaches when running ISO/SAE 21434 assessments. Whereas the ISO/SAE 21434 does not specify exactly how to determine the impact rating and the Attack Feasibility (AF) rating. However, does ISO/SAE 21434 provide recommendations. This paper focuses on the AF rating. The ISO/SAE 21434 recommends three methods which are to either use the Common Vulnerability Scoring System (CVSS) 3.1 exploitability parameter, the Attack Potential approach [3] (referenced and adapted in [1] RC-15-12). Note that the Attack Potential approach [3] is as well applied by [4].

The authors observed as common practice that organizations apply Healing Vulnerabilities to Enhance Software Security and Safety (HEAVENS, [2]) for C-SA or TARA in context of ISO/SAE 21434 [1]. We therefore decided to challenge the claim that the HEAVENS Threat-Level (TL) can be used in equivalence with the ISO/SAE 21434 RC-15-12 Attack Potential approach [1] to rate the Attack Feasibility.

Let's first take one step back. Consider that determination of risk (on item level) always requires two domains: the Impact Level (I) and the AF. In [1] gets the Risk (R) defined as a function of both:

$$R = F(I, AF) \tag{1}$$

This is done similar in [2] although the used names are different. In this case the Security Level (SL) is defined as a function of Impact Level (IL) and the Threat-Level:

$$SL = F(IL, TL) \tag{2}$$

There are other differences to mention:

- Instead of a Risk per [1] S, F, P, O (Safety, Financial, Privacy, Operational) impact domains does [2] define a "HEAVENS value" to determine the Security Level. This HEAVENS value is based on a weighted impact sum which gives safety and financial impact a weight of 10 compared to privacy and operational (Figure 1).
- Financial impact of [2] refers to financial impact on the organization whereas financial impact in [1] refers to the financial impact on the road user.

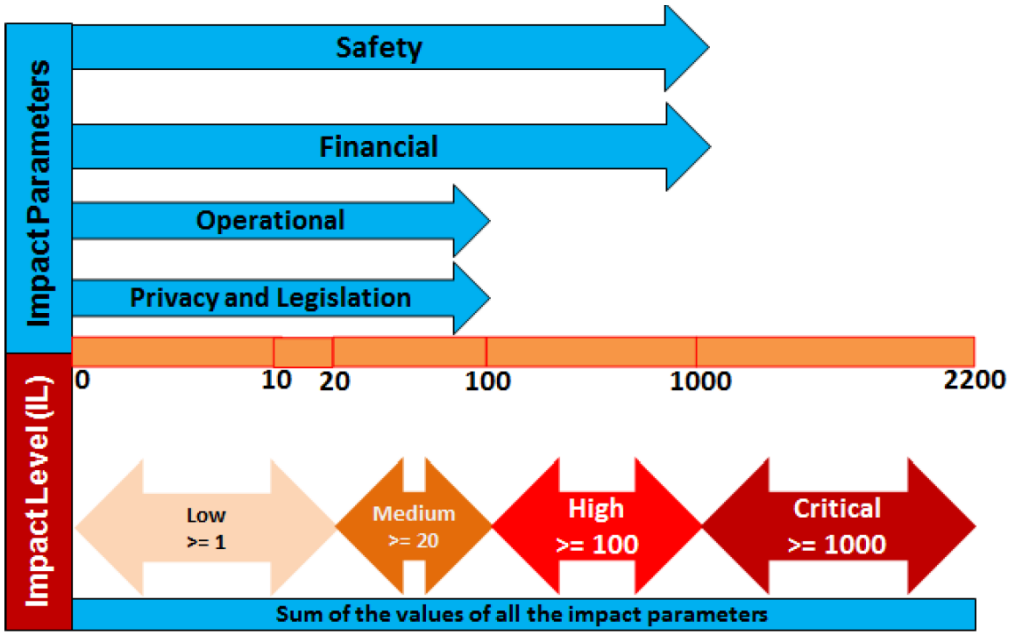

Figure 1: HEAVENS Security Model [2]

Looking at those differences it is obvious that an argument "in conformance with [1] because using HEAVENS [2]" is not adequate without further justification for the [1] Concept Phase (clause 9) item/TARA level. Note that this does not mean that a rationale couldn't be found as [1] Permission PM-15-07 allows to focus on the most critical impact category. In case this is safety it could be assumed that the Risk Treatment decisions would be similar.

The focus of this paper, is not on TARA's which is a [1] clause 9 Work Product (WP) on item level, but on C-SA, which has to be performed because of WP-10-05, WP-08-05 and WP-08-06 of [1]. Consequently, the focus is on AF determination and to analyze whether HEAVENS TL is appropriate to get used for the AF rating. Note that the Recommendation in ISO/SAE 21434 [1] does not require to apply Attack Potential approach ([1] RC-15-11). RC-15-12 is just one recommendation out of the options provided in RC-15-11 (Attack Potential, CVSS, Attack Vector). However, simply stating "we do something else because RC-15-11/12 are just recommendations" is not a strong Cybersecurity argumentation as RC-15-11/12 should get considered state-of-technology. The question to be answered in this work is:

Q1: How can HEAVENS TL [2] be used to determine [1] AF in a way to achieve results comparable to application* of *[1] RC-15-12?

Objective is not to achieve identical results as it is obvious that applying RC-15-12 (attack-potential) versus RC-15-13 (CVSS with exploitability value) and RC-15-14 (attack vector) would hardly result to the same AF values although all those recommendations would in line with [1]). However, does this paper try to identify parameterization and mapping which results in very similar results compared to RC-15-12.

II. TERMINOLOGY

Abbreviation	Meaning
AF	Attack Feasibility as defined in [1]
C-SA	Component Security Analysis: a term used to cover [1] Weaknesses found during development (WP-10-05) and Vulnerability Analysis (WP-08-05) on component level. Note: the judgement whether a weakness is a vulnerability requires in practice to perform the vulnerability analysis.

Abbreviation	Meaning
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration (mitre.org)
E/E	Electrical/Electronic
equ	Equipment
eti	Elapsed time
exp	Specialist expertise
HEAVENS	Healing Vulnerabilities to Enhance Software Security and Safety
I	Impact level as defined in [1]
IL	Impact-Level as defined in [2]
ISO	International Organization for Standardization
item	Item as defined in [1]
kno	Knowledge of item or component (or target of evaluation, TOE)
MITRE	MITRE Corporation – A nonprofit organization based in the United States, responsible for maintaining the Common Weakness Enumeration (CWE) and Common Vulnerabilities and Exposures (CVE) databases, among others
PM	Permission as defined in [1]
Q	Question
R	Risk
RC	Recommendation as defined in [1]
RQ	Requirement as defined in [1]
SAE	SAE International (*previously Society of Automotive Engineers*)
S, F, P, O	Safety, financial, privacy, operational impacts as defined in [1]
SL	Security-Level as defined in [2]
SoC	System-on-a-Chip
TARA	Threat-Analysis and Risk-Assessment, as defined in [1]
TIER	Tier (supplier level, e.g. Tier 1, Tier 2 in the automotive supply chain)
TL	Threat-Level as defined in [2]
TOE	Target-of-Evaluation
UNECE	United Nations Economic Commission for Europe
val	Value
win	Window of opportunity
WP	Work Product

III. COLLECTION OF FACTS

A. Input parameters

Table I. Parameter Scores for Attack Potential and HEAVENS TL

Parameter	Abbreviation	Attack Potential	HEAVENS TL
Elapsed Time	eti	Y	N
Specialist Expertise	exp	Y	Y
Knowledge of item or component (or TOE)	kno	Y	Y
Window of opportunity	win	Y	Y
Equipment	equ	Y	Y

Both approaches use the same four input parameters, but HEAVENS omits the *Elapsed Time*. This is however done based rational: *"The HEAVENS model excludes the Elapsed Time-parameter because this is not a first-order parameter while deriving threat level"* (from 4.4.1.1 State-of-the-art and HEAVENS [2]). We share this concern with respect to *Elapsed Time*. In addition, we try to answer question Q1 above. We therefore suggest calculating this free parameter *Elapsed Time* when applying HEAVENS TL to achieve answer on Q1. This leads to Q2:

Q2: How to derive the 2nd order parameter elapsed time as a function of the other 4 parameters?

$$\mathrm{val}_{\mathrm{eti}} = F(\mathrm{val}_{\mathrm{exp}}, \mathrm{val}_{\mathrm{kno}}, \mathrm{val}_{\mathrm{win}}, \mathrm{val}_{\mathrm{equ}}) \tag{3}$$

Looking up the semantical description of the different parameters in [1] RC-15-12 and [2] does not disclose significant differences. Although they are not identical, they partially use the same sentences which can be explained as [3] is a common base. It can hence be assumed that expert judgment will not depend on whether [1] RC-15-12 or [2] is used for the parameters $(\mathrm{val}_{\mathrm{exp}}, \mathrm{val}_{\mathrm{kno}}, \mathrm{val}_{\mathrm{win}}, \mathrm{val}_{\mathrm{equ}})$.

B. Scoring schemes of input parameters

Table II. ISO/SAE 21434 I.7 Attack Potential scores [1]

Elapsed time	Expertise	Knowledge of item or component	Window of opportunity	Equipment	$\mathrm{Val}_{\mathrm{elap}}$	$\mathrm{Val}_{\mathrm{exp}}$	$\mathrm{Val}_{\mathrm{kno}}$	$\mathrm{Val}_{\mathrm{win}}$	$\mathrm{Val}_{\mathrm{equ}}$
1 week	Layman	Public	Unlimited	Standard	0	0	0	0	0
1 month	Proficient	Restricted	Easy	Specialized	1	3	3	1	4
6 months	Expert	Confidential	Moderate	Bespoke	4	6	7	4	7
3 years	Multiple experts	Strictly confidential	Difficult	Multiple bespokes	10	8	11	10	9
10 years	NaN	NaN	NaN	NaN	19	NaN	NaN	NaN	NaN

Table III. HEAVENS TL parameter scores [2]

Expertise	Knowledge of item or component	Window of opportunity	Equipment	$\mathrm{Val}_{\mathrm{exp\_h}}$	$\mathrm{Val}_{\mathrm{kno\_h}}$	$\mathrm{Val}_{\mathrm{win\_h}}$	$\mathrm{Val}_{\mathrm{equ\_h}}$
Layman	Public	Unlimited	Standard	0	0	0	0
Proficient	Restricted	Easy	Specialized	1	1	1	1
Expert	Confidential	Moderate	Bespoke	2	2	2	2
Multiple experts	Strictly confidential	Difficult	Multiple bespokes	3	3	3	3

Interpretation of Figure 2 and Figure 3 shows that:

- The weighting in [2] is the same for all parameters whereas [1] RC-15-12 has slight variations (10, 8, 11, 10, 9) which means a variation of weights around 10-20 %.
- The scales are 100 % linear in [2] whereas the scales in [1] RC-15-12 are partially almost linear and partially nonlinear (can be fitted with x^2).
- In both schemes, doing a higher score indicates a higher difficulty of the attack.

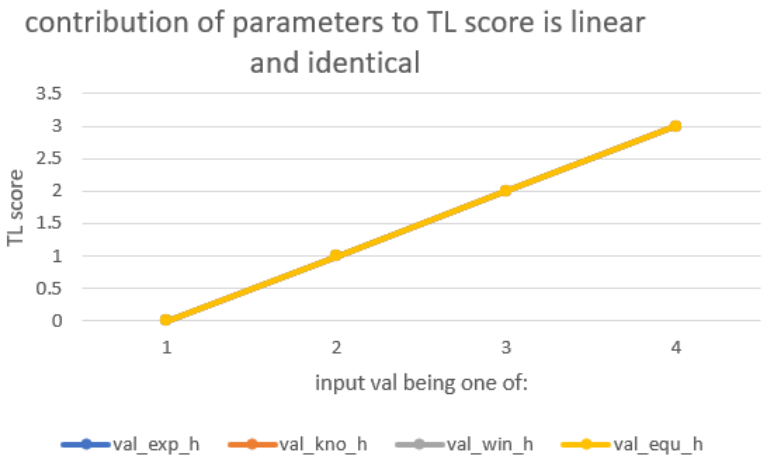

Figure 2: Contribution of parameters to TL score is linear and identical

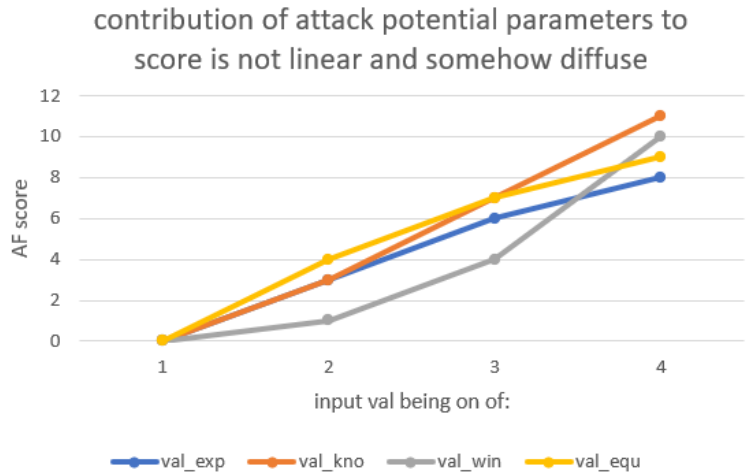

Figure 3: Contribution of Attack Potential parameters to score is not linear and somehow diffuse

C. Assignment of AF and TL based on scores

Table IV. Attack Potential score to AF map

AF_{val}	**AF**
0 to 13	high
14 to 19	medium
20 to 24	low
25 or more	very low

Table V. HEAVENS TL score to TL map

TL_{val}	TL
0 to 1	critical
2 to 3	high
4 to 6	medium
7 to 9	low
9 or more	none

Visualization of Table IV and Table V results in the diagrams below. The *AF's* and *TL's* are represented by numbers counting from 0 upwards.

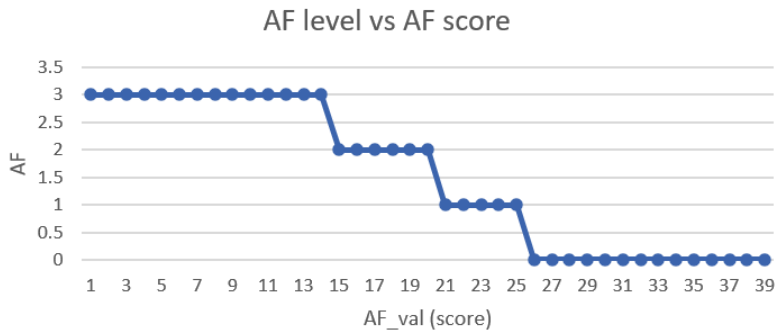

Figure 4: Visualization of AF score to AF map [1]

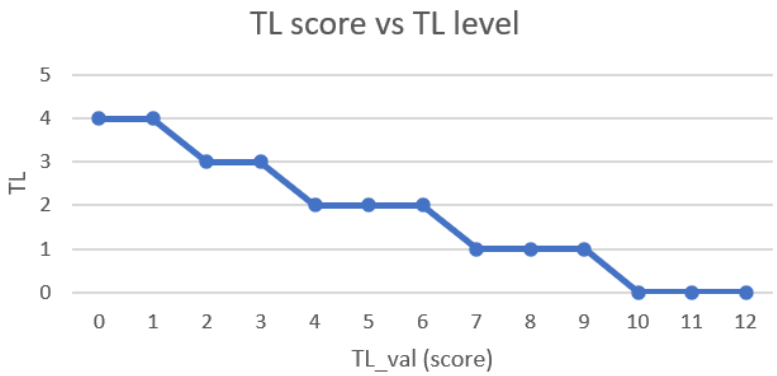

Figure 5: Visualization of TL score to TL map [2]

Observations:

- Different terms and neither [1] RC-15-12 nor [2] further describe those terms. They are implicitly defined by the scoring in both schemes.
- [2] uses 5 levels instead of 4 levels in [1].
- [2] 5 level mapping is closer to a linear function compared to [1] RC-15-12.
- [1] RC-15-12 has a long plateau for AF==*high*==3 which has almost double the size compared to AF medium, low and very low.
- If we would re-assign TL *critical* (value of 5 in Figure 5) to TL *high* (value of 4) and normalize the x-scale we would get a map closer to Figure 4.

The observations lead to the next question:

Q3: How to map TL levels [critical, high, medium, low, none] to AF level [high, medium, low, very_low]?

IV. PRAGMATIC EMPIRICAL PROPOSAL

The intention of the proposal is to answer questions Q1, Q2 and Q3. Questions Q2 and Q3 can be regarded as question broken down from Q1. Whether the proposals for Q2 and Q3 allow us to answer Q1 is to be judged in section *IV.B.*

A. Proposal for Q2:

Q2: How to derive the 2nd order parameter elapsed time as a function of the other 4 parameters as in (3)?

$$\mathrm{val}_{\mathrm{eti}} = F(\mathrm{val}_{\mathrm{exp}}, \mathrm{val}_{\mathrm{kno}}, \mathrm{val}_{\mathrm{win}}, \mathrm{val}_{\mathrm{equ}})$$

Proposal P1:

$$val_{eti} := \frac{\sum_{i \neq eti} val_i}{2} = (val_{exp} + val_{kno} + val_{win} + val_{equ})/2 \quad (4)$$

Rationale:

- Higher scores (val's) from 1st order parameters are expected to increase the 2nd order parameter *elapsed_time*.
- The Attack Potential scheme [1] RC-15-12 will cause the result of the SUM to be in the range of [0,38]. The division by 2 scales it down to [0, 19] which is exactly the range of elapsed time as per [1] RC-15-12.

The function is linear with respect to the input parameters and hence the simplest approach. We basically follow the attempt "start with a linear approximation before including more complex and nonlinear terms". It is clear that this deviate from the original *elapsed_time* scale in [1] RC-15-12 which is illustrated in Figure 6 based on data from Table II. It can be nicely approximated with a quadratic function but for simplicity the decision made to start with the simple equation above from Proposal P1.

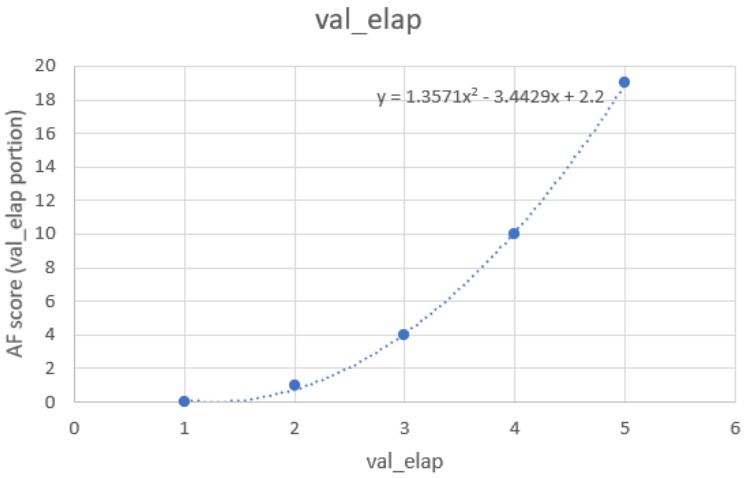

Figure 6: RC-15-12 eti scale

B. Proposal for Q3

Q3: How to map TL levels [critical, high, medium, low, none] to AF level [high, medium, low, very_low]?

Table VI. Proposal for TL to AF mapping

TL_{val}	TL	AF
0 to 1	critical	High
2 to 3	high	High
4 to 6	medium	Medium
7 to 9	low	Low
9 or more	none	very_low

Rationale:

- The relationship between columns TL_{val} and TL is defined by HEAVENS [2] and we do not want to interfere into the HEAVENS scheme itself.
- The relationship of columns TL and AF is motivated by:
  - The intuitive name matches although both schemes do not define those enumerations precisely.
  - The observation from III.C *Assignment of AF and TL based on scores* "If we would re-assign TL *critical* (value of 5 in Figure 5) to TL "high" (value of 4) and normalize the x-scale we would get a map closer to Figure 4". Look back at both figures: Attack Potential [1] RC-15-12 does not have a *critical* or *very-high* but a long plateau on *high*. The proposal appears promising to use HEAVENS TL in a way to achieve comparable results.

V. ANALYSIS OF RESULTS

In order to answer Q1,

Q1: How can HEAVENS TL [2] **be used to determine** *[1]* **AF in a way to achieve results comparable to application of** *[1]* **RCV-*15-12?***

we ran an analysis over all possible combinations of the 4-tuple $[\mathrm{val}_{\mathrm{exp}}, \mathrm{val}_{\mathrm{kno}}, \mathrm{val}_{\mathrm{win}}, \mathrm{val}_{\mathrm{equ}}]$. Those are $4^4 = 256$ combinations which are feasible to compare. For all combinations we calculate $AF_{\mathrm{diff}} = \mathrm{AF}_{\mathrm{attackPotential}} - \mathrm{AF}_{\mathrm{heavens}}$ and look at the histogram.

Table VII. Histogram results for the differences in AF rating

AF_{diff}	Histogram value	Note
0	189	Equal AF level by both methods
-1	12	Cases where the proposed scheme leads to lower AF rating
1	55	Cases where the proposed scheme leads to a higher AF rating
SUM	256	

The results are very convincing:

- For only 5 % of input combinations the scheme results in a lower AF rating. Only those could potentially lead to a missing risk reduction requirement.
- For around 20 % of input combinations the scheme results in a higher AF rating. Those could only lead to additional risk reduction requirements.

- No difference in AF rating is bigger than 1.

Looking at the results in more detail:

$$AF_{\text{attackPotential}} == high \text{ are judged } AF_{\text{heavens}} == high\ or\ medium \tag{5}$$

If the Cybersecurity Management System policy required to treat high and medium by risk reduction would not any potential risk reduction requirement get missed.

$$AF_{attackPotential} == medium \text{ are judged } AF_{heavens} == medium \tag{6}$$

Except for 2 out of 33 which are judged *low* and is almost a perfect match for level *medium*.

$$\text{All: } AF_{attackPotential} == low \text{ are judged } AF_{heavens} == low \text{ or } medium \tag{7}$$

None *low* judgement would get downgraded to *very_low,* but some get judged slightly more conservative (a higher AF leads to a more conservative risk treatment decision).

$$\text{All: } AF_{attackPotential} == very\ low \text{ are judged } AF_{heavens} == very\ low \text{ or } low \tag{8}$$

Most *very_low* judgements match but some get judged slightly more conservative.

An answer to question Q1 is given when the proposals P1 and P2 are considered.

VI. CONCLUSION

The results show that using the proposed rules very similar results can be achieved when applying HEAVENS TL [2] instead of [1] RC-15-12. The impact of the small differences even vanishes further when considering that:

- The Input parameters $[val_{exp}, val_{kno}, val_{win}, val_{equ}]$ determination require expert judgment. This is expected to lead to variations when done by different experts. A numerical counting system cannot address those uncertainties.
- [1] RC-15-13 (CVSS with exploitability value) is expected to show differences compared to RC-15-12 derived AF values. It already works with different and more IT security driven input parameters. The advantage of CVSS is more in its common use in CWE MITRE and related databases.
- [1] RC-15-14 (attack vector) approach is expected to create even more different AF values as it is based on the "distance" only.
- Considering that RC-15-13 and RC-15-14 are as well recommended AF determination methods in [1], it seems clear that applying HEAVENS TL [2] in combination with proposals P1 and P2 are expected to get closer results to RC-15-12.
- The proposed scheme simplifies the Attack Feasibility (AF) determination compared to [1] RC-15-12 which allows for easy application within threat-analysis tools.
- One could view it a drawback that the *Elapsed Time* parameter cannot be set explicitly. The authors however regard this as an advantage as the *Elapsed Time* is a second order parameter as explained in [2].

Using HEAVENS TL [2] in combination with proposals P1 and P2 appropriate to achieve results which are comparable to Attack Potential approach as suggested in [1] ***RC-15-12.***

REFERENCES

[1] International Organization for Standardization, "Road vehicles – Cybersecurity engineering," ISO/SAE 21434:2021, Geneva, 2021.

[2] A. Lautenbach und M. Islam, „HEAVENS: Healing Vulnerabilities to Enhance Software Security and Safety," Chalmers University of Technology, Gothenburg, Sweden, 2021.

[3] International Organization for Standardization and International Electrotechnical Commission, „Information Security, Cybersecurity and Privacy Protection – Evaluation for IT Security – Methodology for IT Security Evaluation," ISO/IEC 18045, Geneva, Switzerland, 2022.

[4] EVITA Project Concortium, „Specification and Evaluation of E-Security Relevant Use Cases," EVITA Project, 2009.