Unreliable yet Useful – Reliability Annotations for Data in Cyber-Physical Systems

Michael Engel, Florian Schmoll, Andreas Heinig, and Peter Marwedel
Design Automation for Embedded Systems
Faculty of Computer Science
TU Dortmund, Germany
Email: {firstname.lastname}@tu-dortmund.de

Abstract: Today, cyber-physical systems face yet another challenge in addition to the traditional constraints in energy, computing power, or memory. Shrinking semiconductor structure sizes and supply voltages imply that the number of errors that manifest themselves in a system will rise significantly. Most cyber-physical systems have to survive errors, but many systems do not have sufficient resources to correct all errors that show up. Thus, it is important to spend the available resources on handling errors with the most critical impact.

We propose an "unreliability" annotation for data types in C programs that indicates if an error showing up in a specific variable or data structure will possibly cause a severe problem like a program crash or might only show rather negligible effects, e.g., a discolored pixel in video decoding. This classification of data is supported by static analysis methods that verify if the value contained in a variable marked as unreliable does not end up as part of a critical operation, e.g., an array index or loop termination condition. This classification enables several approaches to flexible error handling. For example, a cyber-physical system designer might choose to selectively safeguard variables marked as reliable or to employ memories with different reliability properties to store the respective values.

This work is supported by the DFG Priority Program SPP1500 under grant no MA943/10-1