Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
©2022 ESREL2022 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_R26-01-246-cd

An Analytic Approach to Analyze a Defense-in-Depth (DiD) Effect as proposed in IT Security Assessment

Thomas Termin
Institute for Security Systems, University of Wuppertal, Germany. E-mail: termin@uni-wuppertal.de

Daniel Lichte
Institute for the Protection of Terrestrial Infrastructures, German Aerospace Center, Germany. E-mail: daniel.lichte@dlr.de

Kai-Dietrich Wolf
Institute for Security Systems, University of Wuppertal, Germany. E-mail: wolf@iss.uni-wuppertal.de

Latest approaches in IT security assessments interpret the Common Vulnerability Scoring System (CVSS) parameters as barriers connected in series. In contrast to the classic multiplicative approach according to CVSS for determining exploitability via numerical values associated with the CVSS parameters, an additive approach is proposed in Braband (2019). Logarithmized CVSS scores are introduced to overcome the computational limitations with ordinal values. The log score sum across all barriers is sorted on a scale corresponding to a likelihood of exploitability (LoE) category. CVSS world is not only decomposed and remodeled into a mathematically admissible algorithm, but also contains an inherent defense-in-depth (DiD) effect. With each barrier added, the LoE decreases. This architectural interpretation can neither be falsified nor confirmed with previous CVSS metrics. Unlike in the IT security domain, tools exist in physical security to compute DiD in an objectively consistent manner. In our paper, we apply these considerations to a physical security setup in order to replicate his systemic modification based on CVSS. In a detailed analysis, we examine the boundary conditions and measures that must be taken in quantitative physical security metrics to emulate the DiD effect in IT security.

Keywords: Physical Security, IT Security, CVSS.

1. Introduction

For the design of a security system, a well thought-out evaluation of the security functions in the application is required. In both physical security and safety, quantitative metrics are used for this purpose (Garcia 2005; Zio 2012). In physical security, the probability that an attacker reaches an asset faster than the defender reaches the attacker is used as the basis for evaluation (Lichte et al. 2016).

In safety, the evaluation metric is classically a failure rate or a system reliability over a specific period of time (Lichte et al. 2019). The underlying metrics in the disciplines are based on a time-based probability related to physical processes and states. In IT security, it is common to use scores, i.e., semi-quantitative assessments, because this underlying metric is missing (Yee 2013).

Common IT security metrics do actually not map the physical processes as in physical security or safety. This is partly because the paradigms in IT differ from those in the physical world. Whereas in IT, different entry points can be used to get to an asset (Wheeler 2011), a physical attacker is guided along a path determined by the placement of barriers and their openings to convenient authorized access (Garcia 2005).

In addition, the use of probabilities in IT is a different interpretation than in physical security or safety. In IT, probability means, for example, that 90% of publicly known vulnerabilities are identified and closed (Jones 2007). In physical security, on the other hand, probability means that, for example, 65% of the time it takes an attacker 30 seconds to overcome a barrier (Lichte et al. 2016). In both cases, these are probabilities. However, these do not fit together properly.

In physical security, risk is assessed on the basis of vulnerability via the interaction of protection, observation and intervention. Since scenarios are considered that have not yet occurred, the epistemic probability of attack is assumed to be 100%. Physical vulnerability is thus assessed on a very concrete, performance-based level.

In addition to the quantitative intervention capability metric (ICM) of Lichte et al. (2016), in which uncertainties about the security functions of a physical system are taken into account in the form of density functions for protection, observation and intervention, there is also the semi-quantitative scoring system Performance Risk-based Integrated Security Methodology

(PRISM) of the Harnser Group (Harnser 2010). In PRISM, the integral parameters of protection, detection, and intervention are scored between "1" (low) and "5" (high) and summed. This leads to deviations compared to the quantitative metric: For example, if protection were at "3," detection were at "1" (minimum design), and intervention were at "5," then the vulnerability score according to the PRISM would be in the midrange (score of "9"). However, according to the ICM, the system would be maximally vulnerable under these constraints. A certain interplay of the three performance mechanisms is required to achieve a protective effect.

In the context of metric accuracy, Krisper (2021) and Termin et al. (2021) analyze problems with the use of semi-quantitative approaches.

In IT security, this performance mechanism is obviously missing. A common metric used internationally is the Common Vulnerability Scoring System (CVSS) v3.1 (First.org 2022). An exploitability score is calculated using the scenario-describing parameters Attack Vector (AC), Attack Complexity (AC), Privileges Required (PR) and User Interaction (UI), to which numerical values are assigned.

The association of these values corresponds to ISO/SAE 21434 of an Attack Feasibility category (SAE 2022). From a physical perspective, this is the threat probability (Witte et al. 2020).

For CVSS, in addition to the Exploitability, the Impact, consisting of the protection goal violation of confidentiality, availability and integrity, is further used to determine the Vulnerability Score. Since the numerical values of the parameters are on an ordinal scale and actually only a ranking is possible, building log values of the numerical CVSS score values is suggested in Braband (2019).

A barrier-based approach is applied to CVSS metrics, postulating a defense-in-depth (DiD) effect. From these considerations, the scientific question arises: How can the hypothesis on the DiD effect be assessed or confirmed? With our paper, we want to contribute to the genesis of a metric tool to evaluate the quality of metrics or metric modifications respectively. For this purpose, we adapt approaches from IT and transfer them to physical security to analyze metrical considerations quantitatively

2. Background

The CVSS parameters Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR) and User Interaction (UI) can be interpreted as barriers connected in series, which corresponds to the principle of defense in depth (DiD) (Braband 2019). The following classifications can be used: AV represents the location of the IT attack (physical barrier), AC the complexity of the attack from a technical point of view (technical barrier) and PR the rights required on the part of the user or UI the need for user interaction (organizational barrier).

As proposed in Braband (2019), the parameters AV to UI can be interpreted as the likelihood of exploitation (LoE). LoE describes that an attacker will successfully overcome the barriers AV to UI. In order to determine the LoE, the numerical values of CVSS are converted into a semi-quantitative approach on an interval scale. This is done by applying the logarithm to the CVSS base metrics of the AV to UI.

Here, the absolute parameter values range from 0.2 to 0.8 in the base metric, which is why the logarithm of the respective numerical values is set to the base of 0.6. That is the difference between the upper and lower limit of possible numerical values. As an example, this is done in Eq. (1) for the characteristic "Physical" of the parameter AV:

$$\text{logScore (AV = "Physical", num. v.} = 0.2) = log_{0.6}(0.2) = 3 \quad (1)$$

Secondly, LoE score is calculated by building the sum of the logarithmic scores, which depend on the characteristics of the parameters (see Eq. (2)).

$$\text{LoE} = log_{0.6}(AV) + log_{0.6}(AC) + log_{0.6}(PR) + log_{0.6}(UI) \quad (2)$$

The result space of the LoE scores is divided into intervals. The lowest score sum, "0", corresponds to a very high probability level, scores "1-3" to a high probability level, and so on. (see Table 1). The following abbreviations are used: “Very Likely = VL”, “Likely = L”, “Possible = P”, “Unlikely = UL”, “Very Unlikely = VUL”.

Table 1. LoE Intervals With Corresponding Barriers (Source: Braband (2019))

Like-lihood	VL	L	P	UL	VUL
LoE-Score	0	1-3	4-5	6-7	8-9
Barriers	0	1	2	3	4

Thirdly, the probability levels of the LoE scores can be assigned to a number of barriers (compare Table 1 third line). In addition to the specific protection effect (the LoE score), barrier depth can be included in the evaluation.

Adding another barrier, as contended in Braband (2019), reduces the LoE. Assuming that the variable "System Check" (SC) is taken into account as a “procedural barrier” with the exemplary characteristics Low (score "0") and High (score "1") in Braband's scheme, the LoE score (here LoEmod) results in Eq. (3).

$$\text{LoEmod} = log_{0.6}(AV) + log_{0.6}(AC) + log_{0.6}(PR) + log_{0.6}(UI) + log_{0.6}(SC) \quad (3)$$

Using LoEmod, the LoE intervals can be extended with the section "Very very unlikely = VVUL" (compare Table 2).

Table 2. LoEmod Intervals With Corresponding Barriers (Barrier-Based CVSS Scheme Extended)

Likelihood	VL	L	P	UL	VUL	VV UL
LoE-Score	0	1-3	4-5	6-7	8-9	10
Barriers	0	1	2	3	4	5

As can be interpreted from the previous table, every additional barrier can potentially reduce exploitability. The argument that the barrier-based approach to assess exploitability provides better results than the classical CVSS is difficult to verify or falsify with the CVSS metrics. In this a quantitative tool is needed to systematically analyze the DiD effect.

3. Approach

Unlike in IT security, tools exist in physical security to compute DiD in an objectively consistent manner. Considerations presented in the background chapter can be applied to physical security to emulate the systemic modification of the scientist.
Security functions in the physical world are evaluated via the interplay of protection (P), observation (O) or detection (D), and intervention (I). According to the semi-quantitative Harnser metric (Harnser 2010), protection, detection and intervention are assessed using scores between "1" (low) to "5" (high) (compare Table 3).

Table 3. Harnser Score Levels To Compute Vulnerability (Source: Harnser (2010))

Protection Score (P)	Detection Score (D)	Intervention Score (I)
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5

In a similar way to CVSS, numerical values can be assigned to these scores (compare Table 4). Despite the fact that the assessment parameters in physical security are on a much more concrete level than the scenario-describing parameters of CVSS, they could be interpreted in the same way (compare Fig. 1).

Table 4. Harnser Score Levels With Corresponding Numerical Values (Source: Harnser (2010) Extended)

P	D	I	Numerical Value
1	1	1	0.83
2	2	2	0.66
3	3	3	0.5
4	4	4	0.33
5	5	5	0.16

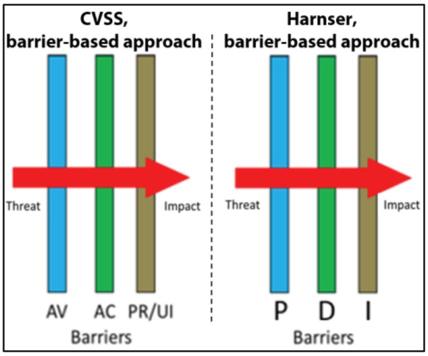


Fig. 1. Mapping The Barrier-Based CVSS Principle To Physical Security (Source: Braband (2019))

Instead of the LoE, likelihood of vulnerability (LoV) categories are determined here. For this, we logarithmize the numerical Harnser scores according to the proposed aggregation scheme. The base b to which log values are built is set to 0.6. It approximates the range from 0.16 to 0.8 quite well. Thus the LoV results in Eq. (4):

$$\text{LoV} = log_{0.6}(P) + log_{0.6}(D) + log_{0.6}(I) \quad (4)$$

Using Eq. (4), log scores can be calculated and mapped to the numerical Harnser scores (compare Table 5).

Table 5. Harnser Score Levels With Corresponding Numerical Values And Log Scores

P	O	I	Numerical Value	log Score (b = 0.6)
1	1	1	0.83	0
2	2	2	0.66	1
3	3	3	0.5	2
4	4	4	0.33	3
5	5	5	0.16	5

Following the categorization of Table 1, the LoV can be classified as follows (compare Table 6):

Table 6. LoV Intervals With Corresponding Barriers

Likelihood	Likely	Possible	Unlikely
LoV-Score	0-5	6-10	11-15
Barriers	1	2	3

The definition of the category "Likely = log score sum 0-5" is based on the fact that a minimum log score sum of "0" and only a maximum log score sum of "5" can be achieved in the presence of a single barrier. If a second barrier is now added, a maximum log score of "10" can be achieved. This is again the upper limit of the second category, and so on.

As a first step, we substitute the parameter "detection" by "observation". This is done because detection is an event that has protection and observation components, so the protection would be considered "twice".

In a second step, it is important to consider what the interpretation of these performance mechanisms as barriers means in terms of the security functions of a physical system. Since a protective effect is only given if elements of protection, observation and intervention interact, the interconnection of the performance mechanisms as barriers would only be possible under the assumption that they are "performance-activated".

In the case of the protection barrier, for example, the protection performance mechanism is particularly dominant, but there are also portions of observation and intervention.

However, these two are less developed than protection, e.g. as the protection score increases, the protection time also increases, whereas the other two performance mechanisms remain the same (compare Fig. 2). Similarly, the performance principle is applied to the detection and intervention barrier.

In the time-based intervention capability metric (ICM), as introduced by Lichte et al. (2016), density functions are assigned to the performance mechanisms to account for uncertainties in the performance of security functions. The mean and standard deviation are control variables to describe these density functions. In order to analyze and evaluate the postulated DiD effect, performance-activation must be emulated within the ICM.

The system under consideration consists of a protection, observation, and intervention barrier, i.e., DiD = 3. Consequently, when protection, observation and intervention are connected in series according to the modified evaluation scheme for CVSS, there is a protection-activated barrier, an observation-activated barrier, and an intervention-activated barrier (compare Fig. 3).

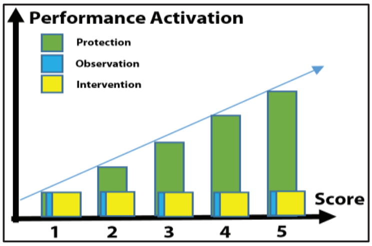


Fig. 2. Principle Of Designing Protection-Activated Barriers

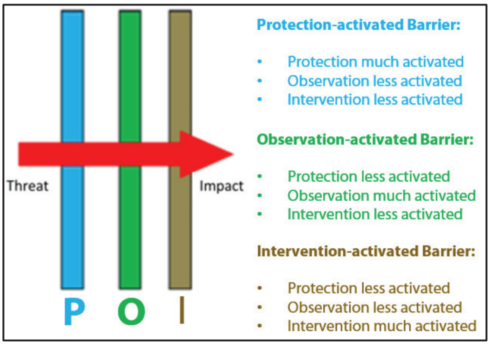

Threat
Impact
P
O
I
Protection-activated Barrier:
Protection much activated
Observation less activated
Intervention less activated
Observation-activated Barrier:
Protection less activated
Observation much activated
Intervention less activated
Intervention-activated Barrier:
Protection less activated
Observation less activated
Intervention much activated

Fig. 3. Boundary Conditions of Barrier-Based CVSS Principle From A Physical Security Perspective

Mapping the barrier-based CVSS approach to the fictitious system under consideration, DiD = 3 results in the aforementioned LoV categories: "Likely", "Possible" and "Unlikely" (compare Table 7). These can each be assigned a corresponding probability interval, e.g., "Likely" (DiD =1) 0.66-1, etc. (compare Table 7).

Thus, with a single barrier (DiD = 1), an LoV of 0.66-1 can be achieved when considering either a protection barrier, an observation barrier or an intervention barrier that each can be scored from "1" to "5".

Table 7. Likelihood Of Vulnerability (LoV) Scale

Category:	Likely	Possible	Unlikely
LoV-Score	0-5	6-10	11-15
Barriers	1	2	3
Transf. Prob.	0.66-1	0.33-0.66	0-0.33
Upper Value	1	0.66	0.33
Lower Value	0.66	0.33	0
Mean	0.83	0.495	0.165
Interpretation	Weak	Medium	Strong

A barrier depth of one (DiD = 1) corresponds to the weakest configuration, whereas a DiD = 3 corresponds to the strongest configuration, respectively. If, for example, there is an LoE (in physical security an LoV) of "Unlikely", then it can be assumed that it is the same as saying there are three barriers (DiD) or, for example, only one strong barrier or three weaker barriers.

Consequently, there is the claim that in both cases - calculation of the LoV via the log score sum of the integral parameters and determination of the LoV via the number of barriers - the result is the same. In the following, the DiD effect is emulated using the proposed quantitative metric.

3.1 Strength equals vulnerability

In a first step, the strength of a barrier is interpreted as reduction of vulnerability. A total of five barrier configurations are considered as examples (compare Table 8).

Table 8. Analysis Run I, DiD = 3

Barrier 1 (B1)	Barrier 2 (B2)	Barrier 3 (B3)
Strong	None	None
Strong	Weak	Weak
Weak	Weak	Weak
Strong	Medium	Weak
Medium	Medium	Weak

Adapting the classification presented in chapter 3, "Strong" can be described by a vulnerability interval of 0 - 0.33 with a mean value of 0.165, i.e. if a barrier of the type "Strong" is present, then it can also assume vulnerability values of 0 - 0.33.

In the following analysis, only the upper, mean and lower value of an interval that a barrier strength can have are assumed for simplicity. For the "Strong" category, these are 0.00, 0.165 and 0.33. The vulnerability values for the other two categories are defined in similar manner.

According to the ICM, vulnerabilities of a set of barriers are multiplied across the path under consideration (Lichte et al. (2016). In a further step, all possible permutations are calculated and the results are plotted (compare Fig. 4).

With the exception of the configuration "B1 = weak, B2 = weak, B3 = weak", the results of the configurations considered lie largely within the interval limits of the category “Unlikely” which reach from Lower (0) to Upper (0.33). In principle, additional barriers cannot make the overall vulnerability worse.

Vulnerability is a probabilistic value between 0.00 (minimum vulnerability) and 1.00 (maximum vulnerability).

Assuming the vulnerability of a barrier one (V_B1) is 0.5 and vulnerability of a barrier two (V_B2) is 0.4, then the total vulnerability (V_tot) is (0.5x0.4 =) 0.2. This is the product of the vulnerability of each barrier along a path. If now a third barrier is added, which has a V_B3 of 1.00, then the vulnerability is not changed (0.5x0.4x1 = 0.2).

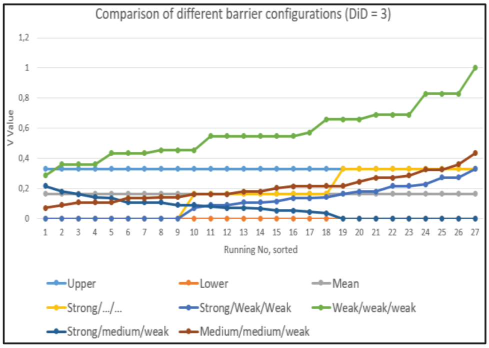


Fig. 4. Comparison Of Barrier Configurations At DiD = 3; Strength = Vulnerability

If, on the other hand, V_B3 is minimal, i.e. 0.00, then the product of the individual barrier vulnerabilities also becomes (0.5x0.4x0.00 =) 0.00. The vulnerabilities V_B1 and V_B2 can then be arbitrarily high or low. As long as a barrier has a vulnerability of 0.00, the total term is 0.00.

In conclusion, the postulated DiD effect is demonstrably partially correct with his hypothesis, insofar as barrier strength is interpreted as vulnerability.

3.2 Strength equals performance-activation of barriers, small scatter

From a scientific point of view, it is difficult to assess vulnerability directly without knowing the interplay of protection, observation and intervention.

In a further consideration, the question arises whether the hypothesis of DiD effect can be recalculated, insofar as the "strength" of the barriers is not interpreted as the vulnerability of the barriers, but as the activation of performance-activation of the barriers.

If there is only one barrier, for example a protection-activated barrier, then the question arises how the parameters of protection, observation and intervention of this barrier must be defined in the approach of the intervention capability, so that protection-activation prevails and vulnerability values of 0.66 to 1 can be represented in the result. This is the probability interval, which can be assigned to the category "Likely" or to DiD = 1.

First, it must be determined what protection-activated specifically means. The following considerations can be made:

It is known that the "control variables" in the ICM are the mean (μ) and the standard deviation (σ). To define e.g. "protection-activation", simplifications and assumptions are generally a good first step. Thus, the hypotheses to achieve vulnerability values between 0.66 and 1 (in the full bandwidth) are intuitively:

- Protection (time) increases with increasing score, e.g., for score “1” or log score “0” μ_P = 10 (sec) and for score “5” or log score “5” μ_P = 30 (sec).
- The dispersion of P is constant and small with increasing score, e.g., σ_P = 5 (sec).
- The intervention time is "poor", i.e., quite high. The scatter is very high.
- The observation time is also quite high. The scatter is very high.

Then, permutations (different combinations of μ and σ) can be analyzed to find the "best fit" of parameter combinations that yields vulnerability values between 0.66 and 1. This is an optimization problem, which is addressed here by systematic parameter setting. The analysis to find the best fit is not presented here in detail. In summary, the distribution of parameters for reaching performance-activation is as follows:

- P: {"t_P": norm((10, 15, 20, 25, 30), 5), "t_O": norm(5, 4), "t_I": norm(35, 30)} V: [0.87 0.80 0.74 0.68 0.62]
- O: {"t_P": norm(35, 25), "t_O": norm((10, 15, 20, 25, 30), 5), "t_I": norm(35, 30)} V: [0.66 0.72 0.77 0.82 0.87]
- I: {"t_P": norm(20, 10), "t_O": norm(12, 10), "t_I": norm((10, 15, 20, 25, 30), 10)} V: [0.67 0.75 0.82 0.88 0.92]

In order to be able to map the vulnerability results obtained by the integral parameters via the BICM over the entire interval (here 0.66 to 1), the barriers that are actually "singular"-activated, i.e., purely protective, observational, and intervention, must be at least "double-activated," i.e., two parameters are actually strongly activated and one is less activated.

Now the twist is to prove that the approach presented in the background chapter brings improvements. For this reason, a budget of resources is required. Within the Harnser metric, a maximum of five points per value, which basically represent resources, can be allocated. These scores can be interpreted as coins that can be distributed by a system operator.

If fifteen coins are available, all slots can be filled up. In reality, resources are classically restrictive (Sowa 2011). For example, only ten coins are available and a decision must be made on how to distribute them. This could be an equal distribution to all barriers or a concentration on specific barriers.

In this paper, we suppose there are five coins. The initial question is now: Should a system operator focus on one barrier or distribute the coins over all three barriers? For answering the question, different configurations (permutations) need to be calculated and analyzed.

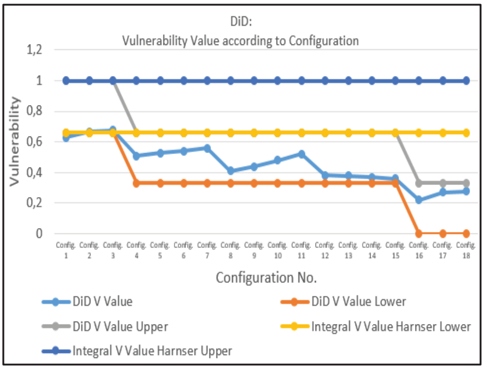
According to the purely additive Harnser metric, vulnerability would be identical for the permutations because the identical number of coins are given. In the quantitative approach, the five coins are distributed in different configurations to one to three barriers. It is to be examined to what extent the protection capability changes when certain parameters (combinations) are "turned up", i.e. activated more strongly. The experimental setup and the vulnerability results (DiD V Values) shown in Table 9.

Table 9. Excerpt Of Experimental Setup;
5 Coins On DiD = 1 (Config. 1-3), DiD = 2 (Config. 4-15) And DiD = 3 (Config. 16-18)

Configuration	P	O	I	Defense-in-Depth (DiD) Vulnerability Value (V)
1	5	0	0	0.628
2	0	5	0	0.665
3	0	0	5	0.676
4	4	1	0	0.509
5	3	2	0	0.526
6	2	3	0	0.54
7	1	4	0	0.56
8	4	0	1	0.41
…	…	…	…	…
16	3	1	1	0.22
17	1	3	1	0.27
18	1	1	3	0.277

The results are illustrated in Fig. 5. In the light blue graph (compare Fig. 5), the DiD vulnerability results are shown according to configuration. Additionally, the corresponding interval boundaries lower and upper for DiD = 1, DiD = 2 and DiD = 3 are inserted. As can be seen from the graph, the DiD vulnerability curve is largely within the interval boundaries (orange and grey graphs).

Moreover, the lower and upper interval limits for the case of the integral parameter combination are compared with the DiD V values via the addition (dark blue and yellow graphs). The DiD vulnerability curve lies largely below the curves of the interval limits. Since five coins are involved, the same vulnerability level is obtained for any configuration. With the exception of configurations one to three (DiD = 1), DiD provides different results than the calculation of the integral parameters via addition. Under the given boundary conditions, the DiD effect can be confirmed.



Fig, 5. Comparison Of Barrier Configurations At DiD = 1,…, DiD = 3; Strength = Performance-Activation; Small Scatter

3.3 Strength equals performance-activation of barriers, large scattering

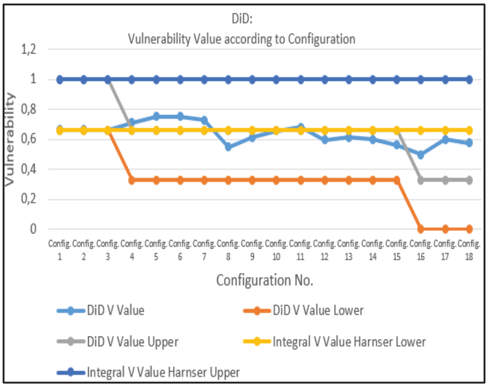
The parameters of the BICM require a double activation if the scatter of the parameter that is to be particularly activated is low. From a scientific point of view, the question arises of possibilities to set the parameters of P, O, and I in such a way that the principle of performance-activation can actually be replicated by considering only one activated parameter.

For this, we examine vulnerability results using the BICM considering large variations of the mean values. Our analysis provides the following results:

- P: {"t_P": norm((10,30,50,70,90), 40), "t_O": norm(50, 40), "t_I": norm(50, 40)}
  V: [0.97 0.94 0.8 0.78780897 0.66]
- O: {"t_P": norm(50, 40), "t_O": norm((10,30,50,70,90), 40), "t_I": norm(50, 40)}
  V: [0.66 0.78 0.88 0.94 0.97]
- I: {"t_P": norm(50, 40), "t_O": norm(32.5, 40), "t_I": norm((10,30,50,70,90), 40)}
  V: [0.66 0.78 0.88 0.94 0.97]

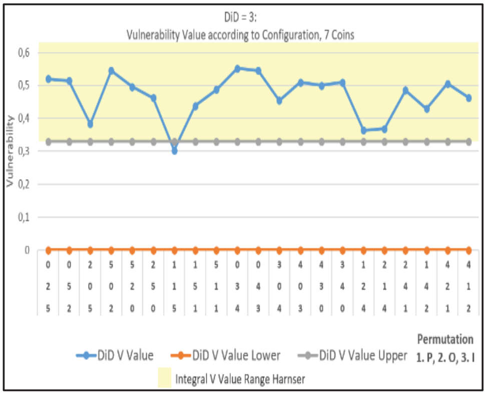
Like in the previous analysis, we calculate the results for all 18 configurations (compare Fig. 6). Here, however, the confirmation of the DiD effect is only partially apparent. For the first three configurations (DiD = 1), the results of the BICM lie in the same probability range as the results of the sum of the integral parameters (compare Fig. 6 dark blue and yellow graphs). For the configurations in the case DiD = 2 this is only conditionally the case.

The results of the BICM are either at the upper value according to the barrier-based CVSS scheme or above it. In the case of DiD = 3, all results of the balanced intervention capability metric are above the presumed probability interval for DiD = 3 at about up to 27% (Config. 17). If the results of the BICM are compared with the assumed probability interval for the sum of the integral parameters, it can be seen that the results of the BICM matches the results over the sum of integral parameters well.



Fig, 6. Comparison Of Barrier Configurations at DiD = 1,…, DiD = 3; Strength = Performance-Activation; Large Scatter

The last question to be answered is: Should a system operator now focus more on protection, observation or intervention? In a final analysis run, we increase the coin count from five to seven. Based on the boundary conditions that the activated parameter and the less active parameters have a high scatter, possible permutations are calculated again (compare Fig. 7).



Fig, 7. Comparison Of Barrier Configurations at DiD = 2,…, DiD = 3; Strength = Performance-Activation; Large Scatter

In general, it can be stated that a strong protection-activation is not beneficial, a strong observation-activation gives better results than a strong protection and a strong intervention-activation has the best effect on vulnerability. This leads to the following ranking: 1. intervention barrier, 2. observation barrier, 3. protection barrier.

4. Conclusion and outlook

In this paper, we redesigned the architecture of the physical system to emulate postulated DiD effect as proposed in IT security assessment. For this, we interpret the performance-mechanisms as performance-activated barriers. For each barrier, a certain interplay of P, O and I has been worked out by defining mean values and standard deviations.

A cost function equivalent has been introduced to compare vulnerability results over the sum of integral parameters and over the BICM. It can be confirmed that under certain boundary conditions - here: low dispersion of the activated parameter - the DiD effect can be demonstrated. If high scatter is used (see chapter 3.3), the results can be approximated quite well by the sum of integral parameters via the BICM.

In general, it must be questioned whether it makes sense to split up barriers into their basic functionality in the form of AV to UI and to place them one after the other. The reason for this is that AV to UI are variables that function on a different level than protection, observation and intervention. AV to UI are much more abstract as concepts than mechanisms considered in the physical world.

AV to UI generally involve more parameters and values that contribute than, for example, protection, which is a single parameter measured over time. Protection probability is an elementary level considered in physical security represented by a distribution over time (Lichte et al. 2016).

An AV is initially a whole scenario mapping that is described in general terms. This is, of course, a much larger construct, with much more and potentially uncertain information behind it than is typically required for the mechanisms of protection, observation and intervention.

Looking at this background, it is not likely that DiD is a proper description of the mechanisms reducing vulnerability via the mapping of the AV to UI variables from a physical point of view, because DiD describes countermeasures to prevent AV in advance. Still our results show that the DID add on in CVSS assessment proposed yields better results for some scenarios.

Overall, we have shown that quantitative tools from physical security can be used to emulate metric considerations from IT in a quantitative and objective way. In this context, it is necessary to adapt the quantitative metric to the boundary conditions assumed for the semi-quantitative metric.

In future research, we intend to use the findings to develop a generic toolbox that can be used to analyze the quality of metrics. Furthermore, we want to develop metric frameworks so that security levels for physical security, IT security, and cyber-physical security can be derived and compared.

References

Braband, J. (2019). A New Approach towards Likelihood Evaluation in Railway Cyber Security Assessment. In: Proceedings of the Third International Conference on Reliability, Safety, and Security of Railway Systems.

First.org (2022). https://www.first.org/cvss/.

Garcia, M. L. (2005). Vulnerability Assessment of Physical Protection Systems. Sandia National Laboratories, Burlington, Elsevier.

Harnser Group (2010). A Reference Security Management Plan for Energy Infrastructure. European Commission.

Jones, J. R. (2007). Estimating software vulnerabilities. IEEE Security & Privacy, 5(4), 28-32.

Krisper, M. (2021). Problems with Risk Matrices Using Ordinal Scales. arXiv preprint arXiv:2103.05440.

Lichte, D. and K.-D. Wolf (2019). Bayesian network based analysis of cyber security impact on safety. In Proc. European Safety and Reliability Conference (ESREL) (pp. 1502-1509).

Lichte, D., S. Marchlewitz and K.-D. Wolf (2016). A Quantitative Approach to Vulnerability Assessment of Critical Infrastructures With Respect to Multiple Physical Attack Scenarios. In: Future Security 2016, Proc. intern. conf., Berlin, Germany.

SAE (2022). https://www.sae.org/standards/content/iso/sae21434.

Sowa, A. (2011). Metriken–der Schlüssel zum erfolgreichen Security und Compliance Monitoring. Wiesbaden: Vieweg+Teubner Verlag.

Termin, T., D. Lichte and K.-D. Wolf (2021). Risk analysis for mobile access systems including uncertainty impact. In: Proceedings of the 31th European Safety and Reliability Conference and 16th Probabilistic Safety Assessment and Management Conference.

Witte, D., Lichte, D. and K.-D. Wolf (2020). Threat Analysis: Scenarios and Their Likelihoods. In 30th European Safety and Reliability Conference, ESREL 2020 and 15th Probabilistic Safety Assessment and Management Conference, PSAM15 2020 (pp. 4589-4595).

Wheeler, E. (2001). Security Risk Management: Building an Information Security Risk Management Program from the Ground Up, Waltham, Syngress.

Yee, G. O. (2013). Security metrics: An introduction and literature review. Computer and Information Security Handbook, 553-566.

Zio, E. (2012). An introduction to the basics of reliability and risk analyses. Series in Quality, Reliability and Engineering Statistics, Vol. 13, World Scientific.