Energie der ausgeführten Tasks (E_K, E_A, E_D) innerhalb des 10ms dauernden Messzyklus und der Ruheenergie der DSP E_R, die während dieser Zeit allein dadurch entsteht, dass die DSP nicht von der Stromversorgung entkoppelt sind. Das heißt für die *fail safe* Implementierung im ersten Modus mit einem ausgeführten Task **K**, zwei ausgeführten Task **A** und drei aktiven DSP:

$$E_{SRS\text{-}FS1} = E_K + 2*E_A + 3*E_R$$

Im dritten Modus mit nur einem aktiven DSP, der alle drei Tasks ausführt, würde sich die Energie wie folgt berechnen:

$$E_{SRS\text{-}FS3} = E_K + E_A + E_D + E_R$$

und ist somit nur kleiner, wenn

$$E_{SRS\text{-}FS3} < E_{SRS\text{-}FS1}$$
$$E_K + E_A + E_D + E_R < E_K + 2*E_A + 3*E_R$$
$$E_D < E_A + 2*E_R$$

Dies gilt jedoch nur unter der Annahme, dass E_K beim Vergleich redundanter Werte und beim Akzeptanztest annähernd gleich bleibt. Für die *fail operational* Implementierung ist die Berechnung unter den gleichen Annahmen analog. Im ersten Modus erhalten wir:

$$E_{SRS\text{-}FO1} = E_K + 3*E_A + 4*E_R$$

Für den dritten Modus mit zwei aktiven DSP, einem Task **K**, einem Task **A** und zwei Task **D**:

$$E_{SRS\text{-}FS3} = E_K + E_A + 2*E_D + 2*E_R$$

Woraus folgt:

$$E_{SRS\text{-}FO3} < E_{SRS\text{-}FO1}$$
$$E_K + E_A + 2*E_D + 2*E_R < E_K + 3*E_A + 4*E_R$$
$$E_D < E_A + E_R$$

Was sogar noch ein wenig ungünstiger ist, als im *fail safe* Fall.

ZUSAMMENFASSUNG UND DISKUSSION

Der vorgeschlagene Ansatz, durch den Austausch von Messwerten Kosten bei Strom und Hardware einzusparen, ohne dabei Einbußen in der Fehlererkennungs- und -korrekturrate in Kauf zu nehmen, erscheint bei ersten Betrachtungen durchaus sinnvoll. Jedoch ist an einigen Stellen noch viel Arbeit nötig, um dies eindeutig zu klären. Dazu gehört als erstes die Fertigstellung der Tasks, um Machbarkeit, Stromverbrauch und Timing zu überprüfen. Weiterhin müssen die bisher nur am Rande betrachteten Sonderfälle wie (absichtlich) falsche Werte und fehlende Verkehrsteilnehmer eingehender untersucht werden. Als drittes werden echte Sensormessungen im Feld benötigt, um beispielsweise Einflüsse wie den Signal-Rausch-Abstand oder nicht-punktförmige reflektierende Objekte mit in die Betrachtungen und speziell den Akzeptanztest einfließen zu lassen.

Trotz dieser Lücken halten wir den Ansatz für wert, weiter verfolgt zu werden. Wir konnten bei unseren Literaturrecherchen keine ähnlichen Ansätze finden, bei denen Referenzwerte auf so einer niedrigen Systemebene ausgetauscht werden können wie hier. Und selbst wenn damit keine Einsparungen in Bezug auf Energie oder Hardware möglich sind, so stellt es doch ein zusätzliches Mittel dar, um die Robustheit des Systems deutlich zu erhöhen. Dies liegt im Wesentlichen an drei Punkten:

- Wir erhalten externe Referenzwerte, bei deren Erzeugung mit hoher Wahrscheinlichkeit nicht die gleichen Fehler passiert sein können, wie im eigenen Fahrzeug.
- Dadurch, dass sich die Software von Task **A** und **D** unterscheidet, aber gleiche Ergebnisse entstehen, erhalten wir eine Art N-Version-Programming, was die Maskierung von Fehlern deutlich erschwert.
- Dieser Unterschied in der Software wird höchstwahrscheinlich auch unterschiedliche Komponenten der Hardware ansprechen und dadurch eventuelle Fehler in diesen Teilen aktivieren, die sonst unentdeckt blieben. Damit erhöht sich die Beobachtbarkeit des Systems, wodurch Fehler schneller gefunden und entsprechende Gegenmaßnahmen, wie etwa Selbstreparatur, eingeleitet werden können.

DANKSAGUNG

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16EMO0177K gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

LITERATUR

[1] S. Inc., “Dual-core lockstep processors,” 03 2017. [Online]. Available: http://articles.sae.org/15319/

[2] L. D. Daniel Wanner, Annika Stensson Trigell and J. Jerrelind, “Survey on fault-tolerant vehicle design,” International Battery, Hybrid and Fuel Cell Electric Vehicle Symposium (EVS26), 05 2012.

[3] IHP, “Emphase project page,” 01 2017. [Online]. Available: http://www.emphase-projekt.de/

[4] Maciej Kucharski, Dietmar Kissinger and Herman Jalli Ng, “A Monostatic E-Band Radar Transceiver With a Tunable TX-to-RX Leakage Canceler for Automotive Applications” in Proc. 2018 IEEE MTT-S International Microwave Symposium (IMS), 2018

[5] Herman Jalli Ng, Maciej Kucharski, Wael Ahmad, and Dietmar Kissinger, “Multi-Purpose Fully Differential 61- and 122-GHz Radar Transceivers for Scalable MIMO Sensor Platforms,” IEEE J. Solid-State Circuits, vol. 52, no. 9, pp. 2242–2255, Sept 2017.

[6] B. Parhami, “Design of reliable software via general combination of n-version programming and acceptance testing,” in Software Reliability Engineering, 1996. Proceedings., Seventh International Symposium on, Oct 1996, pp. 104–109.

[7] Christopher Temple and Antonio Vilela, „Fehlertolerante Systeme im Fahrzeug – von fail-safe zu fail-operational". 07 2014. [Online]. Available: http://www.elektroniknet.de/elektronik-automotive/assistenzsysteme/fehlertolerante-systeme-im-fahrzeug-von-fail-safe-zu-fail-operational-110612-Seite-2.html

[8] Israel Koren and C. Mani Krishna, CHAPTER 5 - Software Fault Tolerance, In Fault-Tolerant Systems, Morgan Kaufmann, Burlington, 2007, Pages 147-191, ISBN 9780120885251