PESARO 2018

The Eighth International Conference on Performance, Safety and Robustness in Complex Systems and Applications

ISBN: 978-1-61208-628-6

April 22 - 26, 2018

Athens, Greece

PESARO 2018 Editors

Michael Hübner, Ruhr-University Bochum, Germany
Claus-Peter Rückemann, Leibniz Universität Hannover / Westfälische Wilhelms-Universität Münster / North-German Supercomputing Alliance (HLRN), Germany

PESARO 2018

Forward

The Eighth International Conference on Performance, Safety and Robustness in Complex Systems and Applications (PESARO 2018), held between April 22, 2018 and April 26, 2018 in Athens, Greece, continued a series of events dedicated to fundamentals, techniques and experiments to specify, design, and deploy systems and applications under given constraints on performance, safety and robustness.

There is a relation between organizational, design and operational complexity of organization and systems and the degree of robustness and safety under given performance metrics. More complex systems and applications might not be necessarily more profitable, but are less robust. There are trade-offs involved in designing and deploying distributed systems. Some designing technologies have a positive influence on safety and robustness, even operational performance is not optimized. Under constantly changing system infrastructure and user behaviors and needs, there is a challenge in designing complex systems and applications with a required level of performance, safety and robustness.

The conference had the following tracks:

- Machine Learning Algorithms in Image and Signal Processing
- Safety and Robustness

We take here the opportunity to warmly thank all the members of the PESARO 2018 technical program committee, as well as all the reviewers. The creation of such a high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated their time and effort to contribute to PESARO 2018. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

We also gratefully thank the members of the PESARO 2018 organizing committee for their help in handling the logistics and for their work that made this professional meeting a success.

We hope that PESARO 2018 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in the area of on performance, safety and robustness in complex systems and applications. We also hope that Athens, Greece, provided a pleasant environment during the conference and everyone saved some time to enjoy the historic charm of the city.

PESARO 2018 Chairs

PESARO Steering Committee

Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway
Mohammad Rajabali Nejad, University of Twente, the Netherlands
Omar Smadi, Iowa State University, USA

Yulei Wu, University of Exeter, UK

PESARO Industry/Research Advisory Committee
John Favaro, INTECS, Italy
Jean-Pierre Seifert, TU Berlin & FhG SIT Darmstadt, Germany
Roger Rivett, Jaguar Land Rover, UK

PESARO 2018
Committee

PESARO Steering Committee
Wolfgang Leister, Norsk Regnesentral (Norwegian Computing Center), Norway
Mohammad Rajabali Nejad, University of Twente, the Netherlands
Omar Smadi, Iowa State University, USA
Yulei Wu, University of Exeter, UK

PESARO Industry/Research Advisory Committee
John Favaro, INTECS, Italy
Jean-Pierre Seifert, TU Berlin & FhG SIT Darmstadt, Germany
Roger Rivett, Jaguar Land Rover, UK

PESARO 2018 Technical Program Committee
Morteza Biglari-Abhari, University of Auckland, New Zealand
Quentin Bramas, University of Strasbourg, France
Andrea Ceccarelli, University of Florence, Italy
Salimur Choudhury, Algoma University, Canada
Dieter Claeys, Ghent University, Belgium
Frank Coolen, Durham University, UK
Faten Fakhfakh, University of Sfax, Tunisia
John Favaro, INTECS, Italy
Francesco Flammini, UMUC Europe, Italy
Víctor Flores Fonseca, Universidad Católica del Norte, Chile
John-Austen Francisco, Rutgers, the State University of New Jersey, USA
Simos Gerasimou, University of York, UK
Denis Gingras, Université de Sherbrooke, Canada
Teresa Gomes, University of Coimbra, Portugal
Denis Hatebur, University Duisburg-Essen, Germany
Mohamed Hibti, EDF R&D, France
Hind Castel, Telecom SudParis | Institut Mines Telecom, France
C. Michael Holloway, Safety-Critical Avionics Systems Branch | NASA Langley Research Center, Hampton, Virginia, USA
Christoph-Alexander Holst, Institute Industrial IT / OWL University of Applied Sciences, Germany
Rémy Houssin, University of Strasbourg, France
Michael Hübner, Ruhr-University of Bochum, Germany
Christos Kalloniatis, University of the Aegean, Greece
Atsushi Kanai, Hosei University, Japan
Sokratis K. Katsikas, Norwegian University of Science & Technology (NTNU), Norway
M.-Tahar Kechadi, University College Dublin (UCD), Ireland
Peter Kieseberg, SBA Research, Austria

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Exploring Deep Neural Networks for Regression Analysis

Florian Kästner, Benedikt Janßen, Frederik Kautz, Michael Hübner
Chair for Embedded Systems of Information Technology
Ruhr-University Bochum, Bochum, Germany
Email: {Florian.Kaestner, Benedikt.Janssen, Frederik.Kautz, Michael.Huebner}@rub.de

***Abstract*—Designing artificial neural networks is a challenging task due to the vast design space. In this paper, we present our exploration on different types of deep neural networks and different shapes for a regression analysis task. The network types range from simple multi-layer perceptron networks to more complex convolutional and residual neural networks. Within the exploration, we analyzed the behavior of the different network shapes, when processing measurement data characteristic for mass spectrometers. Mass spectrometers are used to determine single substances within gaseous mixtures. By applying deep neural networks for the measurement data processing, the behavior of the measurement system can be approximated indirectly through the learning process. In addition, we evaluate the usage of reinforcement learning to design the neural network's architecture.**

Keywords–ANN; MLP; CNN; Reinforcement Learning.

I. INTRODUCTION

In traditional machine learning approaches, manually designed features have to be provided for the input data. Extracting reasonable features is crucial for a successful usage of those algorithms. Moreover, the process of feature extraction is time consuming and requires expert knowledge regarding the specific applications. In contrast, Artificial Neural Networks (ANNs) are capable of automatically extracting features from given input data, superseding manually designed features. Furthermore, the increasing depth of Deep Neural Networks (DNNs) allows extracting very complex and abstract features out of several different representations with respect to prior levels. All these features are then used to form a proper output.

However, the design of ANNs is a challenging task due to the degrees of freedom for their architecture, such as depth of the ANN, width and type of the layers, as well as data flow paths. In addition, the training method has an impact on the ANN's performance, and has several degrees of freedom itself, for instance the initial parameter values, the batch size, the learning rate, and optimization algorithm.

In this paper, we present our results of the exploration of end-to-end trained ANNs for the processing of mass spectra measured with a miniaturized mass spectrometer [1]. Mass spectra allow the analysis of gaseous mixtures to determine their constituents. Within the exploration, we used a gaseous mixture with the constituents listed in Table I. In order to exclude any unknown effects of real measurement systems, we created a Python module to generate noisy mass spectra of the given mixture, based on the constituents' characteristic mass-to-charge ratio peaks. The noise is evenly distributed, and explained in Figure 1 a), Figure 1 b) shows the resulting spectra. The generated mass spectra are normalized so that the sum of the constituents adds up to one. The noise within the generated mass spectra and the mass spectra's minimal and maximal, as well as mean values are depicted in Figure 1. In summary, our goal is to extract the constituents' concentration of the generated noisy mass spectra, without assuming any pre-conditional knowledge. This type of problem definition for machine learning is called multi-output-regression.

TABLE I. DATA SET CONCENTRATION RANGE OF CONSTITUENTS

Constituent	Concentration range
H_2O	0.0 % - 3.0 %
CO_2	0.2 % - 5.6 %
N_2	65.0 % - 80.0 %
O_2	15.0 % - 21.0 %

Within the scope of the exploration, we analyzed the structure and hyper parameters of different kinds of ANNs suitable for this purpose, implemented with TensorFlow [2] without manually extracting features. Due to the time-invariant application we focus on feedforward-ANNs starting with the traditional Multi-Layer Perceptrons (MLPs). MLPs consist of at least three *fully-connected layer*, in which every neuron is connected to every neuron in the previous layer. In order to use spatial information in the signal and lower the number of parameters, we included Convolutional Neural Networks (CNNs). CNNs apply filter kernels on the input data that compute the dot product, and thus combine spatial information [3]. In addition, CNNs apply pooling layers that reduce the data dimension by down-sampling.

For every layer we apply the Rectifier Linear Unit *ReLU*-activation function, due to its properties of smoothing the issue of vanishing or exploding gradients as shown by Glorot et al. [4]. Another important property of this activation function applied to ANNs is the *sparse activation*, meaning that a certain number of neurons within a network will never fire. Although, this feature is desirable when designing ANNs, our exploration results of the network size could be influenced, due to the varying number of dead neurons. However, in order to not further increase the exploration complexity, we assume that this property does not influence the exploration, if the weight initialization is uniformly distributed.

To speed-up training, smooth the issue of exploding gradients, and to avoid over-fitting we use batch normalization with trainable scale and shift parameters. Within the scope of this work, we relinquish further methods avoiding over-fitting like dropout.

Although, applying batch normalization and ReLU-activation function relieves the issue of vanishing or exploding gradients, the problem still exists and becomes more crucial when the network is deeper. Therefore, we extend our exploration with *Residual neural Networks* (ResNets), and *highway networks*. The distinctive property of ResNets are *shortcuts*. Shortcuts implement the possibility to route the data flow around layers, and afterwards recombine the processed and

 ISBN: 978-1-61208-628-6

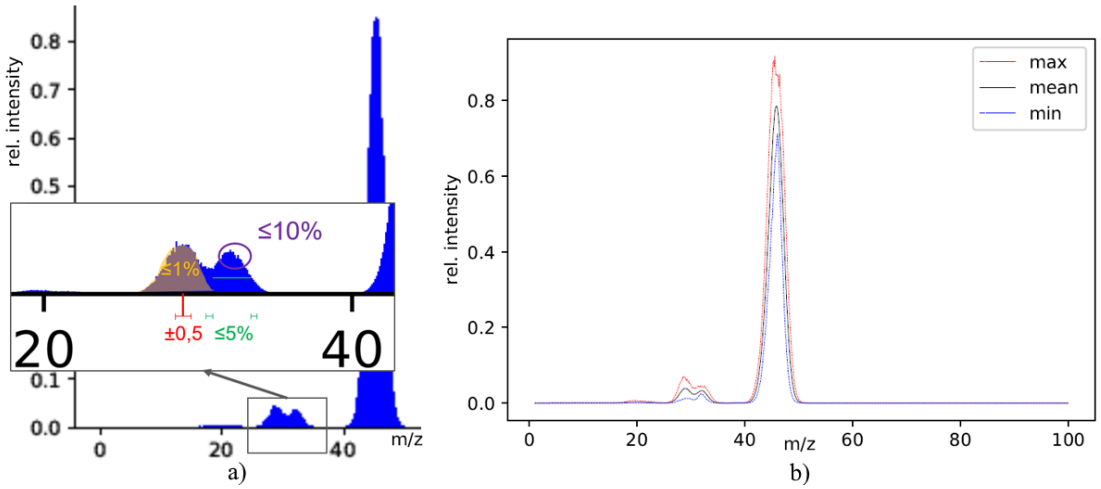

Figure 1. Mass spectra: area of each constituent peak varies by $\leq 1\,\%$, position by $\pm 0.5\,\frac{m}{z}$, variance by $\leq 5\,\%$, and each measurement value by $\leq 10\,\%$.

bypassed data [5]. In particular, the bypassing is done by an identity shortcut connection. Thus, the original residual block simply adds the outcome of the convolution layers with the original input. If the dimensions do not match after applying convolution due to stride, padding and amount of feature map parametrization, the input can be compressed, preferably with not trainable methods, or extended through padding. Shortcut methodologies are subject to current research. Due to the shortcut connections, the influence of vanishing gradients is far lower than with traditional ANNs. Moreover, the back-propagation can be applied much more efficient and simpler. Highway networks follow a similar approach, however, they employ a gating function optimized within the training phase to filter the data through the shortcut [6].

The related work within this field of research is presented in Section II. The method of our exploration is twofold. We further used Reinforcement Learning (RL) to automate the exploration for the MLP networks. The results of the RL based exploration can be found in Section IV. A discussion and summary of the current results, as well as an outlook to future work can be found in Section V.

II. Related Work

An early work within the direction of our approach was published by Massicotte et al. [7], who investigated into the calibration of high-pressure measurement systems with MLP networks. The authors compared an ANN-based method to a spline-based method, and state that the ANN-based method achieves better results with lower quality reference data, and thus, enables a reduction of the time necessary for calibration data acquisition. Moreover, the spline-based method requires the parallel measurement of the temperature to consider temperature effects, which is not the case for the Ann-based method.

Several different classification methods for analyzing mass spectra data were analyzed by the authors of [8]. Those classification methods include linear discriminant analysis, quadratic and discriminant analysis, k-nearest neighbor classifier, classification trees, Support Vector Machines (SVMs), and random forest. Wu et al. found that Random Forrest outperforms the other classification methods in overall misclassification as well as in stable assessment of classification errors.

The authors of [9] used an unsupervised method for extracting features from mass spectra data followed by classification realized with SVMs. Their methodology results in greater 95 % correctly classified samples.

The work described in [10] uses a RL method (Q-learning) based algorithm capable of generating high performance standard CNN. Created CNNs are outperforming existent networks with similar layer types and are competitive with state of the art networks making use of more complex layer types.

Referring to the screening methodology in the medical and genetic fields, the authors of [11] developed an approach which randomly generates a high number of networks with different parameter initialization and architectures. Configurations that show good results are used for further training. Regarding the steady growth of computational power Pinto et al. [11] claim that this approach can speed up development success and understanding of biological vision.

With the use of Cartesian Genetic Programming (CGP), Suganuma et al. [12] automatically construct a CNN for an image classification task with CIFAR-10 data set. Within the process the CNN structure is represented by CGP encoding method and is further optimized to reach best possible results. With this approach the authors claim to automatically find network architectures which are comparable with common state of the art CNNs.

III. Empirical Exploration

Within this Section we demonstrate our approach to explore the shape of four different types of ANNs. The goal is to investigate, which structure suits best for the given qualitative analysis. This task represents a complex empirical optimization due to the high amount of adjustable hyperparameters, including among others batch-size, optimizer, and learning rate. Thus, the empirical approach can be seen as a starting point for further explorations preferably using optimization method such as RL described in Section IV.

The input vector consists of 990 floating point values representing the mass spectra from 0 to $100\,\frac{m}{z}$. The last layer of

 ISBN: 978-1-61208-628-6

every ANN within this work is built as a fully-connected layer with four neurons representing the constituents concentrations, where no activation function is applied. Due to the regression task we define the cost function as the Mean Squared Error (MSE) between the labeled constituents concentrations and the outcome of the last layer. The corresponding loss function is defined in Equation 1, with the true value y and the prediction $\hat{y}$ for each of the four constituent.

$$MSE = \frac{1}{4}\sum_{i=0}^{4}(y_i - \hat{y}_i)^2 \quad (1)$$

We apply batch normalization with trainable scale and shift parameters for all networks at certain points in hierarchical structure. For training we use a fixed batch size consisting of 25 randomly picked samples and Adaptive Moment Estimation (Adam) as the optimization method. The Adam optimizer was chosen due to the adaptive learning rate for every parameter and its good results dealing with sparse gradients. For further information, we refer to [13]. Those sparse gradients can result from the properties of ReLU activation function. As a weight initialization we choose the *Xavier method* [14]. To avoid overfitting, we apply early stopping. The break condition is an increasing deviation of the prediction from the label of the last three to the previous three predictions of the verification dataset, after the network has been trained with all samples in the dataset consisting of 100000 mass spectra. After the training, we verify the accuracy of the networks based on the deviation of the output of the last layer and the corresponding labels using a new dataset of 10000 mass spectra.

A. Multi-Layer Perceptron Network

For the exploration of MLP networks, we created networks with different depths, starting from three up to 13 layers. The choice of the layer sizes is based on NumPy's *logspace()* function with base 10.0, generating a list of layers defined by the input layer size and the output layer size. The input layer size has been set within the range of $1.1\times$ to $0.05\times$ of the length of the input vector. We assume that the resulting funnel-shape of the networks is a suitable approximation to follow the feature extracting policy in order to raise the depth of the network with a sufficient number of neurons within the layers. This implies that we assume the data to be compressed and the function of the network is more dependable on the depth than on the width of the layers. We further save a significant number of parameters when downsizing the width of the fully-connected layers. The observed deviation on the test dataset is depicted in Figure 2. With an increasing depth of the network, the deviation tends to be larger. The best overall result for this exploration is achieved with a depth of four fully-connected layers with a mean of 1.5 %. The result of the exploration matches our expectations. The vanishing gradient problem prevent the network to perform better with increasing network depth. This represents a well-known problem in the deep learning domain. In Section III-C, we tackle this problem with the introduction of residual blocks allowing us to build deeper networks.

B. Convolutional Neural Network

CNNs are a famous type of ANNs in the computer vision domain, especially in object detection, segmentation and tracking applications [15]. They are mainly responsible for

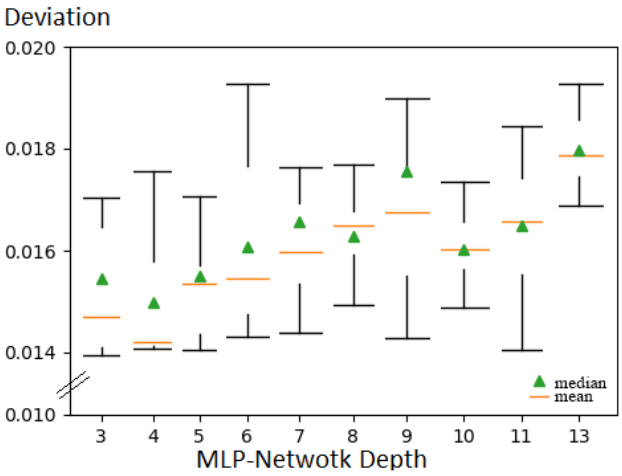

Figure 2. Deviations for different MLP configurations.

the today's popularity of ANNs due to their success in this field starting with ImageNet in 2011. One reason for their success is the property of the corresponding convolutional layer to combine spatial information applying 2-dimensional filter kernels to the input followed by pooling to reduce dimensions along the depth of the network. We also want to take advantage of these feature assuming the existence of spatial relationships.

Instead of reshaping the input and perform a 2-dimensional convolution we apply a 1-dimensional convolution with different kernel-sizes and filter-depths. The output of this convolution is a 2-dimensional feature map, which consist of corresponding height and depth. We further could apply a 2-dimensional convolution. However, we still assume that the spatial relationships only exist among the first dimension. Therefore, we decide to use 2-dimensional 1x1 convolution to reduce the shape back to a 1-dimensional outcome. To also reduce the shape among the first dimension we can apply the 1-dimensional convolution with a specific stride. The feature map shape of the 1 dimension is then given by the quotient of the 1 dimension of the input shape and the stride. These two convolutions represent the basic block of our CNN. The basic principle is visualized in Figure 3.

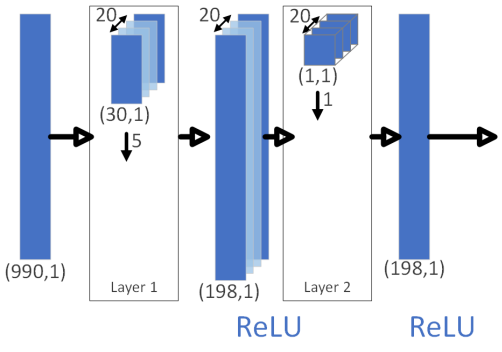

Figure 3. Visualization of the basic CNN principle.

We design the CNN by simply stacking those basic blocks and adjusting the hyperparameters, which are the stride, the

 ISBN: 978-1-61208-628-6

number of feature maps, and the kernel size. The output of the last basic block is fed to a fully-connected layer with a fixed number of neurons of 99 followed by the output layer. The exploration is done with five CNNs ranging from two to six stacked basic blocks. We reduce the shape of the first dimension by using a stride of five in the first basic block. We further use a stride of two in the last basic block except for the first CNN, where just two basic blocks are involved. The stride parameter for all other basic blocks is set to one. The kernel size and number of kernels within a layer varies, starting with a wide kernel and a low number of kernels. Table II lists the chosen CNN configurations. While going deeper, we downscale the kernel size and increase the kernel depth. The result of this evaluation can be seen in Figure 4. Contrary to the MLP exploration, the accuracy does not drop rapidly as the network depth's increases, instead the deviation on the test dataset is approximately the same. Therefore, we follow that the influence of vanishing gradient is intensified in MLP networks. CNNs can be deeper, as the convolution requires less parameters, and owns an aggravated forward- and backpropagation path, due to the spatial connections, compared with the MLP network. The overall accuracy is slightly lower compared to those of the MLP exploration. To design deeper networks, we add block-wise shortcuts to the MLP and CNN as introduced in the next Section.

TABLE II. CNN CONFIGURATIONS EXPLORED

number of stacked basic blocks	List of layer configurations with [(kernelsize,number of kernels)] in hierarchical order
2	[(15,30),(10,60)]
3	[(15,20),(10,30),(5,60)]
4	[(15,20),(10,30),(10,60),(5,300)]
5	[(30,20),(20,30),(20,80),(10,200),(5,400)]
6	[(30,20),(20,30),(10,60),(5,180),(1,300),(3,500)]

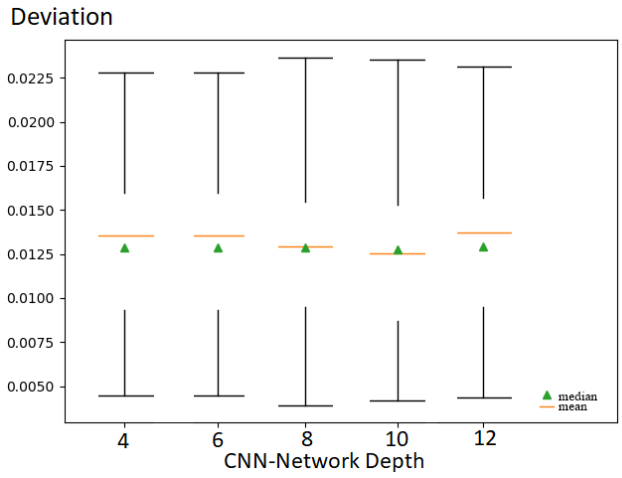

Figure 4. Deviations for different CNN configurations.

C. Residual and Highway Network

Residual Networks or ResNets are the state-of-the-art networks for various applications and especially famous in image recognition tasks. He et al. [16] reformulated the layers to learn residual functions with respect to the input of the layer. This basic principle eases the learning due to the stepwise

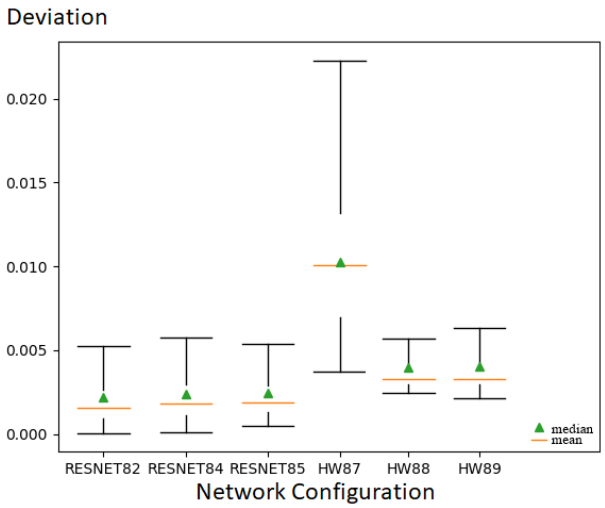

Figure 5. Deviations for different ResNet and Highway configurations.

replacement of the product with the sum of the output of the layers in the backward path, and thereby reduces the problem of vanishing gradients rapidly. Thus, He et al. were able to design a ResNet with 152 stacked layers which outperformed all previous plain networks. We adopt this principle to our needs extending our basic convolution pair described in Section III-B with an identity mapping. The resulting principle residual block is shown in Figure 6. For simplicity reasons, we forego to reduce the shape of the first dimension. Thus, the dimensions of the input and the output of the block are the same. If this would be not the case the input has to be downscaled or upscaled, preferable without or a low number of trainable parameters. To downscale the first dimension among the depth of the network at certain points, we apply the basic convolution pair without shortcuts with a specific stride after a significant number of residual blocks. This could also be replaced with a pooling layer in the future.

A similar principle is used with Highway Networks. The main difference is the use of a gating function for identity mapping. However, this difference is only valid considering the original ResNet and the original Highway Network. Recent developments regarding different types of ResNet blurred these difference [17]. In the original highway network, developed by Srivastava et al. [18], the output y of a basic highway block is defined as follows:

$$y = F(x, \boldsymbol{W_F}) \cdot T(x, \boldsymbol{W_T}) + x \cdot (1 - T(x, \boldsymbol{W_T})) \quad (2)$$

Where x represents the input of the layer and F represents the nonlinear activation function with the weight parameters $\boldsymbol{W_F}$. T is defined as the transform gate, while the term $1 - T$ is depicted as the carry gate. This gating units can be seen as a learnable dataflow control unit through the network. We use this principle to continue our exploration. Therefore, we extend fully-connected layers with this gating unit. Similar to the ResNet approach we keep the dimensions equal inside the block units. We further apply fully-connected layers without gating units after a significant amount of highway blocks in order to reduce the shape of the first dimension.

Figure 5 shows the deviation result of 3 different configurations based on our residual and highway basic blocks. The

 ISBN: 978-1-61208-628-6

residual blocks consist of a 1-dimensional convolution with kernel size 15, and 5 or 10 kernels, as well as a 2-dimensional 1×1 convolution. For the ResNet exploration we used 120, 80, and 40 layers. For the exploration of the highway network, we analyzed configurations with 24×500 and 24×20, 35×100 and 35×50, as well as 30×100 and 30×50 highway layers.

ResNet82 performs best on the given test dataset with an mean deviation of 0.24 %. This network represents also the deepest one in our exploration containing 120 layers. However, the deviation difference to the other *ResNet* configurations are negligible. For instance, *ResNet85* consists of only 40 layers with mean deviation of 0.238 % on the test dataset. The highway network *HW87* is built with 48 highway blocks and owns a very low overall accuracy. In comparison, *HW88*, consisting 70 blocks, and *HW89*, consisting 60 blocks, perform better on the test dataset. This corresponds to our expectations as the results of the exploration of Srivastava et al. [18] also show a similar tends, where the accuracy is not sufficient for smaller highway Networks and increases with increasing depth.

Figure 8 shows the validation error during training of the best performing ANN of every type of ANN we explored over 500000 epochs. As can be seen, the ResNet82 converges very fast and without high fluctuations till break conditions. The MLP network with four layers is comparable to the other ANN types. The CNN with 10 convolution pairs started to converge faster but did not improve the prediction after 20000 epochs. HW88 shows a very fluctuating convergence, especially at the early training epochs. While parametrization of the gating units starts to work properly, the deviation with the validation dataset drops.

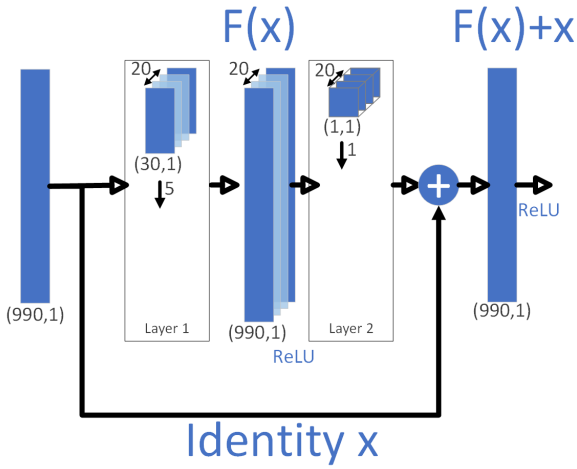

Figure 6. Visualization of the residual block principle.

IV. Reinforcement Learning

As shown in Section III, the exploration of ANNs is a very complex optimization problem. Therefore, we start to explore the shape of ANNs with RL. The first results of this heuristic exploration are described in this Section. In general, a RL problem is based on the Markov decision process, in which an agent is taking actions, measuring the reaction of the environment, updating the policy and taking a new action based on the previous information. For further investigations we refer to [19]. For our purpose, we use a Q-learning methodology, which is a model-free, off-policy, temporal difference RL method. We focused the RL-based exploration on the MLP networks shape, in order to receive a MLP configuration with a sufficient accuracy. More precisely, we train an agent to the design an MLP network for our application. Thus, we first have to define a discrete state-action space. Starting from one hidden layer after the fixed size of the input layer, the agent can choose at every step either to add 10 neurons to the current layer or to extend the network with another hidden layer starting with 10 neurons reaching a new state. At each step the network is trained with the same hyperparameters outlined in Section III. The maximum width of every hidden layer consists of 400 neurons, while the maximum depth is set to 10 layers. If the agent is reaching a depth of 10 layers, or a deviation on the validation dataset below 0.1 %, the episode is stopped. The reward is defined as the reciprocal deviation on the validation dataset.

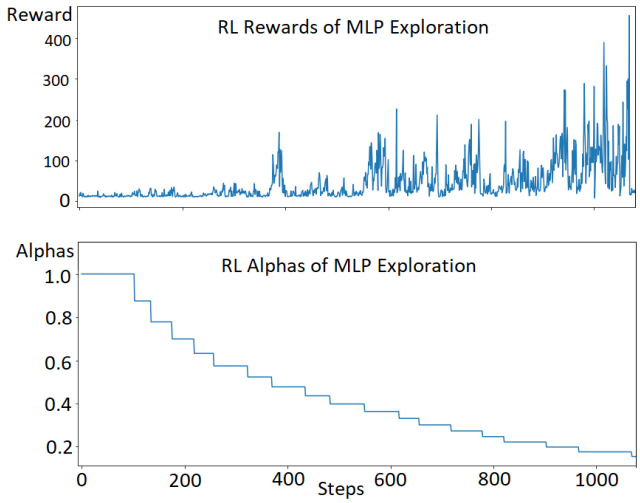

Figure 7. Reward and Alpha of Reinforcement Learning approach

We choose an ϵ-greedy policy, where a random action is chosen with the probability of α, otherwise the currently optimal action is chosen, which owns the highest value in the Q-Table. After every step, the Q-Table is updated with the learning rate β, following the temporal difference mechanism. α and β are decreasing over time in a logarithmic manner, after each episode. We verify the functionality of this method by using 1000 steps, including 70 episodes, to train the agent. Figure 7 shows the progress of the obtained reward over time as well as the logarithmic decrease of α. As can be seen, the reward increases and reaches a maximum the last episodes, which corresponds to a deviation of 0.22 % on the verification dataset. However, most interesting is the evolution of the Q-values. As we expected, for the first layers the agent is more likely to add neurons to the current layer till a size of 100 neurons. However, the agent does not want to drop the width of the sizes rapidly as we have expected. Instead the optimal policy of the agent extends the network in a much smoother way for the following layers. The best configuration on the verification dataset is: 90, 100, 70, 100, 100, 100, 60, 20, 50.

 ISBN: 978-1-61208-628-6

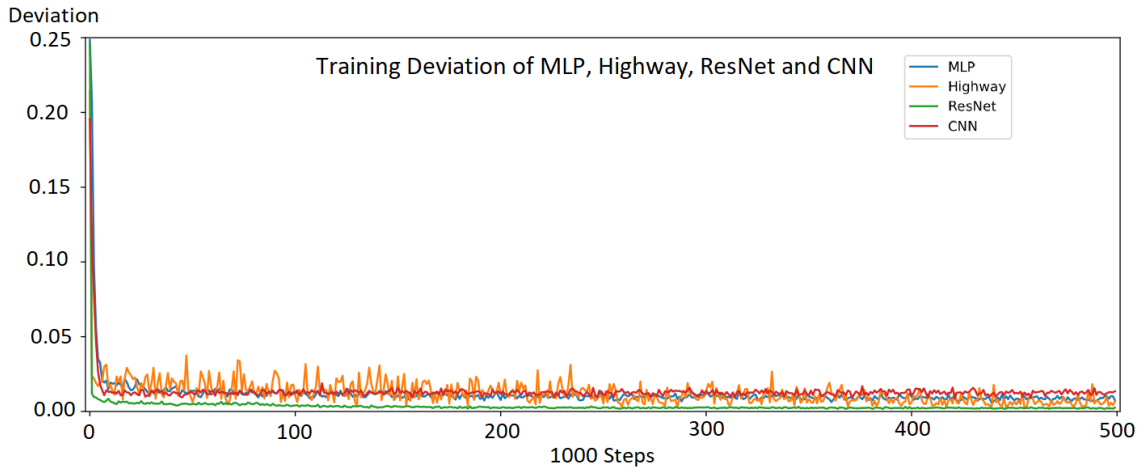

Figure 8. Validation error for best ANN of each class within training process.

V. Conclusion and Outlook

In this paper, we presented an empirical exploration of different types of feedforward ANNs, namely MLP networks, CNNs, ResNets, and highway networks. Our goal is to find a suitable type and shape of ANNs to predict the concentration of four mixture constituents. The results represent the starting point for further explorations for this multi-target-regression task. Therefore, we explored the shape of a traditional MLP network first and investigated the effect of applying convolution layers to extract spatial relationships on the generated dataset. We further extend the exploration by increasing the depth of both network types with the help of shortcuts, namely residual blocks and highway blocks. The best result was achieved with a ResNet configuration containing 120 layers, which also represents the biggest network created in this research. Due to the high complexity of the exploration task, we simultaneously develop a Q-learning strategy to automatically explore the shape of a MLP network in order to find a configuration owning a sufficient accuracy. In future work, we want to combine the results from both approaches. Thus, the most promising approach is the automatic exploration with RL using residual blocks. We also want to extend our approach with recurrent units, to take aging effects of the mass spectra into account.

Acknowledgment

This work was done under the support of BMWi project MiMEP (03ET1314A).

References

[1] W. Kuipers et al., “Realization of a miniaturized mass spectrometer based on a microfluidic device,” in Proceedings of the 1. International Conference on Microfluidic Handling Systems, 10 2012.

[2] M. Abadi et al., “TensorFlow: Large-scale machine learning on heterogeneous systems,” 2015, software available from tensorflow.org.

[3] Y. LeCun, P. Haffner, L. Bottou, and Y. Bengio, Object Recognition with Gradient-Based Learning. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 319–345.

[4] X. Glorot, A. Bordes, and Y. Bengio, “Deep sparse rectifier neural networks,” in Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics, ser. Proceedings of Machine Learning Research, vol. 15. Fort Lauderdale, FL, USA: PMLR, 11–13 Apr 2011, pp. 315–323.

[5] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” CoRR, vol. abs/1512.03385, 2015.

[6] R. K. Srivastava, K. Greff, and J. Schmidhuber, “Highway networks,” CoRR, vol. abs/1505.00387, 2015.

[7] D. Massicotte, S. Legendre, and A. Barwicz, “Neural-network-based method of calibration and measurand reconstruction for a high-pressure measuring system,” IEEE Transactions on Instrumentation and Measurement, vol. 47, no. 2, Apr 1998, pp. 362–370.

[8] B. Wu et al., “Comparison of statistical methods for classification of ovarian cancer using mass spectrometry data,” Bioinformatics, vol. 19, 2003, pp. 1636–1643.

[9] M. Ceccarelli, A. d’Acierno, and A. Facchiano, “A machine learning approach to mass spectra classification with unsupervised feature selection,” in Computational Intelligence Methods for Bioinformatics and Biostatistics, F. Masulli, R. Tagliaferri, and G. M. Verkhivker, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 242–252.

[10] B. Baker, O. Gupta, N. Naik, and R. Raskar, “Designing neural network architectures using reinforcement learning,” CoRR, vol. abs/1611.02167, 2016.

[11] N. Pinto, D. Doukhan, J. J. DiCarlo, and D. D. Cox, “A high-throughput screening approach to discovering good forms of biologically inspired visual representation,” PLOS Computational Biology, vol. 5, no. 11, 11 2009, pp. 1–12.

[12] M. Suganuma, S. Shirakawa, and T. Nagao, “A genetic programming approach to designing convolutional neural network architectures,” in Proceedings of the Genetic and Evolutionary Computation Conference, ser. GECCO ’17. New York, NY, USA: ACM, 2017, pp. 497–504.

[13] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” CoRR, vol. abs/1412.6980, 2014.

[14] X. Glorot and Y. Bengio, “Understanding the difficulty of training deep feedforward neural networks,” in JMLR W&CP: Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics (AISTATS 2010), vol. 9, May 2010, pp. 249–256.

[15] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” in Advances in Neural Information Processing Systems 25, F. Pereira, C. J. C. Burges, L. Bottou, and K. Q. Weinberger, Eds. Curran Associates, Inc., 2012, pp. 1097–1105.

[16] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” CoRR, vol. abs/1512.03385, 2015.

[17] ——, “Identity mappings in deep residual networks,” CoRR, vol. abs/1603.05027, 2016.

[18] R. K. Srivastava, K. Greff, and J. Schmidhuber, “Highway networks,” CoRR, vol. abs/1505.00387, 2015.

[19] R. S. Sutton and A. G. Barto, Introduction to Reinforcement Learning, 1st ed. Cambridge, MA, USA: MIT Press, 1998.

 ISBN: 978-1-61208-628-6

From Resilience to the Design of Antifragility

Danielle Sandler dos Passos
University Institute of Lisbon, ISCTE/IUL
Faculty of Science of the University of Lisbon, FCUL
The Robotics & Industrial Complex Systems, RICS
Lisbon, Portugal
e-mail: danielle.passos@uninova.pt

Helder Coelho
Department of Informatics of the Faculty of Sciences of
the University of Lisbon, FCUL
Lisbon, Portugal
e-mail: hcoelho@di.fc.ul.pt

Flávia Mori Sarti
School of Public Health of
the University of São Paulo, USP
São Paulo, Brazil
e-mail: flamori@usp.br

***Abstract*— Resilience has been highlighted for the last few years as one of the most important mechanisms of survival and evolution of systems. However, with the complexity and exponential advance of Information and Communication Technologies (ICT), volatility, uncertainty and disorder have become constant in our daily lives, creating the need for adjustments and improvements in resilience, in order to maintain its efficiency. As a consequence, various skills, such as adaptation, learning, self-organization and others, have been added to it, increasing it to antifragility. Focusing on this process of evolution, this work confronts the dissociation between resilience and antifragility, proving in the end, that antifragility is the resilience in its most advanced form.**

Keywords - Resilience; Antifragility; Complexity; Information and Communication Technologies; Stigmergy.

I. INTRODUCTION

Today, with days full of change and uncertainty, shocks and unexpected events have become more frequent, making it difficult to maintain a constant equilibrium and stimulating the emersion of a new mechanism of resilience [1][2], no longer centered on the search for balance nor on the return to its original form, but rather on the development of competences which promote improvements to the systems, allowing them to evolve through stress and disorder.

In this scenario, with increasing complexity and widespread diffusion of Information and Communication Technologies (ICT), learning and self-organization skills present in complex systems become essential to survive, providing to the systems a greater adaptability and efficiency, which allow them not only to resist, but also to evolve in the face of chaos [3].

This "new" mechanism of survival and evolution, called resilience by many, is called antifragility by Taleb [4], describing it as something beyond resilience because it improves with shocks and it is not only resistant to them. However, such dissociation between resilience and antifragility does not seem coherent to us. Our objective in this work is to demonstrate that antifragility and resilience should not be dissociated since antifragility corresponds to an advanced and improved form of resilience.

The rest of the paper is structured as follows. In Section II, we present a bibliographical review addressing (1) resilience, through its epistemological origin and the definitions of Holling [5][6] and (2) complexity and ICT, and how they are intertwined with resilience. In Section III, we show the antifragility and the evolution of resilience and we compare their definitions in order to prove their similarities. Finally, in Section IV, we present our concluding remarks.

II. RESILIENCE

A. ITS EPISTEMOLOGICAL ORIGIN AND THE HOLLING' DEFINITIONS

Coming from the Latin term "*resiliens*", whose meaning is "to turn back", resilience, in general, refers to the ability of an object (agent or system) to return to or recover its original shape or position after having been stressed [7].

Initially addressed in studies with children, in which it was linked to the degree of adaptation of beings in different situations [8], resilience was defined as: "*the persistence of systems and their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables*" (Holling [5]). However, after other studies, it was evident that resilience is not only related to internal factors (or characteristics of being), but also to external factors [9] - [13].

Still in this light, Rutter [14] states that resilience does not come from the personality of each subject, but from a dynamic process that varies according to each context and which presents itself in different ways, once each person assimilates each problem in a unique way [15].

Moreover, just as we are influenced by the environment and other agents, we also influence them, establishing an

 ISBN: 978-1-61208-628-6

interdependence between systems, agents and environment, from which unpredictable scenarios do emerge, permeated with uncertainties, volatility and instability, in which only dynamic mechanisms will be useful in the search for survival [16]-[20]. This idea is similar to Jen's idea [21], where new non-qualitative features emerge in a structural stability through of certain dynamic characteristics of the system, and the idea of De Florio [22], where resilience is not a property that systems have or do not have, but rather the emerging result of a dynamic process.

In this context, we came to see resilience in a more holistic and systemic way, shown by Holling [6], with the improvement of its previous definition, through the categorization of resilience in:

1) *Engineering Resilience*: initially described as the ability not to suffer from disorder, remaining in constant equilibrium [23], the resilience involved here acquires a more dynamic character, which allows the system to change or move in the face of stress, but, at the end of the process, there is always a return to the initial state or position. To this, in its more static version - where the balance is preserved and always maintained in the same form - the definition of robustness was linked, where robust is the one that remains intact, resistant to shocks and disorder [4];

2) *Ecological Resilience*: linked to the idea of dynamic balance, in which systems change and evolve when they are disturbed [4][6], changing state and/or position after stress, in this strand, adaptation and self-organization mechanisms are responsible for allowing systems to learn and improve with respect to past situations, in order to better take advantage in future ones [24][25].

In line with this broader form, and in view of the interconnections between environment, systems and their emerging properties, a more comprehensive and anti-reductionist approach encompassing complex elements present in our daily lives becomes necessary [4].

B. Its Relationship With The Complexity & ICT

Broader than the traditional thinking, complex thinking chooses to adopt the duality, recursion and systemicity, with the aim of highlighting and covering all relationships and influences among environment, systems and agents, as well as their results and forms of dissemination [26][27].

Together with complex thinking comes the General Systems Theory (GST), which argues that every system around us is complex, open, dynamic and adaptive. Thus, through the interaction between its parts and with the environment, new properties emerge and allow the survival, adaptation and evolution of the system, through mechanisms of evolutionary selection [16] [28].

In general, Complex Adaptive Systems (CAS) are formed by a set of diverse agents that get directly interconnected and act guided by common goals and by the spirit of cooperation, which allows them to develop collective competencies and evolve as a whole [29]-[32].

Still under the logic of complexity, equilibrium and stability are rejected because they do not provide the system with any learning or stimulus for its improvement. In contrast, the state "on the edge of chaos" and a no-interference policy with bottom-up structure are exalted as enhancers of the growth capacity and evolution of the systems [33]-[37].

In this context, stigmergy begins to gain prominence. Described by Grassé [38] as a coordination mechanism used by insects - where an insect leaves traces in the environment that influence the later work of the same or others, without any form of planning, control or direct interaction between the agents [39]. Nowadays, we can see stigmergy in most of the complex systems that surround us [40]. Encompassing mechanisms of self-organization and learning, in addition to elements of cognition and cooperation, stigmergy provides to the systems the ability to adapt and evolve [41] [42].

In addition, it is important to note that every complex system consists of networks of interactions between its parts, and it is important to consider its modulation and technologies, as these aspects directly interfere in the capacity of resilience and system evolution [43].

Structured systems under dense networks - with high degree of interconnection - at the same can be very efficient - with large and rapid exchange of information [44] - or very problematic, since the high proliferation power of this type of structure can quickly lead the system to collapse [45]. On the other hand, systems based on more specialized networks, with low redundancy (number of agents performing the same function) - tend to be less resilient, suffering more with the removal or inactivity of one of its agents, especially if they are the most interconnected (hubs) [46][47].

In this context, ICT also gain prominence, since they allow systems and agents to interconnect in different ways, which stimulate the emergence of new contexts, paradigms and cultures [48]-[50].

Such as a complex adaptive system, ICT, when integrated into the routine of agents, become powerful mechanisms of relationship and of dissemination of knowledge. They aid agents and systems in their processes of innovation and learning [51], either through smoother routines or through routines that drive systems "on the edge of chaos" [52].

III. The Antifragility and The Evolution of Resilience

As an intrinsic property of complex systems, resilience makes the system able to assimilate and adapt to its surroundings, allowing it to evolve in the face of disorder rather than stagnate or succumb [53]-[56].

As Hayek's neoliberal discourse dictates, no agent should interfere with the natural trajectory of the system and/or prevent its mechanism of self-organization from acting, as this may weaken the system or even lead to its extinction [4]. In addition, we should not try to predict the future based on past data – because in the face of constant changes the future would appear unpredictable – but rather accept its uncertainty and constantly seek to improve our adaptability to cope well with what will come [57].

This results in a "General Resilience" that gives systems the ability to deal with uncertainties, changes and surprises through mechanisms of adaptation, learning and self-

organization, enabling systems to improve when faced with shocks and disturbances [58].

In consonance, we see the Adaptive Cycle of Resilience (ACoR), which emphasizes that every system, at some point, will go through ruptures because even in equilibrium it accumulates fragilities and vulnerabilities [52].

Therefore, it is essential that systems improve their resilience mechanisms, but not only that. The antifragility emerges here, since the systems should not only seek to resist, but rather seek to improve when exposed to volatility and disorder [4] [52].

As Dahlberg [3] does for resilience, Taleb [4] also portrays the malfunctions of intervention for antifragility, arguing that both the optimization and the specialization, from human intervention, make systems more vulnerable. In addition to that, antifragility also acts as a powerful mechanism of risk mitigation [59] when using creation processes and recombination of elements to face the unpredictable [60].

Aven [61] also highlights that, in practical terms, when explaining a situation, we can easily replace the concept of fragility with that of resilience – fragile is the one not being resilient - which again demonstrates the incoherence in the distinction between antifragility and resilience.

In the field of industry, De Florio [62] shows the antifragility as an advanced mechanism of resilience, which is distinguished by its elasticity and machine learning ability. An idea also defended by Hole [63], which explains fragility, robustness and antifragility as stages of a spectrum, in which antifragility figures as an advanced degree of resilience.

Finally, in Table I, we interconnect concepts and definitions of resilience, robustness and antifragility, in order to demonstrate their similarities and resemblances, proving that antifragility is a type of resilience, in the broadest and most advanced form, in a quantitative way.

TABLE I - COMPARING DEFINITIONS OF RESILIENCE, ROBUSTNESS AND ANTIFRAGILITY

Resilience	Robustness	Antifragility
Characterized by low vulnerability to perturbations. Is the "*ability of these systems to absorb changes of state variables, driving variables, and parameters, and persist*" [5]	Robustness is a property of simple or complicated system characterized by predictable bahavior, enabling the system to bounce back to its normal state following a perturbation [3]	
Positive end of the distribution of developmental out comes among individuals at high risk [64]		It not only survive disturbance and disorder but actually develop under pressure [4]
Dynamic process encompassing positive adaptation within the context of significant adversity [65]		"*gets better with every shock*" [52]
An emergence property related to the self-organized behavior of SAC [30]		It not only resists the ravages of time but become ables to cope with an unpredictable future, through the creation and recombination of novel components [60]
"*Resilience requires a constant sense of unease that prevents complacency.*" [53]		*"The robust or resilient is neither harmed nor helped by volatility and disorder, while the antifragile benefits from them."* [4]
It is the capacity to provide sufficient response to uncertainty together with a process of learning from doing and building a knowledge repository from tough experiences [66]		*"systems able to learn while enacting elastic and resilient strategies"* [62]
Resilience enables the system to cushion the effects of unforessen disturbances by absorbing the shock and adapting to changing conditions forward to a more advanced level better suited for future hazards [56]		*"being antifragile means being able to grow despite the crises that might arise"* [52]
Mashup of adaptative and absorptive capacity, fostered by innovation and learning capabilities [31,30]		Stronger through learn fostered by resilient strategies [62]
"*the joint ability of a system to resist (prevent and withstand) any possible hazards, absorb the initial damage, and recover to normal operation*" [67]		*"is a new way of thinking about mitigation risk"* [59]
Capability of organizations related to ordinary adoptive practices that lead the system to higher levels of efficiency [68]		"*is rewarded with good results and protected from adverse events*" [61]

IV. CONCLUDING REMARKS

At the end of this study, it is shown the equivocation when dissociating resilience from antifragility. This is because, after exposing some of the current definitions of resilience and confronting with the definitions of antifragility, we can affirm that antifragility is synonymous of resilience in its most advanced form *($Resilience_{new}$),* where systems, in addition to resisting stress and volatility, also grow with them, thanks to their adaptive capabilities.

As proof of this, we can return to the idea of De Florio [62] (1):

$$\textbf{\textit{Antifragility = Elasticity + Resilience + Machine Learning}} \quad (1)$$

where elasticity is directly associated with the idea of adaptability and machine learning with the capacity for self-organization and learning of systems. The main elements of stigmergy are as described in (2).

$$\textbf{\textit{Stigmergy = self-organization + learning + adaptability}} \quad (2)$$

Aligned with this idea, we also see the description of resilience given by Folke [24]: *"is not only about being persistent or robust to disturbance. It is also about the opportunities that disturbance opens up in terms of recombination of evolved structures and processes, renewal of the system and emergence of new trajectories ".*

Thus, in front of the necessities, the resilience has been improving until the "new" resilience, resulting from the mix of stigmergy and resilience (Figure 1) - in its simple form.

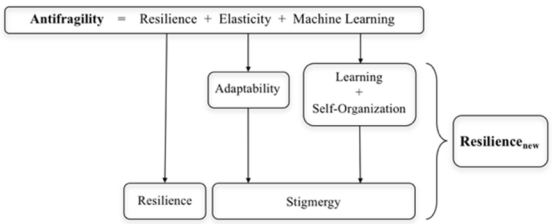

Figure 1. The Evolution of Resilience

From this, we can describe antifragility as (3):

$$\textbf{\textit{Antifragility = Resilience}}_{new} \quad (3)$$

In addition, Taleb [4], in portraying resilience through the figure of Phoênix – bird, which never gets extinguished, always being reborn from the ashes after its death - demonstrates its most archaic definition, which is today the synonymous of robustness, in which there is only resistance to shock, without any improvement nor learning. With such a

description, the author is denying the evolution of resilience and refuting all its improvements, due to the increase in complexity and the widespread dissemination of ICT.

Thus, at the end of this work and after a vast review of the studies cited here, it is noticed that the increase in complexity and the introduction of ICT in our daily life triggered the process of evolution of resilience, which in its most advanced stage appears as antifragility.

REFERENCES

[1] J. L. Casti, X-Events: The Collapse of Everything. New York: HarperCollins, 2012.

[2] G. J. Lewis and N. Stewart, "The measurement of environmental performance: an application of Ashby's law," Systems Research and Behavioral Science, vol. 20, pp. 31-52, 2003.

[3] R. Dahlberg, "Resilience and Complexity: Conjoining the Discourses of Two Contested Concepts," Culture Unbound, vol. 7, pp. 541-557, 2015.

[4] N. N. Taleb, Antifragile: Things that gain from disorder. Random House, 2012.

[5] C. S. Holling, "Resilience and Stability of Ecological System," Annual Review of Ecology and Systematics, vol. 4, pp. 1-23, 1973.

[6] C. S. Holling, "Engineering resilience versus ecological resilience," Engineering within ecological constraints, vol. 31, 1996.

[7] M. Panteli and P. Mancarella, "The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience," IEEE Power and Energy Magazine, vol. 13, pp. 58-66, 2015.

[8] E. E. Werner, J. M. Bierman, and F. E. French, The children of Kauai: A longitudinal study from the prenatal period to age ten. University of Hawaii Press, 1971.

[9] A. S. Masten, and N. Garmezy. "Risk, vulnerability, and protective factors in developmental psychopathology," Advances in clinical child psychology, pp. 1-52, 1985.

[10] E. E. Werner and R. S. Smith, Overcoming the odds: High risk children from birth to adulthood. Ithaca, NY: Cornell University Press, 1992.

[11] D. Cicchetti and M. Lynch, "Toward an ecological/transactional model of community violence and child maltreatment: Consequences for children's development," Psychiatry, vol. 56, pp. 96-118, 1993.

[12] D. M. Fergusson and M. T. Lynskey, "Adolescent resiliency to family adversity," Journal of child psychology and psychiatry, vol. 37, pp. 281-292, 1996.

[13] E. L. Cowen, P. A. Wyman, W. C. Work, J. Y. Kim, D. B. Fagen, and K. B. Magnus, "Follow-up study of young stress-affected and stress-resilient urban children," Development and Psychopathology, vol. 9, pp. 565-577, 1997.

[14] M. Rutter, "Resilience in the face of adversity. Protective factors and resistance to psychiatric disorder," The British Journal of Psychiatry, vol. 147, pp. 598-611, 1985.

[15] R. P. Pesce, S. G. Assis, N. Santos, and R. D. Oliveira, "Risk and Protection: Looking for an Equilibrium That Provides Resilience," Psicology: theory and research, vol. 20, pp. 135-143, 2004.

[16] J. D. Thompson, Organizations in action: Social science bases of administrative theory. Transaction Publishers, 1967.

[17] N. Garmezy, "Children in poverty: Resilience despite risk," Psychiatry, vol. 56, pp. 127-136, 1993.

[18] E. Morin, Introduction to complex thought. Porto Alegre: Sulina, 2006.

[19] A. O. Sordi, G. G. Manfro, and S. Hauck. "The concept of resilience: different views," Brazilian Journal of Psychotherapy, vol. 2, pp. 115-132, 2011.

[20] O. Noran, "Collaborative Disaster Management: An Interdisciplinary approach," Journal of Computer in Industry, vol. 65, pp. 1032-1040, 2014.

[21] E. Jen, "Stable or robust? What's the difference?," Complexity, vol. 8, pp. 12-18, 2003.

[22] V. De Florio, "On resilient behaviors in computational systems and environments," Journal of Reliable Intelligent Environments, vol. 1, pp. 33-46, 2015.

[23] B. Walker, C. S. Holling, S. R. Carpenter, and A. Kinzig, "Resilience, adaptability and transformability in social-ecological systems," Ecology and society, vol. 9, pp. 5, 2004.

[24] C. Folke, "Resilience: The emergence of a perspective for social–ecological systems analyses," Global environmental change, vol. 16, pp. 253-267, 2006.

[25] E. Hollnagel, "Prologue: the scope of resilience engineering," Resilience engineering in practice: A guidebook, 2011.

[26] D. J. Watts, Six Degrees: The Science of a Connected Age. Norton, 2003.

[27] E. Morin, and J. Le Moigne, The Intelligence of Complexity. 2000.

[28] L. Von Bertalanffy, General system theory. 1968.

[29] B. Zimmerman, "Complexity science: a route through hard times and uncertainty," Health Forum Journal, vol. 42, pp. 42-46, 1999.

[30] L. H. Gunderson, Panarchy: understanding transformations in human and natural systems. Island press, 2001.

[31] G. S. Cumming *et al.*, "An Exploratory Framework for the Empirical Measurement of Resilience," Ecosystems, vol. 8, pp. 975–987, 2005.

[32] S. L. Cutter, *et al.*, "A place-based model for understanding community resilience to natural disasters," Global Environmental Change, vol. 18, pp. 598–606, 2008.

[33] I. Gleiser, Chaos and Complexity: The Evolution of the Economic Thought. Rio de Janeiro: Editora Campus, 1992.

[34] I. Prigogine, and I. Stengers, The end of certainty. Simon and Schuster, 1997.

[35] R. T. Pascale, "Surfing the edge of chaos," MIT Sloan Management Review, vol. 40, pp. 83, 1999.

[36] M. Wheatley, Leadership and the new science: discovering order in a chaotic world. San Francisco: Berrett-Koehler Publishers, 2011.

[37] F. A. Hayek, Law, legislation and liberty: a new statement of the liberal principles of justice and political economy. Routledge, 2012.

[38] P. P. Grassé, "La reconstruction du nid et les coordinations interindividuelles chez Bellicositermes natalensis et Cubitermes sp. la théorie de la stigmergie: Essai d'interprétation du comportement des termites constructeurs," Insectes sociaux, vol. 6, pp. 41-80, 1959.

[39] H. V. D. Parunak, "A survey of environments and mechanisms for human-human stigmergy," International workshop on environments for multi-agent system, pp. 163-186, 2005.

[40] F. Heylighen, "Stigmergy as a Universal Coordination Mechanism: components, varieties and applications," Human Stigmergy: Theoretical Developments and New Applications, 2015.

[41] I. J. Aberkane, "From waste to kwaste: on the Blue Economy in terms of knowledge flow," First Complex Systems Digital Campus World E-Conference 2015, pp. 283-290, 2017.

[42] T. G. Lewis and L. Marsh, 2016. Human stigmergy: Theoretical developments and new applications.

 ISBN: 978-1-61208-628-6

[43] G. M. Souza and M. S. Buckeridge, “Complex Systems: New ways of seeing the Botany,” Brazilian Journal of Botany, vol. 27, pp. 407-419, 2004.

[44] J. Fiksel, “Sustainability and resilience: toward a systems approach,” Sustainability: Science, Practice, & Policy, vol. 2, 2006.

[45] P. Crucitti, V. Latora, and M. Marchiori, “Model for cascading failures in complex networks,” Physical Review E, vol. 69, 2004.

[46] M. E. Newman, “The structure and function of complex networks,” SIAM review, vol. 45, pp. 167-256, 2003.

[47] N. Leveson *et al.*, “Engineering resilience into safety-critical systems,” Resilience Engineering–Concepts and Precepts, pp. 95-123, 2006.

[48] R. V. Kozinets, “The field behind the screen: Using netnography for marketing research in online communities,” Journal of marketing research, vol. 39, pp. 61-72, 2002.

[49] M. Castells, The Galaxy Internet: reflections on the Internet, business and society. Zahar, 2003.

[50] F. Heylighen, “ 13 Accelerating socio-technological evolution,” Globalization as evolutionary process: modeling global change, pp. 284, 2007.

[51] B. M. Leiner *et al.,* A Brief History of the Internet. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet, 2017/02/03.

[52] A. Karadimas, E. Hewig, S. Behera, and T. Kotisi, A Case Study of Black Swans and Antifragility. 2014.

[53] E. Hollnagel, Resilience: the challenge of the unstable. 2006.

[54] J. H. Holland, “Studying complex adaptive systems,” Journal of Systems Science and Complexity, vol. 19, pp. 1-8, 2006.

[55] D. D. Woods, “Essential characteristics of resilience,” Resilience engineering: Concepts and precepts, pp. 21-34, 2006.

[56] G. C. Gallopín, “Linkages between vulnerability, resilience, and adaptive capacity,” Global environmental change, vol. 16, pp. 293-303, 2006.

[57] B. Evans and J. Reid, Resilient Life: The Art of Living Dangerously. Cambridge: Polity Press, 2014.

[58] S. Carpenter, B. Walker, J. Anderies, and N. Abel, “From metaphor to measurement: resilience of what to what?,” Ecosystems, vol. 4, pp. 765-781, 2001.

[59] T. Bendell, Building Anti-fragile Organisations: Risk, Opportunity and Governance in a Turbulent World. New York: Routledge, 2016.

[60] A. Danchin, P. M. Binder, and S. Noria, “Antifragility and tinkering in biology (and in business) flexibility provides an efficient epigenetic way to manage risk,” Genes, vol. 2, pp. 998-1016, 2011.

[61] T. Aven, “The concept of antifragility and its implications for the practice of risk analysis,” Risk analysis, vol. 35, pp. 476-483, 2015.

[62] V. De Florio, “Antifragility= elasticity+ resilience+ machine learning models and algorithms for open system fidelity,” Procedia Computer Science, vol. 32, pp. 834-841, 2014.

[63] K. J. Hole, Anti-fragile ICT Systems. Springer-Verlag GmbH, 2016.

[64] M. Rutter, “Psychosocial resilience and protective mechanisms,” American journal of orthopsychiatry, vol. 57, pp. 316, 1987.

[65] S.S. Luthar, D. Cicchetti, D., and B. Becker, “The construct of resilience: A critical evaluation and guidelines for future work,” Child development, vol. 71, pp. 543-562, 2000.

[66] C. A. Lengnick-Hall and T. E. Beck, “Adaptive fit versus robust transformation: How organizations respond to environmental change,” Journal of Management, vol. 31. pp. 738-757, 2005.

[67] M. Ouyang, “Review on modeling and simulation of interdependent critical infrastructure systems,” Reliability Engineering & System Safety, vol. 121, pp. 43–60, 2014.

[68] A. E. Akgün and H. Keskin, “Organisational resilience capacity and firm product innovativeness and performance,” International Journal of Production Research, vol. 52, pp. 6918 - 6937, 2014.

 ISBN: 978-1-61208-628-6

Safety, Cybersecurity and Interoperability of Modern Nuclear Power Plants

Asmaa Tellabi[1, 4], Ines Ben Zid[2, 4], Edita Bajramovic[3, 4], Karl Waedt[4]
[1]University of Siegen, Siegen, Germany
[2]University of Bielefeld, Bielefeld, Germany
[3]Friedrich-Alexander-University Erlangen-Nuremberg, Erlangen, Germany
[4]Framatome GmbH, Erlangen, Germany

E-mail:{firstname.lastname}@framatome.com

***Abstract*—The integration of digital equipment and diverse automation platforms in modern nuclear plants, including Nuclear Power Plants is due to the gradually increasing use of digital technologies. This digitalization either comes gradually based on a succession of refurbishment projects of Instrumentation & Control and Electrical Power Systems or as comprehensive architectures with new-built power plants. Therefore, similar to any critical infrastructure facing a growing risk of cyber-attacks, cybersecurity for Nuclear Power Plants has become a subject of rising concern. We envision that the findings in this paper provide a relevant understanding of the threat landscape facing digital systems in nuclear power plants. The knowledge can be used for an improved understanding and a better identification of security risks during the analysis and design of supporting systems. This paper gives an overview of the security issues and vulnerabilities, helping to better understand the big picture of cybersecurity issues and vulnerabilities in Nuclear Power Plants. Identifying these vulnerabilities and issues helps to establish new security countermeasures. A new draft standard IEC 63096 is presented in this paper as well.**

Keywords-nuclear power plants; cybersecurity interoperability.

I. INTRODUCTION

Digital Instrumentation and Control (I&C) systems are defined as computer-based devices that monitor and control nuclear power plants (NPP). Electrical Power Systems (EPS) provide the redundant power supply for different plant operation scenarios, which have to be fully supported. The EPS may include the connection to external highest voltage (e.g. 400 kW) or high voltage (e.g. 110 kV) grid connections, Emergency Diesel Generators, Station Blackout Diesel Generators, different Uninterruptable Power Supplies (UPS), e.g. for 2 hours and 12 hours.

Furthermore, different inverters and rectifiers are responsible of controlling and monitoring the entire aspects of the plant's health, all plant states and helping to respond with the care and adjustments as needed. They are seen as the nervous system of a nuclear power plants (NPP). Generation III+ and IV reactors are equipped with digital I&C systems, while analog systems in older reactors are being replaced with digital systems [1]. The high level communication between NPPs control networks is done by Supervisory Control and Data Acquisition systems (SCADA) in order to coordinate power production with transmission and distribution demands. Integration of digital I&C systems and the connectivity between NPPs control networks and external networks represent a threat for NPPs, making them a target to cyber-attacks which can include physical damage to reactors. With possibilities of cyber-attacks targeting NPPs increasingly, cybersecurity has aroused as a significant problem [2].

The remainder of this paper is organized as follows. Section II gives background information on typical system architecture in NPPs. Section III outlines some of the notorious publically known cyber-attacks against NPPs. In section IV, a new IEC 63096 standard [3] is described. We conclude the paper in Section V.

II. NUCLEAR POWER PLANTS

The general digital systems configuration of NPPs is almost similar to that of Industrial Control Systems (ICS) SCADA systems. The general architecture can be separated into two distinct domains: I&C systems, EPS and plant-local or corporate IT systems. The restriction on these networks is not similar, but also the nature of the traffic.

According to Fig. 1, operations, such as office automation, document management, and email, which consist of conventional IT systems, such as PCs and enterprise workstations use the corporate network of the Utility. As an illustration, Internet access, FTP, email, and remote access will normally be allowed on the enterprise network level but should not be permitted on the ICS network level.

Nuclear safety is the accomplishment of correct operating conditions, prevention of accidents or alleviation of accident consequences, ending up with the protection of workers, the public and the environment from extreme radiation hazards. On the other hand, nuclear security is the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.

Safety is expected to prevent accidents, while security is implemented to stop intended acts that might harm the NPP or lead to the theft of nuclear materials. Safety evaluations focus on risks arising from accidental events occurrences

 ISBN: 978-1-61208-628-6

originated from nature (such as earthquakes, tornadoes, or flooding), hardware failures, supplementary internal events or interruptions (such as fire, pipe breakage, or loss of electric power supply), or human mistakes (such as the incorrect application of procedures, or incorrect alignment of circuits). For security, the risks, or events, worried about result from malicious acts accomplished with the objective to steal material or to cause damage. Therefore, security events are based on 'intelligent' or 'deliberate' actions achieved intentionally for theft or sabotage and with the purpose to avoid protective measures [2].

Safety and security have various elements in common and both focus on protecting the plant with the eventual purpose of protecting people, society, and the environment. As stated above, the essential objective of each is identical — the protection of people, society and the environment. Whether it was a safety or a security event causing harm, the acceptable risk is likely the same, usually they both adopt the strategy of defense in depth, which is defined as the usage of layers of protection.

First concern is given to prevention. Second, abnormal situations need to be identified early and take action promptly to avoid resulting damage. Mitigation comes in the third place of an operative strategy. Finally, considerable emergency planning should be implemented in case of the failure of prevention, protection and mitigation systems [2].

I&C are censorious in NPPs. They are responsible of monitoring the operational state of the nuclear reactors through interaction with physical equipment, but also in charge of process control. With the introduction of digital technologies in the 2000s, I&C systems shifted from analog technologies to digital technologies. The usage of digital technologies has been steadily increasing [4]. NPPs I&C systems engage in environments dissimilar from those of typical IT systems.

In a typical NPP, I&C architecture contains two types of systems: Non-safety and Safety systems. The Non-safety system is defined as a distributed computer system containing a number of remote control nodes spread across the NPPs, which uses redundant real time data network to communicate with each other and with the Human Machine Interface (HMI).

Communication with third party systems and Operation Maintenance Corporate Systems (OMS) are also supported through open protocols like Object Embedding Linking Process Control, fieldbuses and Modbus-TCP [5].

Additionally, monitoring and manual control of the NPPs processes is done by the use of HMI consoles connected in the non-safety system. In order to display critical information related to safety on the non-safety HMI, the safety system will communicate with the non-safety system through Interface gateways.

On the contrary, a safety system is regularly based on a channelized Programmable Logic Controllers (PLC) that holds a number of PLC nodes distributed across the NPPs. These PLCs and its cabinets are designed to resist seismic events, environmental events and cybersecurity attacks. Furthermore, they can still be able to operate safely.

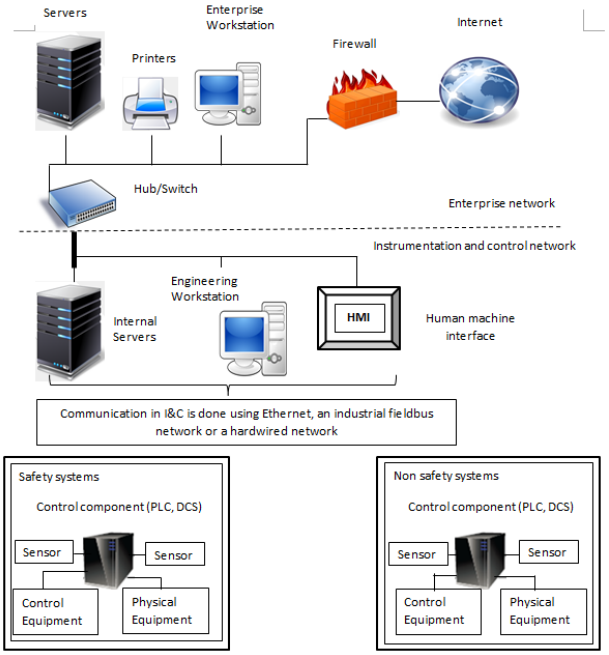

Figure 1. General architecture in nuclear power plants [6].

The purpose of this distribution is to coordinate with safety components in the process system, and also to ensure a safe communication in a safety channel using the redundant real time data safety network or through dedicated high speed links in between safety channels. Distributed control systems (DCSs) or PLCs are common control components in I&C systems, they interact with physical equipment directly and industrial PCs or engineering workstations that are employed to configure control components and their related works.

III. CYBERSECURITY AND CYBER WARFARE RELATED TO NUCLEAR POWER PLANTS

Advancement in electronics and IT was the main motivation behind the replacement of traditional analog I&C systems in NPPs with I&C systems, e.g. systems based on computers and microprocessors. Also, digital systems allow superior reliability, improved plant performance and supplementary diagnostic aptitudes. The systems used today were designed to satisfy performance, reliability, safety, and flexibility requirements, most of them were created a long time ago before new technologies became a crucial part of business operations.

In most typical implementations, these systems are physically isolated from outside networks and are based on proprietary hardware and software. The communication protocols include basic error detection and correction capabilities but lack the secure systems [5]. Accordingly, it is crucial not to connect such systems to an Intranet or the Internet.

 ISBN: 978-1-61208-628-6

A. History of Selected Attacks in NPPs

First, in this section we present some of the notorious attacks against NPPs. In [7], attack taxonomy is defined by 5 dimensions: precondition, vulnerability, target, attack method, effect of the attack. It was combined with a new dimension target—the effect it has on the confidentiality, availability, integrity (CIA) of a system.

1) Ignalina NPP (1992)

At the Ignalina NPP in Lithuania, a technician intentionally introduced a virus into the industrial control system.

- **Precondition:** Direct access to the system.
- **Attack method:** Insider attack.
- **Target:** Availability and integrity.
- **Effect of the attack:** In this case, little harm was caused, but someone with malicious intent could have provoked a serious incident [8][9].

2) Davis-Besse NPP (2003)

This plant located in Ohio was infected by the Slammer worm (also called W32/SQLSlam-A or Sapphire).

- **Precondition:** Unpatched system.
- **Attack method:** At first, the worm scans and sends itself to random IP addresses; if worm reaches a machine that is running Microsoft SQL 2000, it infects that machine and begins scanning and sending itself to another machine.
- **Target:** Availability.
- **Effect of the attack:** The safety parameter display system (SPDS), responsible of collecting and displaying data regarding the reactor core from the coolant systems, temperature sensors and radiation detectors, was unavailable for nearly five hours [8][9].

3) Browns Ferry NPP (2006)

This NPP located in Alabama experienced a malfunction of both reactor recirculation pumps (which use variable-frequency drives to control motor speed and are needed to cool the reactor) and the condensate demineralizer controller (a type of PLC).

- **Precondition:** Device failure, attack method. Both of these devices contain microprocessors that communicate by sending and receiving data over an Ethernet network.
- **Attack method:** Ethernet operates by first sending data to every device on the network; then they have to inspect each packet to define if the packet is intended for them or if they can ignore it, making them vulnerable to failure if they accept enormous traffic.
- **Target:** Availability.
- **Effect of the attack:** The excess traffic produced by network broke down the reactor recirculation pumps and condensate demineralizer controller. As a consequence, the plant's Unit 3 had to be manually shut down in order to prevent a meltdown [8][9].

4) Hatch NPP (2008)

Hatch NPP located in Georgia experienced a shutdown as an unintended consequence of an update performed by contractor. An engineer contractor that manages the plant's technology operations installed an update to a computer on the plant's business network.

- **Precondition:** Human error.
- **Attack method:** The update was intended to synchronize data. The updated computer was connected to one of the plant's industrial control system networks, consequently when the engineer restarted the updated computer; the synchronization changed the control system's data to zero for a short moment.
- **Target:** Availability and integrity.
- **Effect of the attack:** The interpretation of the temporary changed values by the plant's safety system was incorrect. The updated value to zero of the water level signified that there was not enough water to cool the reactor core, which conducted to automatic shutdown for 48 hours of the plant's Unit 2 [8][9].

5) Natanz Nuclear Facility and Bushehr NPP – Stuxnet (2010)

First exposed to public in June 2010, the Stuxnet computer worm infected both the Natanz nuclear facility and the Bushehr NPP in Iran, partially destroying around 1,000 centrifuges at Natanz.

- **Precondition:** Use of commercial-off-the-shelf (COTS) Operating System (OS), Stuxnet infects computers using the Microsoft Windows operating system, exploiting vulnerabilities in the system that allows it to obtain system-level access.
- **Attack method:** The worm uses forged certificates as a result the installed files look to come from an authentic source, misleading antivirus. Iranian nuclear facilities work with Siemens Step 7 SCADA system. Once the machine is infected, Stuxnet inspects the network to find computers attached to a similar system. Stuxnet duplicate itself on other computers by exploiting another set of vulnerabilities found in print spoolers and also through USB flash drives, so it spreads to networks using shared printers. Stuxnet's payload is activated only if the computer is connected to a similar Siemens system. It reprograms the system's PLCs, in charge of controlling centrifuges applied in enriching nuclear fuel, so that they spin rapidly and eventually finish by break down.
- **Target:** Availability and integrity.
- **Effect of the attack:** As a result, Stuxnet destroyed over 1,000 centrifuges at Natanz [8][9].

6) Korea Hydro and Nuclear Power Co. Commercial Network (2014)

Hackers infiltrated and stole data from the commercial network of Korea Hydro and Nuclear Power Co., which operates 23 of South Korea's nuclear reactors.

 ISBN: 978-1-61208-628-6

- **Precondition:** Human error: Access to the confidential data was obtained by hackers through phishing emails to the owner-operator's employees. Some of them finished by clicked on the links and downloaded the malware.
- **Attack method:** Sending phishing emails to employees.
- **Target:** Confidentiality.
- **Effect of the attack:** The hackers acquired the blueprints and manuals of two reactors, electricity flow charts, personal data that belongs to approximately 10,000 of the company's employees, also radiation exposure estimates for nearby residents [8][9].

B. *Security Vulnerabilities*

In general, I&C in NPPs are physically isolated from external networks and have a different operational environment from that of conventional IT systems. As a result, NPPs were regarded as being safe from external cyber-attacks. However, continuous cyber-attacks against NPPs signified that NPPs are as susceptible to cyberattacks as other critical infrastructures [10] and conventional IT systems.

ICS, usually control the physical world and IT systems manage data. ICS are different from traditional IT systems, including dissimilar risks and priorities. Some of the different characteristics include important risk to the health and safety of human lives, severe destruction of the environment, and financial problems such as production deficit, and undesirable effect to a nation's economy. Performance and reliability requirements for ICS are distinct, by using operating systems and applications that may be seen unusual in a classic IT network environment. At first, ICS had slight similarities to IT systems in that ICS were inaccessible systems implementing proprietary control protocols with specific hardware and software. Commonly accessible, low-cost Ethernet and Internet Protocol (IP) devices are now substituting the older proprietary technologies, which raises the likelihood of cybersecurity vulnerabilities and events. Currently, ICS are embracing IT solutions to endorse corporate connectivity and remote access abilities, and are being created and employed via industry standard computers, operating systems (OS) and network protocols, where the resemblance to IT systems comes from. This novel integration deploys IT capabilities, but it meaningfully offers less separation for ICS from the outside world than antecedent systems, increasing the necessity to secure these systems. Despite the fact that security solutions have been designed to deal with these security matters in characteristic IT systems, particular precautions must be engaged when presenting these similar solutions to ICS environments. ICS and IT systems operate in continuously changing environments. The environments of operation comprise, but are not limited to the threat space, vulnerabilities, missions/business purposes, mission/business procedures, enterprise and information security architectures, information technologies, personnel, facilities, supply chain relationships, organizational governance/culture, procurement/acquisition processes, organizational policies/procedures, organizational assumptions, constraints, risk tolerance, and priorities/trade-offs) [4].

1) *Lack or Improper Input Validation*

Attackers exploit vulnerabilities in services and scripts written by I&C vendors, resulting from the non-secure coding practices, allowing attackers to send forged request in order to modify the program execution. In the same way, using vulnerable protocols with for networking will be exploited to create malformed packets. Vulnerabilities found in these protocols and services make an attacker able to manipulate plant component, via well-known attacks. Vulnerable modules that might be concerned include Workstations at Main Control Room (MCR), Remote Shutdown Station (RSS); Process Information and Control System (PICS); Safety Information and Control System (SICS); Human Machine Interface (HMI). The attacks that could take place by exploiting this vulnerability are buffer overflow, command injection, and SQL injection.

2) *Inappropriate Authorization*

Authorization guarantees access to resources only by authorized entities. Access control mechanisms are implemented to ensure appropriate authorization. Absence of or weak authorization mechanisms can be exploited by attackers to gain illegal access to resources and tamper I&C system components. Software installed at operator workstations side must perform access control checks, or it will open a new door for attackers to perform unauthorized actions. Vulnerable modules include Workstations at MCR, RSS, PICS, SICS, HMIs, Safety Automation System (SAS), Protection System (PS), Process Automation System (PAS). Existing module in I&C system must first verify whether the requesting module is allowed to access the resource. Escalation of privilege is one of the attacks that could be performed with authorization vulnerability.

3) *Improper Authentication*

The network protocols used within I&C system architecture during communication, frequently suffer from weak authentication mechanisms to verify the identity of the packet and also the user. Weak authentication vulnerabilities permit attackers to eavesdrop on network communications and capture the identity credentials of legal users, ending with an unauthorized privilege. Mutual authentication before sending or receiving data is not performed by the components of I&C. Not verifying the origin or authenticity of data, permits malicious data into components, credential theft, authentication bypass, etc. Furthermore, non-properly protected confidential data stored in databases can also be exploited. Vulnerable modules that might be touched by this are almost all I&C systems, sub-systems and components [9]. Often, I&C vendors leave behind authentication information from their product code or documentation, which can be definitely accessed and exploited by attackers. Weak passwords or using default passwords are another significant vulnerability to consider. There are numerous possible aspects that can be used to authenticate a person, device, or system, together with something the user knows, something the user has or something the user is. For instance,

 ISBN: 978-1-61208-628-6

authentication could be founded on something known (e.g., PIN number or password), something possessed (e.g., key, dongle, smart card), something the user is like a biological characteristic (e.g., fingerprint, retinal signature), a location (e.g., Global Positioning System (GPS), location access), the time a request is made, or a mixture of these attributes. Normally, the more authentication process includes more factors, the more strong the process will be. Multi-factor authentication refers to the process when two or more factors are used [4].

4) Unencrypted Sensitive Data

Frequently data at rest and in transit is unencrypted, making them vulnerable to disclosure. Moreover, network packets exchanged between several components of I&C are not encrypted but in plaintext form. Vulnerable modules that might be touched by this are almost all I&C systems, sub-systems and components [9]. Exposure of product source code, topology, legitimate user credentials, might result as a consequence.

5) Incorrect Software Configurations and Management

Security breaches and exploitations of plant operations are a result of misconfigurations or vulnerabilities found in I&C software. Modules that are seen vulnerable to this are Workstations at MCR, RSS, PICS, SICS, HMIs, SAS, PS, and PAS. The existence of these vulnerabilities is caused by poor patch management, poor maintenance, and built-in flaws in I&C products. Additionally, improper installations of applications also offer an opportunity to attackers to tamper the system.

6) Lack of Backup Facilities

Some of I&C systems in NPPs do not own backup and restore facilities dedicated to databases and software. NPPs that possess backup facilities often store them offsite, and they are not often exercised and tested. Vulnerable modules that might be concerned by lack of backup facilities are SAS, PS, PAS, Sensors, Actuators, PICS, and SICS [9]. NPPs must be operated 24/7 and the absence of a backup feature can result in catastrophic effects if an incident occurs.

7) Absence of Audit and Accountability

Some attacks are hard to detect since they are launched in a cautious manner like insider attacks. The nonexistence of auditing and logging mechanisms assists attackers into covering their tracks after attacks. Vulnerable modules that might be touched by this are almost all I&C systems, sub-systems and components. Storing activity logs of I&C components and operator actions is vital in order to trace attack patterns, but also to avoid repudiation threats from insiders as well as actions in I&C components and systems.

8) Absence of Security Awareness

Technology advancements and the people using these technologies present multiple risks to information security. The human factor is considered as one of the major sources of information security risk, also one of the most difficult to control. According to a Deloitte's Technology, Media, and Telecommunications (TMT) Global Security Study [11], 70% of the TMT organizations surveyed rate their employees' lack of security awareness as an "average" or "high" vulnerability, which was the case for Korea Hydro and nuclear Power Co. The security controls that conform to the NIST SP 800-53 Awareness and Training (AT) family offer policy and procedures for guaranteeing that each user of an information system is equipped with elementary information system security awareness and training materials before authorization to access the system is granted. Security awareness is a crucial part of ICS incident prevention, mainly when it comes to social engineering threats. Social engineering is seen as a method used to influence individuals into revealing private information, such as passwords. This information can then be exploited to endanger otherwise secure systems. Employing an ICS security program may bring changes to the means used by personnel to access computer programs, applications, and the computer desktop itself [8].

C. Industry and Government Responses to NPPs Cybersecurity

In the previous section, known attacks and vulnerabilities in NPPs were underlined. Since they pose important risks to the economy and to national security, numerous attempts were made by international organizations, regulatory and research institutes, and governments to set up cybersecurity guidelines, standards, and frameworks dedicated to security of NPPs.

For industry adoption and regulatory approval, three features of digital I&C systems are distinguishing.

First, a digital I&C system is more complicated than its analog predecessor because of the number of connections it has among its many components. Second, the digital system rely more on software. Usually, a unit has around 10000 sensors and detectors and 5000 km of I&C cables. The total mass components connected to I&C, is close to 1000 tones. Making I&C system one of the heaviest and most extensive non-building structures in any NPP. Third, the complete reliance on computers increases the importance of cybersecurity. The first two of these features, complexity and software-dependence, introduce new possibilities for common cause failures.

The increased use of commercial "off-the shelf" software is considered as one practice hurting the nuclear industry. This type of software does not deliver a suitable level of protection from external threats and is often seen as a direct approach to penetrate a facility network. The use of insufficient software, mixed with executive-level ignorance of security risks, builds an easy way for an attacker to misuse assets. There is a common misrepresentation which refers to nuclear facilities as being "air-gapped" – totally inaccessible from the Internet – signifying that the industry is safe from cyber-attacks. Considerable commercial software offers Internet connectivity through virtual private networks (VPNs) or else Intranet. These connections often go unlisted and keep on being ignored while implementing software or deploying momentary Internet connections for a project. Furthermore, the focus has been given more to physical safety and protection instead of cybersecurity controls. Therefore, very few developments have been made to reduce cyber risks through standardized control and measures [10].

 ISBN: 978-1-61208-628-6

NPPs are securely maintained and considered as the most protected and secure facilities in the world. However accidents can happen, undesirably affecting environment and people. Vulnerabilities threatening the physical security of a NPPs and their ability to launch acts of terrorism were elevated to a national security issue following the attacks of 9/11, 2001. Consequently, the American congress endorsed new nuclear plant security requirements and has frequently devoted attention on regulation and enforcement by the Nuclear Regulatory Commission (NRC). Years passed after the 9/11 attacks, but security at NPPs persists as a vital matter. To decrease the likelihood of an accident, the International Atomic Energy Agency (IAEA) supports Member States in applying international safety standards to reinforce safety in NPPs [9]. NIST has published a well-established risk management framework in NIST Special Publications (SP) 800-30 [12], 800-37 [13], and 800-39 [14], which analyzes distinct threat scenarios and evaluates the various attack possibilities that can exploit system vulnerabilities. On the other hand, the NIST risk assessment framework, mentioned above, does not describe precise procedures on the approach a company should assess the quantification of risks, i.e. how and to what degree an attack can endanger system confidentiality, integrity, or availability. In 2008, NIST issued a guideline on securing ICS [4]. It systematically explained the security of ICS systems, mostly containing SCADA architecture, distributed control systems (DCS), secure software development, and deployment of controls in order to secure networks. NIST also came up with a guideline on the Security for Industrial Automation and Control Systems while working with the Industrial Automation and Control Systems Security ISA99 Committee.

The IEEE produced the SCADA cryptography standard in 2008 [15], which offers a comprehensive explanation on the way to found secure communication between SCADA servers and workstations. Organizations can also attain certification under this IEEE standard if they fulfill with the requirement. The International Organization for Standardization (ISO) has also issued a standard, ISO/IEC 27002:2013 [16], which gives guidelines for initiating, implementing, maintaining, and improving information security management in organizations [9]. NRC's cybersecurity regulations necessitate each NPPs to present a cybersecurity plan and implementation schedule. The plan must deliver "high assurance" that the digital computer and communications systems implemented in order to perform the next functions will deliver sufficient protection against design basis attacks:

- Safety-related Functions or vital to safety.
- Security functions.
- Emergency mobility functions, as well as offsite communications.
- Support systems plus equipment that, if compromised, would undesirably jeopardize safety, security, or emergency mobility functions [3].

As a result, cybersecurity has been adopted as NPPs regulation requirement under the US code of federal regulation (CFR) [2]. Also, regulatory agencies like the US NRC and IAEA created and distributed regulatory guidelines, considering construction of cybersecurity plans and programs for NPPs. The IAEA and World Institute for Nuclear Security (WINS) are multiplying their efforts in order to protect NPPs by addressing cybersecurity issues and challenges on a global scale. Currently, some of issues include

- Issuing multiple documents addressing cybersecurity on nuclear facilities.
- Providing technical and strategic security training to involved officials of member countries.
- Offering expert guidance and capacity building to officials and representatives.

NSS-17 [17] was issued by IAEA as a technical guidance for guaranteeing computer security at nuclear facilities. Similarly, the IAEA NSS-13 [18] recommends that the available computer-based systems included in nuclear facilities must be protected against compromise, and also an appropriate threat assessment must be realized in order to prevent attacks.

Threats were classified from various adversaries' perspectives, detection and prevention mechanisms for compromises of NPPs information systems were also addressed. Additionally, nothing like usual ICS and SCADA systems, governments, and NPPs regulatory agencies specify that NPPs I&C systems must comply with the following firm safety requirements [4][19]:

- Requirements for annual maintenance, best availability and functionality levels, and environment tests.
- Nuclear reactor safety and also physical protection of nuclear material must be taking in consideration;
- Defining system security levels by bearing in mind safety level ranking, and evaluating safety risks in relation to security threats.
- Verification that security functions do not have opposing effects on the safety and functionality of facilities.
- Management and maintenance must consider the safety and reliability of systems, examination and also qualification by regulatory agencies.
- Redundancy and diversity must be taken in consideration in the design.

However, all of these efforts are continuing and necessitate indefinite time to mature.

The guidelines, standards, and recommendations provided by governments and regulatory authorities necessitate complete review to make sure that they describe and include the newest risk assessment developments, for example, cyber threat information sharing, risk assessment of tacit knowledge, dissemination of risk assessment results, etc. These features are obligatory in order to keep NPPs risk assessment up-to-the-minute on progressive cyber threats and to be able to manage cyber incidents in a proper manner.

On the other hand, at present, the abovementioned guidelines do not provide a detailed approach on imposing security controls and avoiding cyber risks.

 ISBN: 978-1-61208-628-6

IV. SECURITY CONTROLS FOR NUCLEAR POWER PLANTS

Standards are endorsing the improvement of cybersecurity in NPPs. Fig. 2 shows the standardizing processes and procedures, which are important to accomplish an international rewarding collaboration. Abundant standards addressing information security were established in recent years. Still, not all of them are practical to apply in NPPs.

Designed for I&C systems in NPPs, the new draft IEC 63096 is expected to be published in 2019. The standard aims its attention specifically on the selection and application of cybersecurity controls from the contained security controls within the catalogue. Preventing, detecting, also reacting to digital attacks against computer-based I&C systems are the major functions of the selected and applied cybersecurity controls. Based on IEC 62645 [20], IAEA, in addition to country precise guidance in the technical and security application area. Designers and operators of NPPs (utilities), systems evaluators, vendors and subcontractors, and by licensors can use this standard. For that reason, the goal of this standard is to enlarge the SC45A series of documents focusing on cybersecurity with IEC 62645 [20] as its high-level document, by classifying nuclear I&C precise cybersecurity controls for I&C systems into Safety Classes 1, 2, 3 and non-classified (NC) I&C systems. The major differences between this standard and usual IT systems or industrial automation systems standard are the safety classification of I&C nuclear systems and related safety requirements. IEC 62645 [20] was issued in August 2014, and IEC 62859 [21] was published in 2016, along with this new standard related to cybersecurity controls, are planned to be used for I&C systems and NPPs. The new standard is structured as follow:

The first main section designates the intended audience, which is distinguished by parties that are in charge of:

- I&C platform development.
- Project Engineering for I&C system, including installation and commissioning.
- Operation and maintenance of I&C system.

In the second main section, a detailed description of each security control is explained. Inside this structured representation, the purposes of Security Degrees along with the specific control are defined either highly recommended or optional. As well, additional description specifies whether the control conserves the confidentiality, integrity or availability. Each section related to a security control provides specific implementation guidance on how to implement the control; it also differentiates between I&C platform development, project engineering or operation and maintenance.

Based on IEC 62645 [20], the third main section is dedicated to the process of selecting the available security controls. Controls are allocated depending on the security degree of the particular I&C system. Tools and Legacy systems are also considered in this standard. After selecting the security controls, a threat and risk assessment is required in order to detect a residual risk that necessitates the implementation of supplementary security controls.

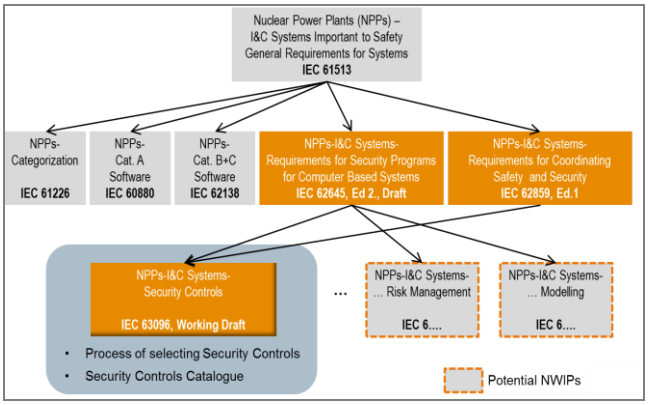

Figure 2. New IEC 63096 Security Controls standard in the SC45A standards hierarchy [3].

Concerning controls three cases are distinguished, using the guidance provided by the Draft ISO/IEC 27009 [22] on sector specific security controls. The following three cases on the refinement of ISO/IEC 27002 security controls are examined [16]:

- Security controls are adopted from ISO/IEC 27002 [16] without any adjustment. If needed, the obligatory details are added by the standardized structure.
- To meet requirements from the nuclear I&C domain, Security controls from ISO/IEC 27002 [16] were modified and described in details to better.
- In order to meet the particular requirements from the nuclear I&C domain, a new security control has been added and inserted into ISO/IEC 27002 [16] clause (5 through 18. This is the case where the ISO/IEC 27002 [16] does not define specific security controls needed in nuclear I&C.

IEC 62541 [23] defines the open platform communication Unified Architecture (OPC UA), it is an automation middleware or machine-to-machine (M2M) protocol. The standard features an object-oriented meta-model to characterize data structures and remote procedure calls, which can be dynamically explored and modified through IP communication, along with security mechanisms such as authentication and encryption. OPC UA is adaptable to manufacturing software, it defines [23]:

- An information model for structure, behavior and semantics description.
- A message model for interactions between applications.
- A communication model to carry data between end points.
- And a conformance model to guarantee interoperability between systems.

The communication services of OPC UA are mainly used in the following domains: Process automation, power plants with, traditional and renewable Building automation, and Factory automation (in particular robotics).

The OPC UA specifications are made up by 13 parts, the first seven parts are related to the core specifications e.g. the

 ISBN: 978-1-61208-628-6

concept, security model, address space model, services, information model, service mappings and profiles. The parts eight to thirteen are related to access type specifications like data access, alarms and conditions, programs, historical access, discovery and aggregates. Interoperability is achievable by using a communication standard that is platform and vendor independent, such as IEC 62451 [23] (OPC UA) and IEC 61850 [24] (Communication Networks and Systems in Substations). OPC UA is a platform-independent standard that helps into reaching interoperability between devices with dissimilar manufacturers and communication protocols. OPC UA simplifies communication by sending messages between OPC UA Clients and Servers. For example, its applicability to the nuclear context is demonstrated by Framatome. Recognizing the potential of OPC-UA in sensors, Framatome started incorporating them into monitoring instruments (SIPLUG®) for mountings and their related electric drives. The solution is employed in the nuclear Industry for monitoring critical systems in remote environments, without undesirably affecting the availability of the system [25].

V. CONCLUSION

This paper gave an overview of security vulnerabilities in I&C systems and EPS inside NPPs, by going through notorious attacks across history and listing some of the vulnerabilities that can be exploitable by malicious attackers. An introduction to a new draft standard, IEC 63096 [3] had being given. The improved performance digital technology has offered a significant influence on I&C systems design in NPPs. The nuclear industry has a conservative methodology in approaching safety, and a considerable effort is obligatory in order to provide the essential evidence and analysis to guarantee that digital I&C systems can be employed in safety-critical and safety-related applications. In general, I&C systems are inaccessible from outside communication systems. Still, this is not sufficient for secure operation inside NPPs, as in the case of Stuxnet. Interoperability has to be addressed from I&C architecture design phase, as the systems have to interact. The threat from cyber-attacks is more and more seen as a problem of national and international security as cyber-attacks evolve, become more advanced and as actors behind them are no longer limited to private hackers or organized criminals, but also nation states and insiders.

In future work, we intend to focus more on the listed vulnerabilities, and introducing security in hardware by using a trusted platform module instead of only focusing on securing software, also some best practices to widen the protection area.

ACKNOWLEDGMENT

Some of the addressed cybersecurity related topics are being elaborated as part of Framatome GmbH's participation in the "SMARTEST" R&D (2015-2018) with German University partners, partially funded by German Ministry BMWi.

REFERENCES

[1] J. Rrushi, R. Campbel, "Detecting cyber attacks on nuclear power plants," The International Federation for Information Processing (ICCIP 2008), Springer, Boston, vol. 290, 2008, ISBN: 978-0-387-88522-3.

[2] INSAG-24, International Nuclear Safety Group, "The interface between safety and security at nuclear power plants," IAEA, 2010.

[3] J. Bochtler, E. Quinn, and E. Bajramovic, "Development of a new IEC standard on cybersecurity controls for I&C in Nuclear Power Plants – IEC 63096," NPIC & HMIT 2017, San Francisco, 2017.

[4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security,", NIST, 2011.

[5] Andrews, M. Holt, "Nuclear Power Plant security and vulnerabilities," Congressional Research Service, January 2014.

[6] W. Ahn, M. Chung, B. Min, and J. Seo, "Development of cyber-attack scenarios for Nuclear Power Plants using scenario graphs," International Journal of Distributed Sensor Networks, vol. 11, April 2015, doi: 10.1155/2015/836258.A.

[7] D. Papp, Z. Ma, and L. Buttyan "Embedded systems security: threats, vulnerabilities, and attack taxonomy," 13th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2015, doi:10.1109/PST.2015.7232966.

[8] C. Baylon, R. Brunt, and D. Livingstone, "Cybersecurity at civil nuclear facilities understanding the risks," Chatham House Report, September 2015.

[9] R. Masood, "Assessment of cybersecurity challenges in nuclear power plants security incidents, threats, and initiatives," Cybersecurity and Privacy Research Institute the George Washington University, 2016.

[10] B. Kesler, "The vulnerability of nuclear facilities to cyber-attack," Defense and Diplomacy Journal, vol. 5, No. 3, 2016.

[11] Deloitte, "Security Awareness: People and Technology," [Online]. Available from: http://www2.deloitte.com/, 2017.12.19.

[12] G. Stoneburner, A.Y. Goguen, and A. Feringa, "NIST Special 800-30: Risk Management Guide for Information Technology Systems,", NIST, 2002.

[13] Joint Task Force Transformation Initiative, "NIST Special Publication 800-37 Rev. 1: Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach," NIST, 2014.

[14] E. Aroms, "NIST Special Publication 800-39: Managing Information Security Risk," NIST, 2012.

[15] "IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links," in IEEE Std 1711-2010, vol., no., pp.1-49, 2011.

[16] ISO/IEC 27002:2013, Information Technology - Security Techniques - Code of Practice for Information Security Controls, ISO/IEC.

[17] IAEA Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities," IAEA, 2011.

[18] IAEA Nuclear Security Series No. 13, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities," IAEA, 2011.

[19] ISO/IEC 27001:2005, Information Technology –information security management systems –requirement, ISO/IEC.

[20] IEC 62645:2014, Nuclear Power Plants – Instrumentation and Control Systems – Requirements for Security Programs for Computer-Based Systems, IEC.

 ISBN: 978-1-61208-628-6

[21] IEC 62859:2016, Nuclear Power Plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity, IEC.

[22] ISO/IEC 20009-1:2013, Information technology – Security techniques – Anonymous entity authentication, ISO/IEC.

[23] IEC 62451-1:2016, OPC Unified Architecture – Part 1: Overview and Concepts, IEC.

[24] IEC 61850:2013, Communication networks and systems for power utility automation, IEC.

[25] V. Watson, A. Tellabi, J. Sassmannshausen, and X. Lou, “Interoperability and security challenges of Industrie 4.0,” 2017, doi:10.18420/in2017_100.

 ISBN: 978-1-61208-628-6

Safety Mechanism Implementation for Motor Applications in Automotive Microcontroller

Chethan Murarishetty, Guddeti Jayakrishna, Saujal Vaishnav
Automotive Microcontroller Development Post Silicon Validation
Infineon Technologies Private Limited
Bengaluru, India
email: {Chethan.Murarishetty, Jayakrishna.Guddeti}@infineon.com, saujalvaishnav@gmail.com

***Abstract*— Safety is a critical feature in automotive microcontroller. Achieving highest safety standards is important in any microcontroller design. This paper presents a methodology to implement a safety mechanism in Brushless Direct Current (BLDC) Motor applications using Infineon Aurix Microcontroller modules like Generic Timer Module (GTM), Capture Compare Unit 6 (CCU6) and Input Output Monitor (IOM). The timer module in an automotive microcontroller is used in many applications like power train, power steering, transmission control, chassis, etc. Most of the recent automotive microcontrollers use GTM due to its scalable and configurable architecture. GTM combines sub-modules of different functionality in a configurable manner to form a complex timer module that serves different application domains. The BLDC motor application is implemented using different sub-modules of GTM like Timer Input Module (TIM), Timer Output Module (TOM), Sensor Pattern Evaluation (SPE) and Clock Management Unit (CMU). The safety concept is derived by using another timer module, CCU6, which implements the Motor Control application. IOM is used to compare the output signals of GTM and CCU6. IOM triggers an alarm if there is any mismatch in the output signals. Hence, a redundant approach is implemented to achieve the highest safety standard.**

Keywords*— *Safety; GTM; Automotive; Infineon Aurix Microcontroller, BLDC Motor; CCU6; IOM.

I. INTRODUCTION

In this paper, we use Infineon Aurix Microcontroller [7] to implement BLDC motor control application. The modules of the microcontroller that are used in this implementation are GTM, CCU6 and IOM. The BLDC motor application implementation is discussed in detail using GTM Integrated Protocol (IP) submodules like SPE, TIM, TOM and CMU and the safety concept for the same application will be discussed later using CCU6 and IOM.

Generic Timer Module (GTM) is used as a timer unit in automotive microcontroller due to its easy integration and configurable architecture. GTM is not just a timer, but it also performs arithmetic operations for signal processing. GTM functionality includes Engine Position Evaluation, Pulse Width Modulation (PWM) generation, PWM evaluation and signal detection, Complex waveform generation, Programmable multi channel sequencer and motor control operation.

Bosch developed the GTM IP [1]. It is designed to offer a flexible and scalable platform to cater to different hardware vendors. GTM primarily offloads the Central Processing Unit (CPU) or any computational core from a huge task load due to its high number of independent programmable sub-modules, and the CPU can perform its own tasks without spending much of CPU cycles in generating complex PWM's. The architecture block diagram of GTM-IP-104 is displayed in Figure 1 [1].

The BLDC motor is a good choice for applications that require high reliability and high efficiency. This paper talks about implementation strategy to achieve the highest safety standard for BLDC motor control applications. Infineon Aurix Microcontroller provides features to implement the safety mechanism. As per International Organization for standardizatio (ISO) 26262 [9] standard, redundancy in the implementation would achieve the highest safety standard. In this implementation, GTM is used to implement the Motor Control Application. GTM generates output signals to drive BLDC motor based on certain specific input from Hall sensors. If there is any bug in the GTM, it may lead to malfunctioning of the motor application. The consequences of this malfunction may result in minor to major accidents or it may be fatal. In order to avoid this, we suggest to enable a module called CCU6, which is part of Infineon Aurix Microcontroller, that generates output signals to drive BLDC motor based on the same hall sensor inputs which are routed to GTM. Only the output signals of the GTM are allowed to drive the BLDC motor, but not CCU6. The output signals of both GTM and CCU6 are compared by IOM module. If there is any mismatch in the output signals, the motor is stopped to avoid any unintended actions.

The rest of the paper is structured as follows. Section II provides an overview of the IP modules that are used in this safety mechanism implementation in motor control applications. Section III describes the configuration of GTM, CCU6 and IOM modules that are programmed in the host software. It also mentions the result parameters that are to be observed in the safety mechanism implementation. Section IV provides details of the measurements taken on the Infineon XMC1000 Motor Control Application Kit. Section V addresses the safety impact on automotive systems. We conclude our work in Section VI.

 ISBN: 978-1-61208-628-6

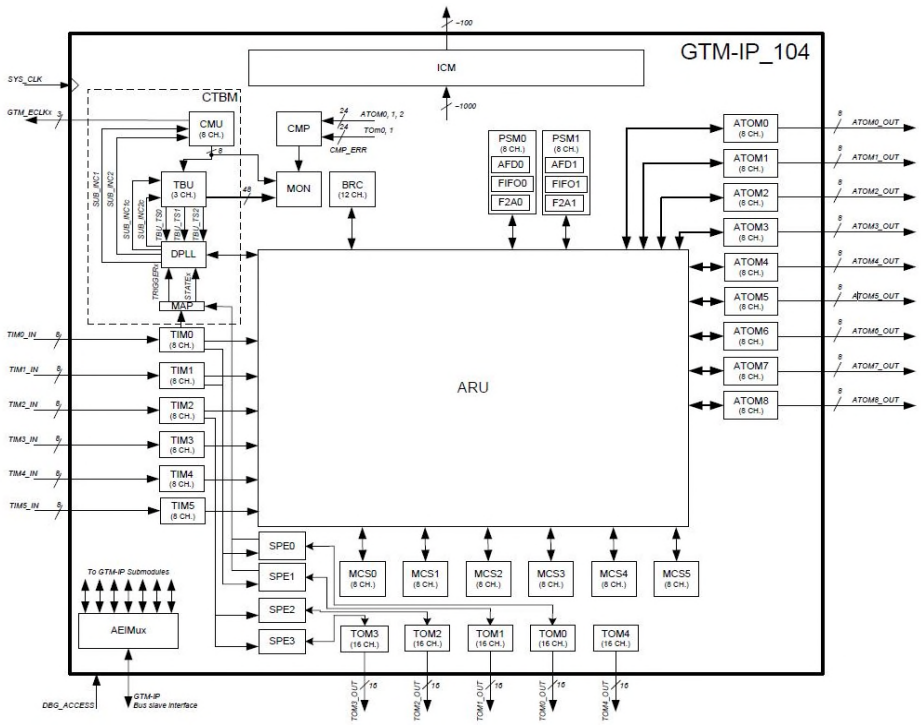

Figure 1. GTM-IP-104 Architecture Block Diagram [1].

II. OVERVIEW OF IP MODULES

This section gives a brief overview of GTM IP (CMU, TOM, TIM and SPE) modules and Infineon specific modules (CCU6 and IOM) that are used in the safety mechanism implementation.

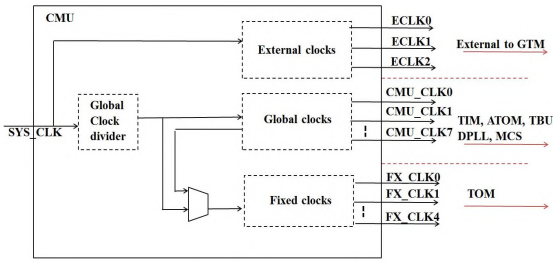

Figure 2. CMU submodule architecture [2].

A. Clock Management Unit (CMU)

The CMU provides the clocks to the internal sub-modules of GTM IP. The CMU sub-module architecture is shown in Figure 2 [2]. The CMU sub-modules description is given below.

1) Configurable Clock Generation Unit (CFGU): 8 programmable clocks available for TIM, ATOM, MCS, DPLL and TBU unit.

2) Fixed Clock Generation Unit (FXU): It generates five fixed clocks for TOM sub-module.

3) External Clock Generation Unit (EGU): Three clock generation circuits available to generate GTM-IP external clocks.

4) The CMU has a sub block Global Clock Divider which divides global clock signal SYS_CLK and the resulting clock is distributed to the rest of the GTM modules as a clock source. For this application, a 100MHz clock is provided to each sub-module of the GTM.

B. Timer Output Module (TOM)

Each instance of the TOM module provides 16 output channels for PWM generation. The architecture of a TOM channel is shown in Figure 3 [2]. A 16-bit counter and two capture compare units (CCU0 and CCU1) for period and duty cycle are available for each channel. Each capture compare unit has a 16-bit compare register. Capture Compare Unit (CCU0) register is used to program Period and Capture Compare Unit 1 (CCU1) register is used to program Duty Cycle of a PWM signal that is to be generated by the TOM Channel.

C. Timer Input Module (TIM)

The GTM captures the input signals coming from IO through the TIM sub-module. Each TIM channel has different modes of operations like PWM signal characterization, input edge counting, interrupt generation after specific number of

 ISBN: 978-1-61208-628-6

rising and/or falling edges. Glitch filtering mechanisms are available for each channel in all the TIM instances. Each TIM instance has 8 channels each.

D. Sensor Pattern Evaluation (SPE)

The SPE sub-module evaluates three hall sensor input and, in conjunction with TIM and TOM modules, drives a BLDC motor. The SPE module functionality includes engine direction detection and signaling, output pattern generation, flexible output pattern generation, fast shut-off mechanism, sensor jitter detection mechanism, etc.

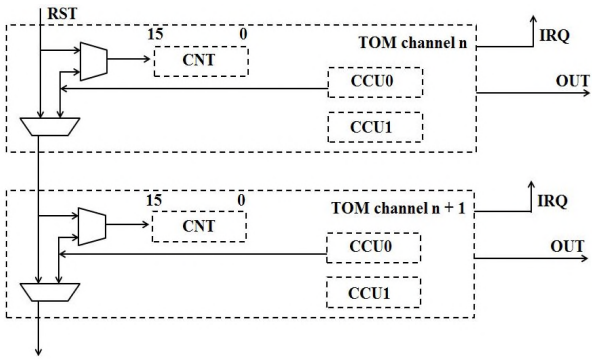

Figure 3. TOM channel architecture.

E. Capture and Compare Unit (CCU6):

CCU6 is another timer IP module in Infineon Aurix microcontroller which supports the control of Brushless DC motor applications using Hall sensors inputs and generates desired PWM to drive the BLDC motor. It has input modules to receive HALL sensor inputs and output modules to drive PWM to the motor inverter bridge.

F. Input Output Monitor (IOM):

IOM is a hardware module in Infineon microcontroller which serves as a smart I/O comparison unit. In this implementation, IOM is used to compare the period and duty cycles of the output signals of GTM (reference signals) and CCU6 (monitor signals). IOM can signal an error to the Safety Management Unit if there is any mismatch in the signals generated out of GTM and CCU6.

III. PROPOSED METHODOLOGY

Firstly, the implementation of the BLDC motor application using GTM sub-modules is explained. The commutation of BLDC motor is controlled electronically. Stator windings must be energized to rotate the BLDC motor. To understand which winding to be energized, it is required to know the rotor position. Hall sensors data which are embedded in the stator is used to determine the position of the rotor.

Figure 4 shows the block diagram of the 3-phase BLDC drive engine which includes the 3-phase inverter and the BLDC motor. Here, the Inverter Bridge is controlled by the PWM to give proper commutations such that two of three phases are with ON state and the remaining one is with floating state. Figure 5 shows the widely used PWM technique, which has been applied to the BLDC motor drive applications. This method does not require a virtual neutral point and large amount of filtering, apart from that it reduces conduction loss [3][4].

Figure 6 shows the control flow of the BLDC motor starting from Hall sensor – TIM – SPE – TOM - BLDC Inverter Bridge. The rotor position is detected using three Hall sensors. The input signal coming from the Hall sensor is sampled in TIM and the validity of the input pattern sequence can be detected and signaled. When a valid input pattern is detected, the SPE sub-module can control the output of a dedicated TOM sub-module, which generates the desired PWM signal to drive the motor.

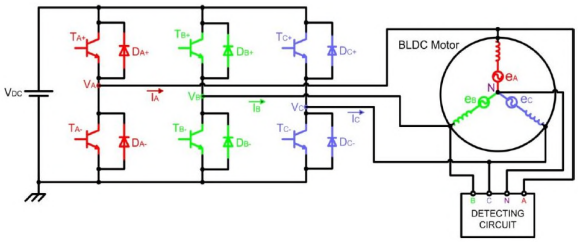

Figure 4. Block diagram for 3-phase BLDC drive [3].

A. GTM IP initialization

- Enable clock control register of GTM IP.
- Enable GTM interrupt mechanism.
- Configure appropriate clock divider value.

B. TIM Configuration

- TIM channels to be configured to receive inputs from GPIO port pins (port pins that sample the HALL sensors).
- TIM channels to be configured in such a way that input waveform coming from port-pin should be filtered to remove any input glitch before it is applied to the SPE module.

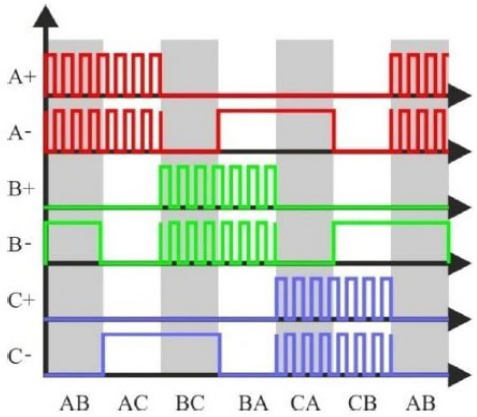

Figure 5. PWM applied to inverter of BLDC motor [3][4].

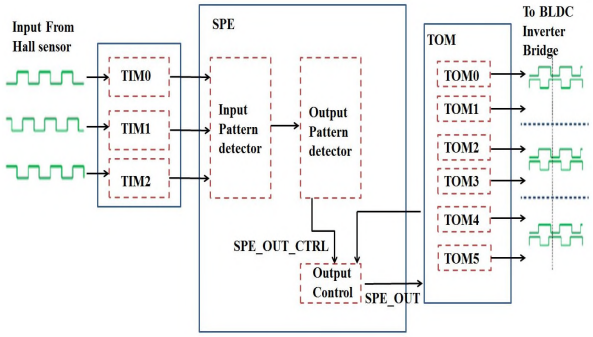

Figure 6. BLDC motor control flow.

- TIM output is sent to SPE.

C. TOM Configuration

- Six TOM channels are configured to generate PWM, as shown in Figure 5.
- Configure any two channels (whose signal is used as A+ and A- for SPE module) with required duty cycle and period for ideal motor rotation. The motor rotation speed can be controlled by varying the duty cycle.
- All six channels are configured in such a way that the output of each channel is controlled by 'SPE'. This eventually produces the six controlling signals for motor inverter bridge. This output is sent to the GPIO pins.

D. SPE Configuration

- Configure the SPE sub-module for motor rotation in forward direction using the SPE control status register.
- SPE input pattern definition register holds the valid input pattern for the motor rotation. The Hall sensor pattern is sampled by TIM and it will be matched with this register. A possible sample pattern for three input signal is as shown in Figure 8. SPE module expects that at every new pattern only one of three input signals changes its value.
- On successful match of input pattern, SPE output definition register defines the output selection for six TOM channels based on the actual input pattern. Depends on the internal architecture of SPE module and register configuration of SPE output pattern register, to produce PWM waveform as shown in Figure 5, values to be programmed in SPE output definition register are shown in TABLE 1.

E. PORT configuration

- Configure three port pins to receive Hall sensor outputs from the motor control board, which serves as inputs to TIM channels.
- Configure 6 port pins to send desired TOM channel PWM outputs to the Inverter Bridge for motor control rotation.

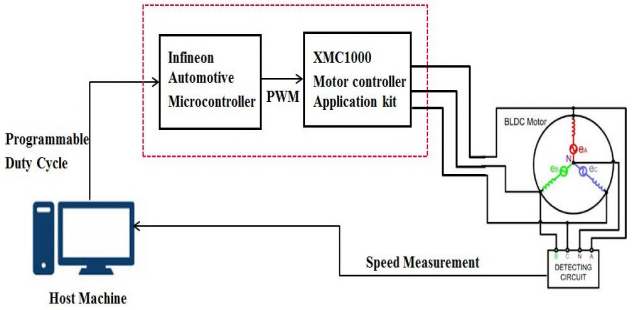

Figure 7. System Block Diagram.

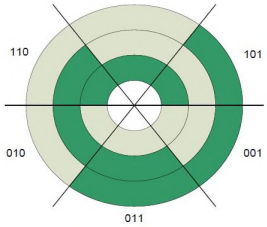

Figure 8. SPE sample input pattern [1].

TABLE 1- SPE OUTPUT DEFINITION REGISTER VALUE

Pattern value	Forward direction	Backward direction
Pattern 0	0x4EA	0xE4A
Pattern 1	0xAE4	0xA4E
Pattern 2	0xEA4	0x4AE
Pattern 3	0xE4A	0x4EA
Pattern 4	0xA4E	0xAE4

F. CLOCK configuration

- Program CMU global and local clock dividers.
- Fixed Clock Generation Unit configured to provide clock to TOM.
- Program Configurable Clock Generation Unit to provide clock for TIM, SPE and other modules.
- Fixed clock and configurable clock are enabled.

G. Capture Compare Unit (CCU6)

- Configure CCU6 of Infineon Microcontroller to receive Hall sensors inputs from I/O pins (which is being routed to TIM as well) and generate 6 output signals. These outputs will not be used to drive the Inverter Bridge, but for comparison with GTM TOM outputs described in Section III, C.

 ISBN: 978-1-61208-628-6

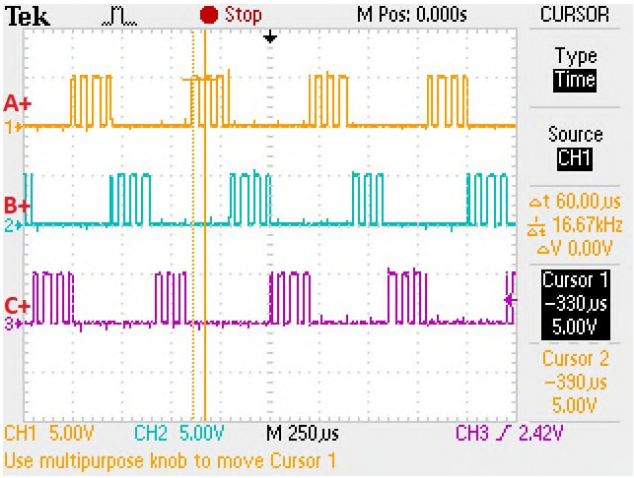

Figure 9. High switch PWM waveform

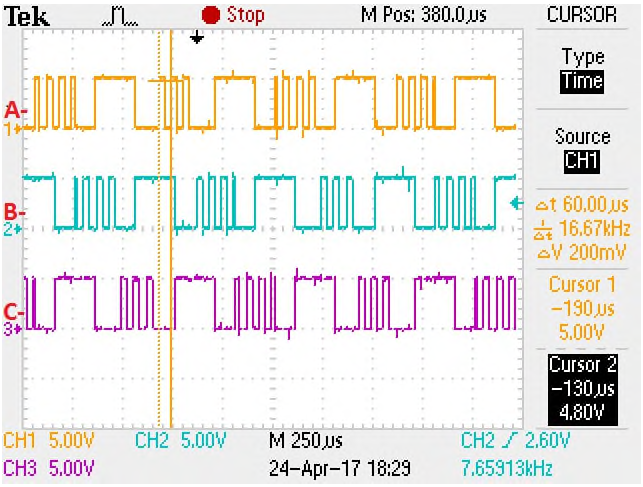

Figure 10. Low switch PWM waveform.

H. *Comparision of output results*

- IOM module of Infineon Microcontroller monitors the signals coming from GTM and CCU6. IOM triggers an alarm to the safety management unit if there is any mismatch in the output (period, duty cycle and edge count). The alarm is forwarded to the Safety management unit and appropriate action will be taken upon alarm trigger.
- GTM module is configured to run the BLDC motor at a desired speed by Host machine/software and the speed of the rotating motor is measured using the speed measurement circuit whose result is given back to the host-machine. Software running on the Host machine compares both values (programmed and read back) and indicates if the motor function is successful or not.

IV. MEASUREMENTS AND RESULTS

The BLDC motor application methodology is implemented using Infineon Aurix microcontroller which uses GTM and CCU6 as timer units. This microcontroller is used with Infineon XMC1000 Motor Control Application Kit, which includes XMC1300 CPU card and the BLDC motor from maxon. Figure 7 shows the flow chart of the implementation.

.

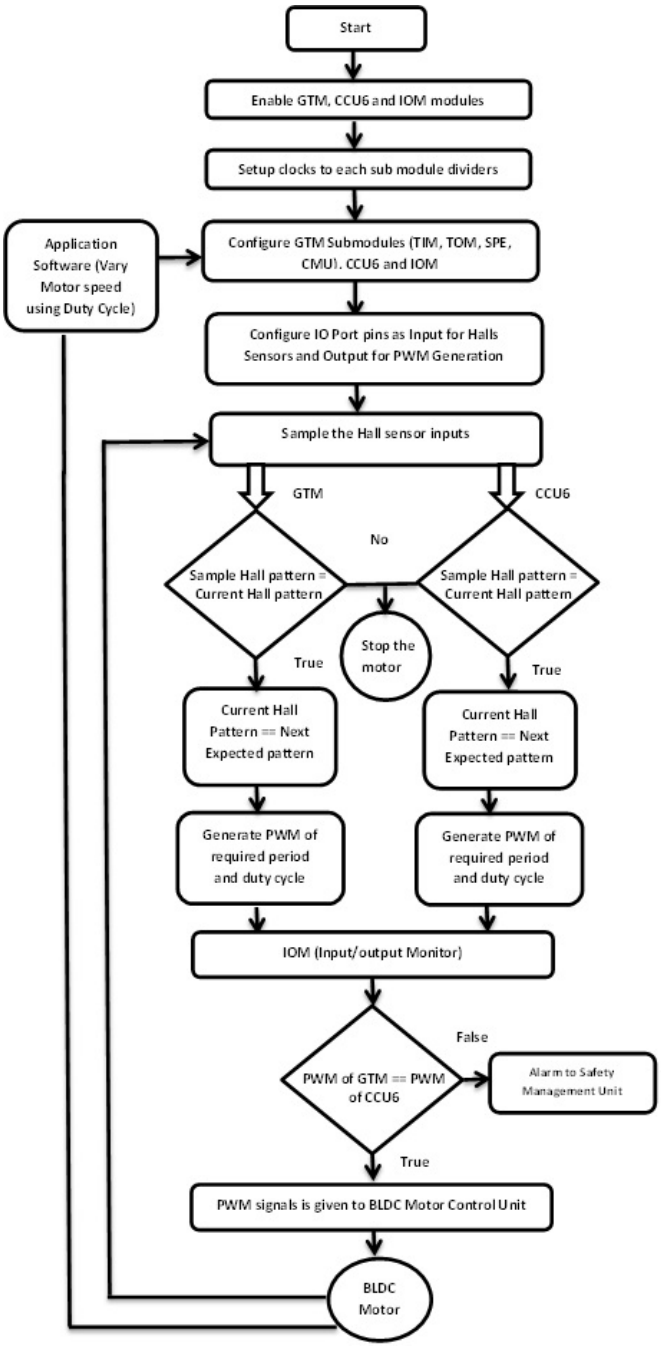

Figure 11. Flow-chart of proposed safety methodology.

The PWM applied to the BLDC motor, which is generated out of SPE-TOM, is shown in Figure 9 and Figure 10. Period and duty cycles are programmed to generate 16.67 KHz frequency PWM, which is ideal for motor rotation. The easiest way to determine revolutions per minute (RPM) is to monitor the pulse frequency from the sensor using a digital input module and then calculate RPM using equation (1). The output of CCU6 signals are not routed to the BLDC motor. CCU6 output signals are only used for comparison with respect to GTM output signals. Output signals from CCU6 and GTM will be monitored by the IOM module. IOM module signals an alarm to the Safety Management Unit if it observes any mismatch between GTM outputs and CCU6 Timer Outputs.

$$\mathrm{RPM} = \frac{\left(\text{pulse freq in}\,\frac{\text{pulses}}{\text{sec}}\right) * \left(60\,\frac{\text{sec}}{\text{min}}\right)}{\left(\text{Sensor}\,\frac{\text{pulses}}{\text{revolution}}\right)} \qquad (1)$$

V. SAFETY IMPACT IN AUTOMOTIVE SYSTEMS

Implementation of this concept in Motor Applications based on GTM, CCU6 and IOM features using Infineon's Automotive Microcontroller gives automotive ECU's a huge safety advantage at system level. Leveraging Infineon microcontroller GTM, CCU6 and IOM module features to create redundancy helps in meeting ever so stringent safety goals. These solutions give a competitive edge over other solutions available currently.

VI. CONCLUSION AND FUTURE WORK

In this paper, we first presented a Generic Timer Module introduction. Hall sensors and TIM were used in rotor input pattern detection and the output pattern generated to drive the BLDC motor using SPE in combination with the TOM sub-module. A safety mechanism was implemented based on a redundant approach using GTM and CCU6 IPs. 2 layers of safety check were performed in the above implementation. First, the IOM triggers an alarm if there is any mismatch in the output of GTM and CCU6 and, second, the motor function can be verified with the help of self-checking of motor speed using sensor and RPM measurement circuit. This implementation would achieve the highest level in Automotive Safety Integrity as defined by International Organization for Standardization (ISO) 26262 [9] Functional Safety for Road Vehicles standard. As an extension to this work, we will implement a speed control of the BLDC motor using PI controller and fuzzy logic controller [8], which will be developed using the MATLAB toolbox.

ACKNOWLEDGEMENT

The authors thank Mr. Shivaprasad Sadashivaiah and Vijay Chachra, Infineon Technologies India, for their support in publishing this paper. We also thank our design, verification, and concept engineers for their support during the trial runs of this method.

REFERENCES

[1] GTM-IP Specification v 1.5.5.1[Online], April 2018: http://bosch-semiconductors.cn/media/automotive_electronics/pdf_2/ipmodules_3/timer_1/GTM-IP_104_Specification_v1551_AppendixB.pdf

[2]GTM-IP Cookbook [Online], April 2018 http://bosch-semiconductors.cn//media/automotive_electronics/pdf_2/ipmodules_3/timer_1/GTM_Cookbook_v05.pdf

[3] J. C. Gamazo-Real, E. Vázquez-Sánchez, and J. Gómez-Gil. "Position and Speed Control of Brushless DC Motors Using Sensor less Techniques and Application Trends." Sensors (Basel, Switzerland) 10.7 (2010): 6901–6947. PMC. Web. April 2018.

[4] V. U. S. Pola and K. P. Vittal, "Recent Developments in Control Schemes of BLDC Motors," *2006* IEEE International Conference on Industrial Technology, Mumbai, 2006, pp. 477-482. Doi: 10.1109/ICIT.2006.372247

[5] XMC1000 Motor Control Application Kit, Infineon Technologies [Online], April 2018: https://www.infineon.com/cms/en/product/evaluation-boards/KIT_XMC1X_AK_MOTOR_001/productType.html?productType=db3a30443ba77cfd013baec9ca5c0caa#ispnTab1

[6] Aurix starter and application kit [Online] April 2018 p27: https://www.infineon.com/dgdl/Infineon-TriCore_Family_BR-2018-BC-v03_00-EN.pdf?fileId=5546d4625d5945ed015dc81f47b436c7

[7] Infineon Aurix Microcontroller [Online] April 2018: https://www.infineon.com/cms/en/product/microcontroller/32-bit-tricore-microcontroller/aurix-safety-joins-performance/aurix-2nd-generation-tc3xx/

[8] M. Çunkas and O. Aydoğdu, Realization of Fuzzy Logic Controlled Brushless DC Motor Drives Using Matlab/Simulink. Math. Comput. Appl. 2010, 15, 218-229.

[9] International Organization for Standardization [Online], April 2018: https://www.iso.org/standard/43464.htm

 ISBN: 978-1-61208-628-6