Systematic Correct-by-Construction Design for Industrial Real-Time Communication

– Friederike Bruns

Abstract

Nowadays, safety-critical manufacturing processes are often controlled by Industrial Distributed Control Systems (IDCS) employing an event-based execution paradigm. The necessity to react to events as soon as they occur counteracts the predictability of strictly scheduled real-time software and adds to the complexity. This leads to the necessity to ensure real-time behaviour in IDCS for safe and efficient operation despite the event-based approach. Following a correct-by-construction development process, such as contract-based design, allows to provide certificates about the correct system behaviour and to mitigate the costs for design cycle re-iterations. This requires in depth knowledge about the overall system behaviour at design time. However, conventional modelling languages for IDCS often abstract the intricacies of the network communication process away. This abstraction can significantly impact execution behaviour, particularly considering the increasing complexity of network configurations over time. The main contribution of this thesis is the extension to the modelling language IEC 61499 tailored for IDCS to enhance the modelling flow of distributed control systems with focus on guaranteeing the required timing behaviour. This extension aims to model the logical messages transmitted over physical channels. The novel modelling elements, **message** and **channel**, serve as the foundation for the correct-by-construction design approach. By explicitly mapping **messages** to **channels**, developers can systematically design their industrial distributed control following a component-based refinement resulting in valid mappings that guarantee adherence to timing requirements. Due to typical network complexity, network configuration itself is rather error-prone. Thus, it is a risk to leave this critical step as an independent unit of the development process. Accordingly, this thesis suggests to utilise the additional information provided within the proposed modelling language enhancement to automate the network configuration saving development time, reducing potential errors and, thereby, preserving the timing specification. The evaluation demonstrates that the modelling enhancement supports several IEC 61499 applications, the examined timing properties arising in such scenarios are utilised for validating the proposed configuration flow, and the overall proposed design flow facilitates the application of verification and validation techniques. Moreover, the evaluation examines the limitations of the proposed approach specifically showcasing arising challenges regarding scalability, due

to technological constraints. This becomes an issue considering reconfiguration efforts, which is addressed in the field of scheduling techniques for network communication protocols. Accordingly, the evaluation highlights the applicability of the proposed approaches and points out possible future enhancements. To conclude, this thesis promotes a systematic and certifiable design approach for distributed control systems, enhancing the reliability and efficiency of real-world manufacturing processes.