Review of "XANDAR: An X-by-Construction Framework for Safety, Security, and Real-Time Behavior of Embedded Software Systems"

1. Main Technical Contributions

This paper proposes the XANDAR framework, which is a new X-by-Construction (XbC) design method specifically designed for the security, reliability, and real-time behavior of embedded software systems. Its main technical contributions include a model-based toolchain that combines design time validation with runtime assurance implemented based on virtual machine manager architecture. This framework not only ensures compliance with critical security and reliability standards, but also supports integration with machine learning (ML) applications. This article focuses on introducing some innovative features, such as progressive software synthesis, time and resource verification, and the application of security/reliability modes. Its runtime architecture is based on XtratuM Next Generation (XNG) Virtual Machine Manager, ensuring time and space isolation. In addition, the framework supports high-performance hardware platforms, bringing significant progress to the development of fault safety and fault operating systems in the automotive and aviation fields.

2. Possible Applications

The functionality of the XANDAR framework can be directly applied to embedded system design in industries that require high security and reliability. For example, automotive systems such as autonomous driving platforms can utilize the XANDAR framework to ensure real-time response to critical events while preventing external threats. In addition, avionics systems, such as the tactical air risk mitigation system TARMS discussed in this article, can benefit from this robust design framework for managing complex flight safety operations. Due to its focus on integrating machine learning applications and managing distributed systems, this framework is equally applicable to industrial automation, robotics, and intelligent infrastructure systems that require high security and reliability.

3. Possible Future Extensions

Future research work can extend the functionality of the XANDAR framework in multiple directions. For example, automating the selection of safety/reliability modes that meet specific system requirements can further simplify the development process. In addition, enhancing support for underlying peripheral drivers and expanding compatibility with more runtime platforms will significantly improve the usability of the framework. Another promising direction is to achieve multi platform deployment, allowing software architecture to run in multiple interconnected environments. Finally, integrating advanced machine learning model validation and runtime adaptability will further enhance the applicability of the framework in cutting-edge artificial intelligence driven systems.

4. Choice of Paper and Personal Interest

The reason why I chose this article is the interdisciplinary research between embedded software engineering and security critical system design. These topics are not only the core direction of my academic research, but also the main areas of my professional experience. As a master's student with experience in embedded systems, I find the XANDAR framework particularly attractive for addressing the multiple challenges of modern embedded systems through a holistic approach. This article has deepened my understanding of model-based development and runtime architecture for virtual machine manager drivers, which is highly consistent with my academic

research focus on system reliability and security. In addition, the discussion in this article about integrating machine learning into security critical environments is consistent with my current projects involving artificial intelligence applications in embedded systems.

5. Review Details

- **Reviewer:** Xukang Wang
- **Date:** November 1, 2024
- **Citation:** T. Dörr *et al*., "XANDAR: An X-by-Construction Framework for Safety, Security, and Real-Time Behavior of Embedded Software Systems," *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Valencia, Spain, 2024, pp. 1-6, doi: 10.23919/DATE58400.2024.10546852.