Towards the Fomal Verification of Ethical Decision-Making in Digital Ethical Twins (DETs) for Smart Manufacturing

In the context of the project ANR JCJC DET, the DETs will be developed to gain more users' confidence in the decisions made by them so that more Digital Twins (DTs) will realize direct control from DTs to Physical Objects (POs). DETs are expected to conduct ethical reasoning about their behavior within smart manufacturing. DETs are also autonomous entities, meaning that they can communicate with each other and act autonomously. The environment of smart manufacturing is highly volatile as well since it operates in a complex ecosystem where machines, humans, and digital systems interact in real time. Continuous data flows, adaptive automation, and rapidly changing production requirements lead to constant fluctuations in operational conditions. In this complex environment, **the major challenge is "How to ensure that decisions of the DETs consistently respect ethical principles from both single DET and the DET system levels?".** The DET system comprises multiple DETs that collaborate autonomously to fulfill their objectives in a share environment.

Model checking seems to be very promising for the formal verification of ethical decision-making in DETs. It is a formal verification technique used to automatically verify whether a system satisfies the given properties. However, industrial applications of model checking are very limited. For example, Bentahar et al. (2013) used symbolic model checking to verify composite web services via a ticket reservation system. This system just described the operation behavior of the ticket reservation from a global point of view. No details about reservation processes were involved. Dennis et al. (2016) proposed a theoretical framework for formally verifying ethical choices in autonomous systems. Three case studies were exploited to illustrate the feasibility of this framework. However, each case study just involved one agent instead of multiples agents. Liu and Bril El Haouzi (2023b) extended Dennis's work by flexibilizing the model of ethical rules. So their approach adapted better to the evolving environment. Kamali at al. (2017) formally verified the individual agent's code for the autonomous vehicle platooning and stated "We are not going to formally verify the vehicular control systems, and leave this to standard mathematical (usually analytic) techniques from the Control Systems field.". On the other hand, several studies tended to verify the whole system. El Menshawy et al. (2018) modeled checking real-time conditional commitment logic using transformation. They chose the aircraft landing gear system in Boniol et Wiels (2014) as their case study, which was a real and industrial case. Liu et al. (2021) applied model checking to verify the agent-based simulation system for aircraft maintenance scheduling. The simulation system was detailed in Liu et al. (2019). The authors also improved their simulation model thanks to the counter-example proposed by model checker NuSMV. To conclude, few studies consider the ethical aspect when formally verifying systems of interest. The systems to be verified are often limited to "toy examples" [Bentahar 2013, Dennis 2016, Liu 2023b]. To the best of our knowledge, no one verifying DT models has considered the ethical aspect. This thesis will attempt to translate ethical principles into specifications to be verified. The formal model will take each DET and the whole system of DETs into consideration. It will finally guarantee that the behavior of single DET model and the whole DET system will respect ethical principles.

The objective of this thesis is to develop a rigorous approach for the formal verification of ethical decision-making of DETs at both the single DET model and the DET system levels. The focus would be placed on model checking techniques to ensure that DETs behave in accordance with both functional and ethical requirements. To this end, the DET models will be transformed into formal representations compatible with model checkers. This work will include an in-depth investigation of **the correctness and soundness of the model transformations**, addressing both theoretical foundations and practical implementation challenges. Furthermore, system-level requirements—including those derived from ethical principles—will be translated into verifiable properties, enabling automated verification of compliance within the model checking environment.

To reach the objective, this thesis will need to answer the following five research questions:

1. **DET formal modelisation: How to formalize the single DET model and system-level behaviors?** The DET system includes the single DET model and system-level behaviors. The single DET model behaviors involve any reachable details in the components. For example, a robotic arm picks and places components on an assembly line. The system-level behaviors refer to how an entire system functions, interacts, and evolves over time where the inner details of the components are ignored. For instance, the production system adjusts workflows dynamically based on the real-time demands. This makes formally verifying both levels of the DET possible. The formal description methods should be expressive to describe complex behaviors and be flexible to be transformed into other formal models.
2. **Meta-model transformation: How to ensure correctness and completeness during the meta-model transformation?** The meta-model transformation will be grounded in the theory of formal description methods, such as Büchi automata, and in the underlying semantics of model checkers, for example, the Kripke structures used in NuSMV. The meta-transformation process will aim to demonstrate the equivalence between the source and target formal representations, thereby establishing the theoretical soundness and feasibility of the model transformation approach.
3. **Model transformation**: **How to ensure correctness and completeness during the model transformation?** This task will focus on deveoping an algorithm to automatically transforming the formal DET model—for example, a Büchi automata-based representation—into a formal model compatible with model checkers, such as the NuSMV specification format. Automation of this transformation process is essential to ensure efficiency, accuracy, and scalability. The outcome of this task will be a model-ready input for the model checker, enabling formal verification of both functional and ethical properties.
4. **Model checking: How to formally verify the system?** Properties expressed in Computational Tree Logic (CTL) and Linear Temporal Logic (LTL) will be defined to capture the expected behaviors of the DET, including both functional and ethical aspects. These temporal logic properties will then be applied to the transformed model to verify the compliance of the DET with the specified requirements. In cases where the model violates any property, the model checker will generate counterexamples, providing concrete scenarios that illustrate the deviations from the expected behavior.
5. **Experimental validation**: **How to validate the proposed formal verification method?** This thesis will ultimately focus on demonstrating the reproduction of counterexamples generated by the model checker in real-world scenarios. Once the identified errors are addressed at the formal verification level, the corresponding issues in practical applications should also be observed and resolved. Conversely, if problems are observed in real scenarios, relevant properties can be formalized, allowing the model checker to generate corresponding counterexamples. This experimental process will thus provide a concrete illustration of how formal methods can be effectively applied in practice.

References:

Bentahar, J., Yahyaoui, H., Kova, M., & Maamar, Z. (2013). Symbolic model checking composite web services using operational and control behaviors. Expert Systems with Applications, 40(2), 508-522. https://doi.org/10.1016/j.eswa.2012.07.069

Boniol, F., & Wiels, V. (2014). The landing gear system case study. In International Conference on Abstract State Machines, Alloy, B, TLA, VDM, and Z (pp. 1-18). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-07512-9_1

Dennis, L., Fisher, M., Slavkovik, M., & Webster, M. (2016). Formal verification of ethical choices in autonomous systems. Robotics and Autonomous Systems, 77, 1-14. https://doi.org/10.1016/j.robot.2015.11.012

El Menshawy, M., Bentahar, J., El Kholy, W., & Laarej, A. (2018). Model checking real-time conditional commitment logic using transformation. Journal of Systems and Software, 138, 189-205. https://doi.org/10.1016/j.jss.2017.12.042

Kamali, M., Dennis, L. A., McAree, O., Fisher, M., & Veres, S. M. (2017). Formal verification of autonomous vehicle platooning. Science of computer programming, 148, 88-106. https://doi.org/10.1016/j.scico.2017.05.006

Liu, Y., Wang, T., Zhang, H., & Cheutet, V. (2021). An improved approach on the model checking for an agent-based simulation system. Software and Systems Modeling, 20(2), 429-445. https://doi.org/10.1007/s10270-020-00807-4

Liu, Y., Wang, T., Zhang, H., Cheutet, V., & Shen, G. (2019). The design and simulation of an autonomous system for aircraft maintenance scheduling. Computers & industrial engineering, 137, 106041. https://doi.org/10.1016/j.cie.2019.106041

Liu, **Y.**, & El Haouzi, H. B. (2023b). Formal verification of ethical choices in industrial cyber-physical systems. In IEEE Conference on Systems, Man, and Cybernetics, SMC 2023. https://10.1109/SMC53992.2023.10394479