PhD Proposal in Artificial Intelligence and Machine Learning

Methodology for integrating neural network IP in a chip with safety assurance

Advisor (s):
Kevin Delmas and Claire Pagetti (ONERA), `name.surname@onera.fr`, `https://www.onera.fr/en/staff/name-surname`
Franck Galtié, (NXP)

Net salary: 2096€ per month with some teaching (64 hours per year on average)
Duration: 36 months

Context

Machine learning-based applications, and in particular neural networks, are becoming widespread in the automotive domain. There are two ways to code them: either off load the execution on a cloud or execute the application on an embedded platform. In this thesis, we consider the second case where the neural network is involved in safety critical applications and executed on board. This means that the implementation must fulfill several properties such as real-time guarantees (i.e. the WCET Worst Case Execution Time must be computable) and safety (i.e. hardware random failure must be detected and mitigated). In the automotive domain, those properties are summarized in the standard ISO 26262 [4]. NXPis a chip maker that designs for many years chips for the embedded market either for aeronautic with the QorIQ Series [6] or automotive with the S32 platform [7]. The automotive chips are designed so that many safety measures are provided. In particular, many hardware run-time checking or SW self-tests are integrated to detect random fault and mitigate the effect on the safety related system (ie. clock monitoring, Error Correction Code; voltage monitoring, Parity, Built-in slef-test, Core Self-test, etc..).

Objectives

The objective is to prepare the next generation of chips to be used for vision-based computer, automotive and autonomous driving or radar / lidar computing. Those chips will integrate neural network hardware IP and should ensure the same level of safety as expected by the ISO 26262.

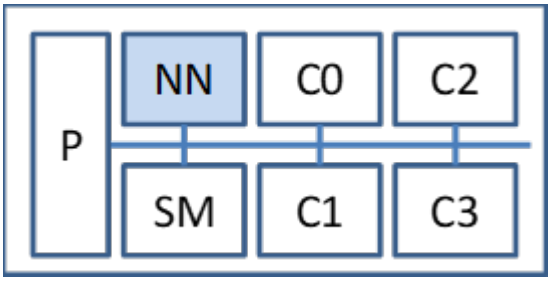

Figure 1: simplified architecture view

A simplified architecture view is portaye in Figure 1: 4 cores (C0 to C3) are connected via an interconnect to a series of peripherals (P, including the DDR or the Ethernet controller), a new hardware component (NN) is in charge of the neural networks computation and the safety component (SM for safety manager) is charge of supervising, making diagnostic and taking decisions (safe state, degraded modes, etc..). Basically, the safety process used to demonstrate the safety integrity level expected by the Iso26262is:

- Identify the possible hardware failures that may occur on the NN IP chip
- Identify the observable effects (called failure modes) of these HW failures
- Provide the monitoring mechanisms integrated to the NN chip used to detect the identified failure modes,
- Demonstrate that the detection ratio and the likelihood of undetected failure modes comply to the requirement provided in the Iso26262,
- Provide recovery mechanisms that can be used to mitigate the HW failures

Such a process has been applied successfully for decades on classical HW IP. Nevertheless, due to the specificities of NN the following issues arise:

1. What are the HW random failure of this novel NN IP
2. What are the observable consequences (failure modes) of a given HW failure? Such identification is not trivial since the consequence of an HW failure may be significantly impacted by the NN implemented on the IP.
3. What are the relevant monitoring mechanisms able to detect the failure model?
4. What kind of evidences can be used to demonstrate a detection ratio?
5. How the safety manager should be modified and extended to provide the recovery mechanisms of the NN component? Is it possible to define a low-level safety channel containing the safety effects of the HW failure?
6. Is there any SW tool which could potentially help make the assessment of the completeness, readiness and robustness of the safety concept defined for the Neural Network?

Addressing these issues may likely need some novel analyses thus impacting the initial assessment process. Consequently, these new activities must be integrated in a generic safety methodology to assess the NN within the System on Chip (SoC). This methodology must be carefully designed to be easily integrated to the safety assessment process of the Iso26262.

PhD Progress

First of all, the PhD student will get acquainted with the safety approach [8, 3] in general and the application of safety for chip design at NXP. They will also understand the next chip architecture and make experiments on the FPGA-based emulator developed at NXP. In parallel, a bibliography will be made on neural networks and their implementations in embedded systems [5, 1]. The next step will be to identify the potential random hardware failures associated to the NN component with a systemic approach (e.g. [2]), to characterize their effect and to validate the assumption by developing an injection fault strategy on the emulator. From those, some hardware mitigation means will be defined and assessed, together with a formal definition of the way the safety manager will interact with the NN component and the application software. Finally, a generic and general safety methodology will be developed to assess NN components and provide guarantees acceptable by an Iso26262evaluation. The PhD student will have to make some stays at Austin NXP.

References

[1] Papers associated with the waters 2019 industrial challenges.

[2] Frédéric Boniol, Youcef Bouchebaba, Julien Brunel, Kevin Delmas, Claire Pagetti, Thomas Polacsek, and Nathanaël Sensfelder. Phylog: a model-based certification framework. In *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, pages 1–9. IEEE, 2018.

[3] Marco Bozzano, Adolfo Villafiorita, Ove Åkerlund, Pierre Bieber, Christian Bougnol, Eckard Böde, Matthias Bretschneider, Antonella Cavallo, C Castel, M Cifaldi, et al. Esacs: an integrated methodology for design and safety analysis of complex systems. In *Proc. ESREL*, pages 237–245, 2003.

[4] ISO. ISO 26262 Road vehicles Functional safety, 2018.

[5] Seul Jung and Sung su Kim. Hardware implementation of a real-time neural network controller with a dsp and an fpga for nonlinear systems. *IEEE Transactions on Industrial Electronics*, 54(1):265–271, 2007.

[6] NXP. QorIQ Processing Platforms: 64-bit Multicore SoCs .

[7] NXP. S-32 Automotive Platform.

[8] Alain Villemeur. *Reliability, availability, maintainability and safety assessment.* John Wiley & Sons, 1992.

Application Procedure

Formal applications should include detailed CV, a motivation letter and transcripts of bachelors' degree. Samples of published research by the candidate and reference letters will be a plus. Applications should be sent by email to: advisor email

More information about ANITI: `https://aniti.univ-toulouse.fr/`