

Towards Dependability Metrics for Neural Networks

Chih-Hong Cheng*, Georg Nührenberg*, Chung-Hao Huang*, Harald Ruess* and Hirotoshi Yasuoka†

*fortiss - Research Institute of the Free State of Bavaria

Email: {cheng, nuehrenberg, huang, ruess}@fortiss.org

†DENSO CORPORATION

Email: hirotoshi_yasuoka@denso.co.jp

Abstract—Artificial neural networks (NN) are instrumental in realizing highly-automated driving functionality. An overarching challenge is to identify best safety engineering practices for NN and other learning-enabled components. In particular, there is an urgent need for an adequate set of metrics for measuring all-important NN dependability attributes. We address this challenge by proposing a number of NN-specific and efficiently computable metrics for measuring NN dependability attributes including robustness, interpretability, completeness, and correctness.

I. INTRODUCTION

Artificial neural networks (NN) are instrumental in realizing a number of important features in safety-relevant applications such as highly-automated driving. In particular, vision-based perception, the prediction of drivers' intention, and even end-to-end autonomous control are usually based on NN technology. State-of-the-practice safety engineering processes (cmp. ISO 26262) require that safety-relevant components, including NN-enabled ones, demonstrably satisfy their respective safety goals.

Notice that the transfer of traditional testing methods and corresponding test coverage metrics such as MC/DC (cmp. DO 178C) to NN may lead to an exponential (in the number of neurons) number of branches to be investigated [1]. Such an exponential blow-up is not practical as typical NN may be comprised of millions of neurons. Moreover, a straightforward adaptation of structural coverage metrics for NN, e.g., the percentage of activated neurons for a given test set [2], does not take into account that the activation of single neurons is usually not strongly connected to the result of the whole network. The challenge therefore is to develop a set of NN-specific and efficiently computable metrics for measuring various aspects of the dependability of NN.

In previous work we have been generating test cases for NN testing based on finite partitions of the input space and by relying on predefined sets of application-specific scenario attributes [3]. Besides correctness and completeness of NN we also identified robustness [4] and interpretability [1] as important NN dependability attributes.

Here we build on our previous work on testing NN, and we propose a set of metrics for measuring the **RICC** dependability attributes of NN, which are informally described as follows.

- **Robustness** of a NN against various effects such as distortion or adversarial perturbation (which is closely related to *security*).

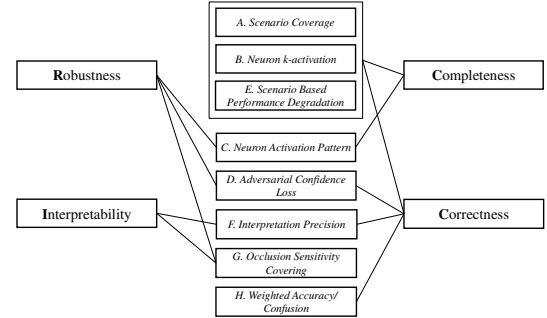


Fig. 1. Relations between **RICC** criteria and the proposed metrics. The group of metrics A., B. and E. cover completeness and correctness.

- **Interpretability** in terms of understanding important aspects of what a NN has actually learned.
- **Completeness** in terms of ensuring that the data used in training has possibly covered all important scenarios.
- **Correctness** in terms of a NN able to perform the perception task without errors.

The main contribution of this paper is an efficiently computable set of NN-specific metrics for measuring **RICC** dependability attributes. Fig. 1 illustrates how the metrics cover the space of **RICC**, where at least two metrics relate to each criterion.


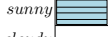

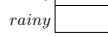

II. QUALITY METRICS

A. Scenario coverage metric \mathcal{M}_{scene}

Similar to the class imbalance problem [5] when training classifiers in machine learning, one needs to account for the presence of all relevant scenarios in training datasets for NN for autonomous driving. A scenario over a list of $\mathcal{C} = \langle C_1, \dots, C_n \rangle$ of operating conditions (e.g., weather and road condition) is given by a valuation of each condition. E.g., let $C_1 = \{sunny, cloudy, rainy\}$ represent the weather condition, $C_2 = \{stone, mud, tarmac\}$ represent the road surfacing, and $C_3 = \{straight, curvy\}$ represent the incoming road orientation. Then $(sunny, stone, straight)$ and $(rainy, tarmac, curvy)$ constitute two possible scenarios.

Since for realistic specifications of operating conditions, checking the coverage of all scenarios is infeasible due to combinatorial explosion, our proposed *scenario coverage metric* is based on the concept of *2-projection* and is tightly connected to the existing work of combinatorial testing, covering arrays and their quantitative extensions [3], [6], [7].

Assumption: Computing the scenario coverage metric requires that the dataset is semantically labeled according to the

C_1, C_2	sunny cloudy rainy	C_1, C_3	straight curvy	C_2, C_3	straight curvy
stone		sunny		stone	
mud		cloudy		mud	
tarmac		rainy		tarmac	



 (sunny, stone, straight)
  (rainy, tarmac, curvy)

Fig. 2. Computing scenario coverage metric via 2-projection table

specified operating conditions, such that for each data point it can be determined whether it belongs to a certain scenario.

Computing \mathcal{M}_{scene} : The metric starts by preparing a table recording all possible *pairs* of operating conditions, followed by iterating each data point to update the table with occupancy. Lastly, compute the ratio between occupied cells and the total number of cells. Eq. 1 summarizes the formula, and an illustration can be found in Fig. 2, where a dataset of two data points $\{(sunny, stone, straight), (rainy, tarmac, curvy)\}$ achieves $\mathcal{M}_{scene} = \frac{2+2+2}{9+6+6}$.

$$\mathcal{M}_{scene} := \frac{\# \text{ of cells occupied by the data set}}{\# \text{ of cells from 2-projection table}} \quad (1)$$

Provided that for each C_i , the size of C_i is bounded by constant α (i.e., the categorization is finite and discrete), then the denominator can at most be $\binom{n}{2}\alpha^2$, i.e., the number of data points required for full coverage is *polynomially* bounded.

Relations to **RICC & improving \mathcal{M}_{scene} :** The metric reflects completeness and correctness attributes of **RICC**. To improve the metric, one needs to discover new scenarios. For the example in Fig. 2, an image satisfying the scenario (cloudy, mud, curvy) can efficiently increase the metric from $\frac{2+2+2}{9+6+6}$ to $\frac{3+3+3}{9+6+6}$.

B. Neuron k -activation metric $\mathcal{M}_{neu-k-act}$

For the frequently used ReLU activation function $f(x) = \max(x, 0)$, a neuron is called active if it outputs a positive value and inactive if it outputs zero. By considering ReLU activation as an indicator of successfully detecting a feature, for close-to-output layers where high-level features are captured, the combination of neuron activation in the same layer also forms scenarios (which are independent from the specified operating conditions). We propose the neuron k -activation metric to measure whether the dataset covers all scenarios.

Again, we encounter combinatorial explosion, e.g., for a layer of 256 neurons, there is a total of 2^{256} scenarios to be covered. Therefore, similar to the 2-projection in the scenario coverage metric, this metric only monitors whether the input set has enabled all activation patterns for every neuron pair or triple in the same layer.

Assumption: The user specifies an integer constant k and a specific layer to be analyzed. Assume that the layer has c neurons.

Computing $\mathcal{M}_{neu-k-act}$: The metric starts by preparing a table recording all possible k -tuples of on-off activation for neurons in the layer being analyzed (similar to Fig. 2 with each C_i now having only 1 and 0 status), followed by iterating each data point to update the table with occupancy. The denominator is given by the number of cells, which has value $\binom{c}{k}(2^k)$.

$$\mathcal{M}_{neu-k-act} := \frac{\# \text{ of occupied cells due to the data set}}{\binom{c}{k}(2^k)} \quad (2)$$

Note that when $k = 1$, our defined neuron k -activation metric $\mathcal{M}_{neu-k-act}$ subsumes commonly seen neuron coverage acting over a single layer [2], [8], where one analyzes the on-off cases for each individual neuron.

Relations to **RICC & improving $\mathcal{M}_{neuron-k-act}$:** The metric reflects the completeness and correctness attribute of **RICC**. To improve the metric, one needs to provide inputs that allows enabling different neuron activation patterns.

C. Neuron activation pattern metric $\mathcal{M}_{neu-pattern}$

Encountering the combinatorial explosion, while k -activation metric captures the completeness, our designed *neuron activation pattern metric* is used to understand the distribution of activation. For inputs within the same scenario, intuitively the activation pattern should be similar, implying that the number of activated neurons should be similar.

Assumption: The user provides an input set In , where all images belong to the same scenario, and specifies a layer of the NN (with c neurons) to be analyzed. Furthermore, the user chooses the number of groups γ , for a partition of In into γ groups $G_1(\text{In}), \dots, G_\gamma(\text{In})$, where for group $G_i(\text{In})$, $i \in \{1, \dots, \gamma\}$, the number of activated neurons in the specified layer is within the range $[\frac{c}{\gamma}(i-1), \frac{c}{\gamma}(i)]$ for each input in this group.

Computing $\mathcal{M}_{neu-pattern}$: Let $G_j(\text{In})$ be the largest set among $G_1(\text{In}), \dots, G_\gamma(\text{In})$. Then the metric is evaluated by considering all inputs whose activation pattern, aggregated using the number of neurons being activated, significantly deviates from the majority.

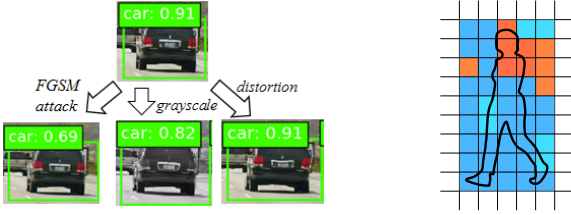
$$\mathcal{M}_{neu-pattern} := \frac{\sum_{i: i \notin \{j-1, j, j+1\}} |G_i(\text{In})|}{|\text{In}|} \quad (3)$$

Relations to **RICC & improving $\mathcal{M}_{neu-pattern}$:** This metric reflects the robustness and completeness attribute of **RICC**, as well as interpretability. To improve the metric, one requires careful examination over the reason of diversity in the activation pattern under the same scenario.

D. Adversarial confidence loss metric \mathcal{M}_{adv}

Vulnerability w.r.t. adversarial inputs [9] is an important quality attribute of NNs, which are used for image processing and designed to be used in safety-critical systems. As providing a formally provable guarantee against all possible adversarial inputs is hard, our proposed adversarial confidence loss metric is useful in providing engineers an estimate of how robust a NN is.

Assumption: Computing \mathcal{M}_{adv} requires that there exists a list of input transformers $\langle T_1, \dots, T_n \rangle$ where for each T_i , ($i \in \{1, \dots, n\}$), given a parameter ϵ specifying the allowed perturbation, one derives a new input $\text{in}' = T_i(\text{in}, \epsilon)$ by transforming input in . Each T_i is one of the known image perturbation techniques ranging from simple rotation, distortion, to advanced techniques such as FGSM [10] or deepfool [11].



(a) A vehicle image and three perturbed images. The largest classification performance drop is achieved by the FGSM technique. (b) This heatmap for a pedestrian contains nine hot pixels in orange, 30 occluding pixels and five hot and occluding pixels.

Fig. 3. Illustrating \mathcal{M}_{adv} and a heatmap for $\mathcal{M}_{interpret}$ and \mathcal{M}_{OccSen} .

Computing \mathcal{M}_{adv} : Given a test set \mathcal{I}_n , a predefined perturbation bound ϵ , and the list of input transformers, let $\text{NN}(\text{in})$, where $\text{in} \in \mathcal{I}_n$, be the output of the NN being analyzed, with larger value being better¹. The following equation computes the adversarial perturbation loss metric.

$$\mathcal{M}_{adv} := \frac{\sum_{\text{in} \in \mathcal{I}_n} \min_{i \in \{1, \dots, N\}} \text{NN}(T_i(\text{in}, \epsilon)) - \text{NN}(\text{in})}{|\mathcal{I}_n|} \quad (4)$$

Intuitively, \mathcal{M}_{adv} analyzes the change of output value for input in due to a perturbation ($\text{NN}(T_i(\text{in}, \epsilon)) - \text{NN}(\text{in})$), and selects one which leads to largest performance drop among all perturbation techniques, i.e., it makes the computed value of $\text{NN}(T_i(\text{in}, \epsilon)) - \text{NN}(\text{in})$ most negative. A real example is shown in Fig. 3a, where the FGSM attack yields the largest classification performance drop among three perturbation techniques, which changes the probability of car from 0.91 to 0.69. Thus, the largest negative value of the probability difference $\text{NN}(T_i(\text{in}, \epsilon)) - \text{NN}(\text{in})$ for this image is -0.22 . Lastly, average the computed value over all inputs being analyzed.

Relations to RICC & improving \mathcal{M}_{adv} : The metric has a clear impact on robustness and correctness. To improve the metric, one needs to introduce perturbed images into the training set, or apply alternative training techniques with provable bounds [12].

E. Scenario based performance degradation metric

Here we omit details, but for commonly seen performance metrics such as validation accuracy or even quantitative statistic measures such as MTBF, one may perform detailed analysis by either considering each scenario, or by discounting the value due to missing input scenarios (the discount factor can be taken from the computed scenario coverage metric).

F. Interpretation precision metric $\mathcal{M}_{interpret}$

Since image classification and object detection are the main applications for NN in automated driving, we propose two specialized metrics for these applications. The interpretation precision metric is intended to judge if a classification or object detection is based on the correct part of the image. E.g., the metric can reveal that a certain class of objects is mostly identified by its surroundings, maybe because it only

exists in similar surroundings in the training and validation data. In this case, engineers should test whether this class of object can also be detected in different contexts.

Assumption: For computing this metric, we need a validation set that has image segmentation ground truth in addition to the ground truth classes (and bounding boxes), e.g., as in VOC2012 data set [13].

Computing $\mathcal{M}_{interpret}$: Here we describe how the metric can be computed for a single detected object, where one can extend the computation to a set of images by posing average or min/max operators. A real example demonstrating the exact computation is shown in Fig. 4.

- 1) Run the NN on the image to classify an object with probability p (and obtain a bounding box in the case of object detection).
- 2) Compute an occlusion sensitivity heatmap H , where each pixel of the heatmap $h \in H$ maps to a position of the occlusion on the image [14]. The value of h is given by the probability of the original class for the occluded image. For object detection we take the maximum probability of the correct class over all detected boxes that have a significant Jaccard similarity with the ground truth bounding box.
- 3) For given probability threshold ρ that defines the set of hot pixels as $P_{hot} = \{h \in H \mid h < \rho\}$ and the set of pixels that partly occlude the segmentation ground truth, denoted by $P_{occluding}$, the metric is computed as follows:

$$\mathcal{M}_{interpret} = \frac{|P_{hot} \cap P_{occluding}|}{|P_{hot}|} \quad (5)$$

An illustrative example of computing $\mathcal{M}_{interpret}$ can be found in Fig. 3b, where for the human figure only five out of nine hot pixels intersect the region of the human body. Thus $\mathcal{M}_{interpret} = \frac{5}{9}$. The set of thirty pixels constituting the human forms $P_{occluding}$.

Relations to RICC & improving $\mathcal{M}_{interpret}$: The interpretation precision metric contributes to the interpretability and correctness of the RICC criteria. It may reveal that a NN uses a lot of context to detect some objects, e.g., regions surrounding the object or background of the image. In this case, adding images where these objects appear in different surroundings can improve the metric.

G. Occlusion sensitivity covering metric \mathcal{M}_{OccSen}

This metric measures the fraction of the object that is sensitive to occlusion. Generally speaking, it is undesirable to have a significant probability drop if only a small part of the object is occluded.

Furthermore, care should be taken about the location of the occlusion sensitive area. If a certain part of an object class is occlusion sensitive in many cases (e.g., the head of a dog) it should be tested if the object can still be detected when this part is occluded (e.g., head of a dog is behind a sign post). \mathcal{M}_{OccSen} is computed in a similar way and based on the same inputs as $\mathcal{M}_{interpret}$:

- 1) Perform steps 1) and 2) and determine P_{hot} and $P_{occluding}$ as for $\mathcal{M}_{interpret}$.

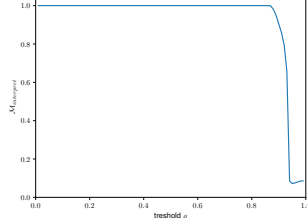
¹The formulation assumes a single-output NN, but it can be easily extended to multi-output scenarios.



(a) Result of object detection



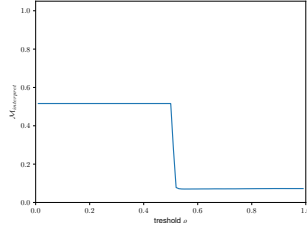
(b) Heatmap for red car (bottom left)



(c) $M_{interpret}$ for ρ



(d) Heatmap for the right person



(e) $M_{interpret}$ for ρ

Fig. 4. Computing $M_{interpret}$ for red car and the right person in front of the red car. The metric shows that the red car is mostly identified by the correct areas. On the other hand, for the person there are a lot of hot pixels in incorrect regions.

$$2) \text{ Derive } \mathcal{M}_{OccSen} := \frac{|P_{hot} \cap P_{occluding}|}{|P_{occluding}|}.$$

If the value is high it indicates that many positions of small occlusions can lead to a detection error. A low value indicates that there is a greater chance of still detecting the object when it is partly occluded. An illustrative example of computing \mathcal{M}_{OccSen} can be found in Fig. 3b, where for the human figure the heatmap only contains five hot pixels intersecting the human body (the head). As there are 30 pixels intersecting the region of the human, we have $\mathcal{M}_{OccSen} = \frac{5}{30}$.

Relations to RICC & improving \mathcal{M}_{OccSen} : Occlusion sensitivity coverage covers the robustness and interpretability of **RICC**. If the metric values are too high for certain kinds of objects, an approach to improve it is to augment the training set with more images where these objects are only partly visible.

H. Weighted accuracy/confusion metric $\mathcal{M}_{confusion}$

In object classification, not all errors have the same severity, e.g., confusing a pedestrian for a tree is more critical than in the opposite way. Apart from pure accuracy measures, one may employ fine-grained analysis such as specifying penalty terms as weights to capture different classification misses.

As such a technique is standard in performance evaluation of machine learning algorithms, the specialty will be how the weights of confusion are determined. Table I provides a summary over penalties to be applied in traffic scenarios, by reflecting the safety aspect. Misclassifying a pedestrian (or bicycle) to be background image (i.e., no object exists) should

TABLE I
QUALITATIVE SEVERITY OF SAFETY TO BE REFLECTED AS WEIGHTS

A is classified to B	B (pedestrian)	B (vehicle)	B (background)
A (pedestrian)	n.a. (correct)	++	++++
A (vehicle)	+	n.a. (correct)	+++
A (background)	+	+	n.a. (correct)

be set with highest penalty, as pedestrians are unprotected and it may easily lead to life threatening situations.

Relations to RICC & improving $\mathcal{M}_{confusion}$: The metric is a fine-grained indicator on correctness. To improve the metric, either one trains the network with more examples, or one modifies the loss function such that it is aligned with the weighted confusion, e.g., it sets higher penalty term when misclassifying a “pedestrian” to “background”.

III. OUTLOOK

We propose a set of NN-specific and efficiently computable metrics for measuring the RICC dependability attributes of NN. At this point, we have also implemented a NN testing tool for evaluating the usefulness of our proposed set of metrics in on-going industrial NN developments. Our ultimate goal is to obtain a complete and validated set of NN dependability metrics. In this way, corresponding best practices can be identified as the basis of new safety processes for engineering NN-enabled components and systems.

REFERENCES

- [1] C.-H. Cheng, F. Diehl, G. Hinz, Y. Hamza, G. Nührenberg, M. Rickert, H. Ruess, and M. Truong-Le, “Neural networks for safety-critical applications challenges, experiments and perspectives,” in *DATE*. IEEE, 2018, pp. 1005–1006.
- [2] K. Pei, Y. Cao, J. Yang, and S. Jana, “Deepxplore: Automated whitebox testing of deep learning systems,” in *SOSP*. ACM, 2017, pp. 1–18.
- [3] C.-H. Cheng, C.-H. Huang, and H. Yasuoka, “Quantitative projection coverage for testing ml-enabled autonomous systems,” *arXiv preprint arXiv:1805.04333*, 2018.
- [4] C.-H. Cheng, G. Nührenberg, and H. Ruess, “Maximum resilience of artificial neural networks,” in *ATVA*. Springer, 2017, pp. 251–268.
- [5] N. Japkowicz and S. Stephen, “The class imbalance problem: A systematic study,” *Intelligent data analysis*, vol. 6, no. 5, pp. 429–449, 2002.
- [6] J. Lawrence, R. N. Kacker, Y. Lei, D. R. Kuhn, and M. Forbes, “A survey of binary covering arrays,” *the electronic journal of combinatorics*, vol. 18, no. 1, p. 84, 2011.
- [7] C. Nie and H. Leung, “A survey of combinatorial testing,” *ACM Computing Surveys (CSUR)*, vol. 43, no. 2, p. 11, 2011.
- [8] “Functional safety beyond iso26262 for neural networks in highly automated driving,” http://autonomous-driving.org/wp-content/uploads/2018/04/Functional_Safety_beyond_ISO26262_for_Neural_Networks_Exida_Florian_ADM5.pdf, accessed: 2018-06-01.
- [9] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, and R. Fergus, “Intriguing properties of neural networks,” *arXiv preprint arXiv:1312.6199*, 2013.
- [10] I. J. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” *arXiv preprint arXiv:1412.6572*, 2014.
- [11] S. M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, “Deepfool: a simple and accurate method to fool deep neural networks,” in *CVPR*, no. EPFL-CONF-218057, 2016.
- [12] J. Z. Kolter and E. Wong, “Provable defenses against adversarial examples via the convex outer adversarial polytope,” *arXiv preprint arXiv:1711.00851*, 2017.
- [13] M. Everingham, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman, “The PASCAL Visual Object Classes Challenge 2012 (VOC2012) Results,” <http://www.pascal-network.org/challenges/VOC/voc2012/workshop/index.html>.
- [14] M. D. Zeiler and R. Fergus, “Visualizing and understanding convolutional networks,” in *ECCV*. Springer, 2014, pp. 818–833.