Technisch sichere Systeme in UAV

Informatik @ HAW HAMBURG

Anwendung 1
HAW-Hamburg
WS 2013/2014
03.12.2013

Mosawer Ahmad Nurzai
M-INF1

Agenda

1. Einführung
2. Motivation
3. Safety-Critical Computer Systems
4. Forschung
5. Fokus
6. Quellen
7. Fragen?

Agenda

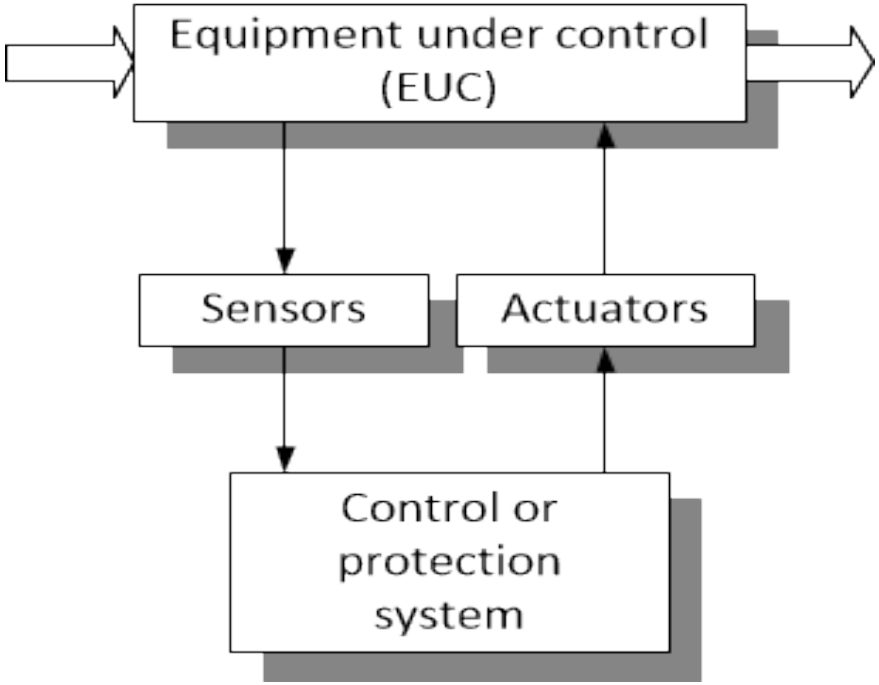
1. Einführung
2. Motivation
3. Safety-Critical Computer Systems
4. Forschung
5. Fokus
6. Quellen
7. Fragen?

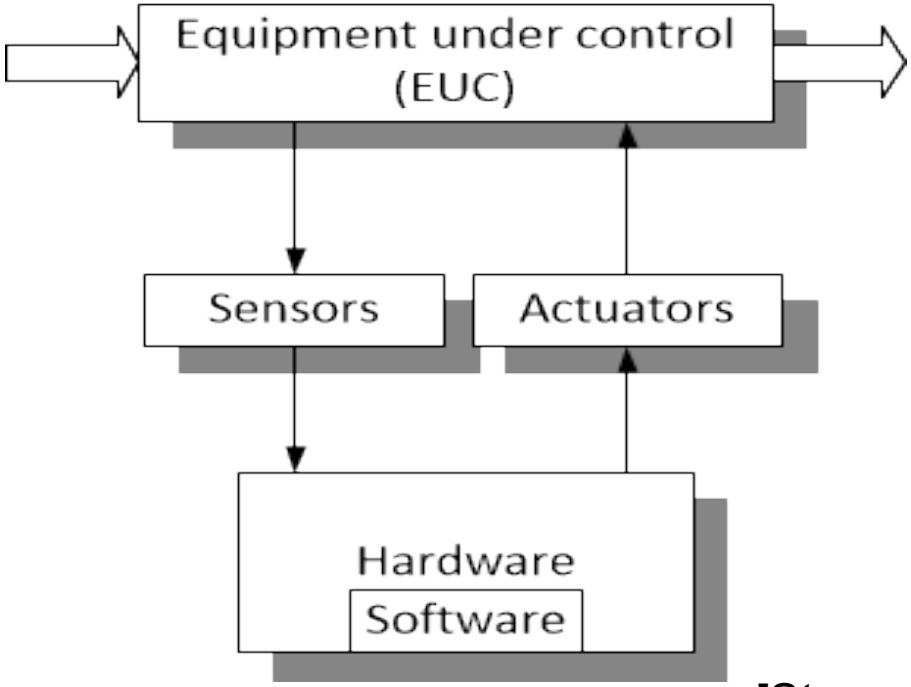
Einführung

- **UAS:**
  Unmanned Aerial System bestehend aus UAV (Unmanned Aerial Vehicle) und zusätzlichen Elementen, wie z.B. Bodenstation.
- **Safety**: (nach DIN EN 61508-4)
  „Freiheit von unvertretbaren Risiken.“
- **Safety-Critical/Related Computer System**: [Storey96]
  Ein System welches die Sicherheit der Ausstattung/Geräte und des Betriebs, im Sinne von Safety, garantiert.

Einführung

- **Funktionale Sicherheit**: (nach DIN EN 61508-4)
  „Teil der Gesamtsicherheit, bezogen auf das EUC [..], die von der korrekten Funktion des E/E/PE-sicherheitsbezogenen Systems, [..] zur Risikominderung abhängt.“





[Storey96]

Motivation

1. Einführung
2. Motivation
3. Safety-Critical Computer Systems
4. Forschung
5. Fokus
6. Quellen
7. Fragen?

Motivation

- Ariane 5 Jungfernflug – 04.06.1996

[Wey2013]

- Nutzung alter Software der Ariane 4
- Ausgelöst durch eine Exception, durch Überlauf bei einer Typumwandlung
  - Exception wurde nicht behandelt → Ausfall des Systems für Messungen

    → Reaktion Abschaltung der Systeme → Selbstzerstörung

[DseWiki2013]
[Lions96]

Motivation

- Nutzung von UAV im zivilen und staatlichen Raum [DeGarmo2004]
  - Landwirtschaft und Wildnis
  - Erdwissenschaft
  - Heimatschutz
  - Zivilbevölkerung / staatliche Interesse
  - Kommerziell

  → Verschiedene Anforderungen an technische Systeme für UAV entstehen
    - Safety
    - Funktionale Anforderung/Sicherheit

Safety-Critical Computer Systems

Informatik @ HAW HAMBURG

1. Einführung
2. Motivation & Historie
3. Safety-Critical Computer Systems
4. Forschung
5. Fokus
6. Quellen
7. Fragen?

Safety-Critical Computer Systems

Informatik @ HAW HAMBURG

- Ein System welches die Sicherheit der Ausstattung/Geräte und des Betriebs, im Sinne von Safety, garantiert. [Storey96]
- UAV ist ein Safety-Critical Computer System
- Ziel: Erlangen von Safety und Reliability (Zuverlässlichkeit)

  → Konflikt

  → Mittelmaß finden durch Hazard & Risiko Analyse

Safety-Critical Computer Systems: Hazard Analysen

- **Hazard**: tatsächliche oder potentielle Gefahr für Mensch oder Umgebung. [Storey96]
- **FMEA** (Failure modes and effects analysis)
- **HAZOP** (Hazard and operability studies)
- **ETA** (Event tree analysis)
- **FTA** (Fault tree analysis)

Safety-Critical Computer Systems: Hazard Analysen

Informatik @ HAW HAMBURG

HAZOP:

Item	Inter-connection	Attribute	Guide word	Cause	Consequence	Recommendation
1	Sensor output	Voltage	No	PSU, sensor or cable fault	Lack of sensor signal detected and system shuts down	
2			More	Sensor fault	Temperature reading too high – results in decrease in plant efficiency	Consider use of duplicate sensor
3			Less	Sensor mounted incorrectly or sensor failure	Temperature reading too low – could result in overheating and possible plant failure	As Above

[Storey96]

Fokus

1. Einführung
2. Motivation
3. Safety-Critical Computer Systems
4. Forschung
5. Fokus
6. Quellen
7. Fragen?

Forschung

Forsberg, H. & Manefjord, T. 2007. Derating concerns for microprocessors used in safety critical applications. Digital Avionics Systems Conference.

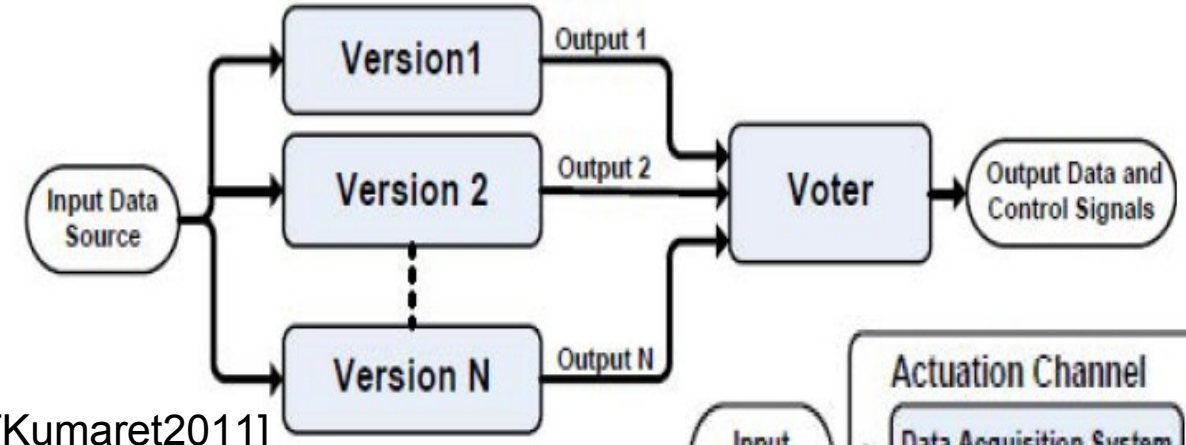
· Funktionieren einer Komponente in Betriebsgrenzen, um Ausfallrate zu reduzieren
  → Ziel Zuverlässlichkeit & Robustheit Komponente erhöhen
· Drosseln verschiedener (HW-)Parameter (Spannung, Frequenz...)

Forschung

Kumar, S. P. & Ramaiah, P. S & Khanaa, V. 2011. Architectural patterns to design software safety based safety-critical systems. SafeComp 2011

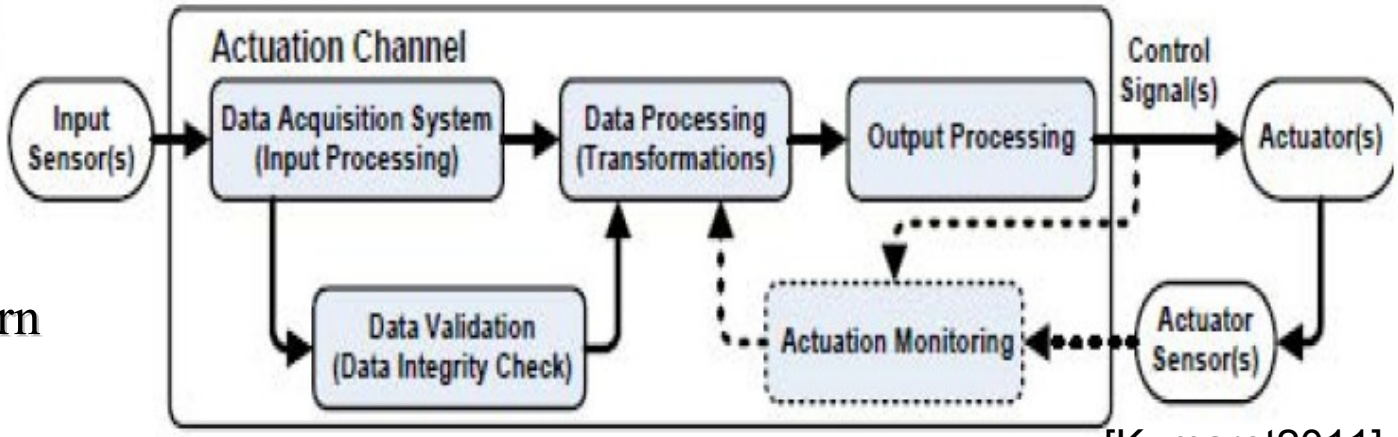
Forschung

· Nutzung verschiedener Design-Pattern für Safety-critical Systems



N-Version Programming Pattern

[Kumaret2011]



Protected Single Channel Pattern

[Kumaret2011]

· Anwendung: Vier Finger Roboter, um Motor und ergriffenes Objekt nicht zu beschädigen

Forschung

Uhlig, D. & Bhamidipati, K. & Neogi, N. 2006. Safety and Reliability Within UAV Construction. DASC 2006.

- Safety und Zuverlässigkeit in der UAV Konstruktion
- Nutzung von auf dem Markt erhältliche Standard Komponenten:
  - Cloud Cap Technology
  - Athena Controls
  - Micropilot

Piccolo SL
von Cloud Cap Technology [CloudCap2013]

Schritte um Safety und Zuverlässigkeit zu gewährleisten:

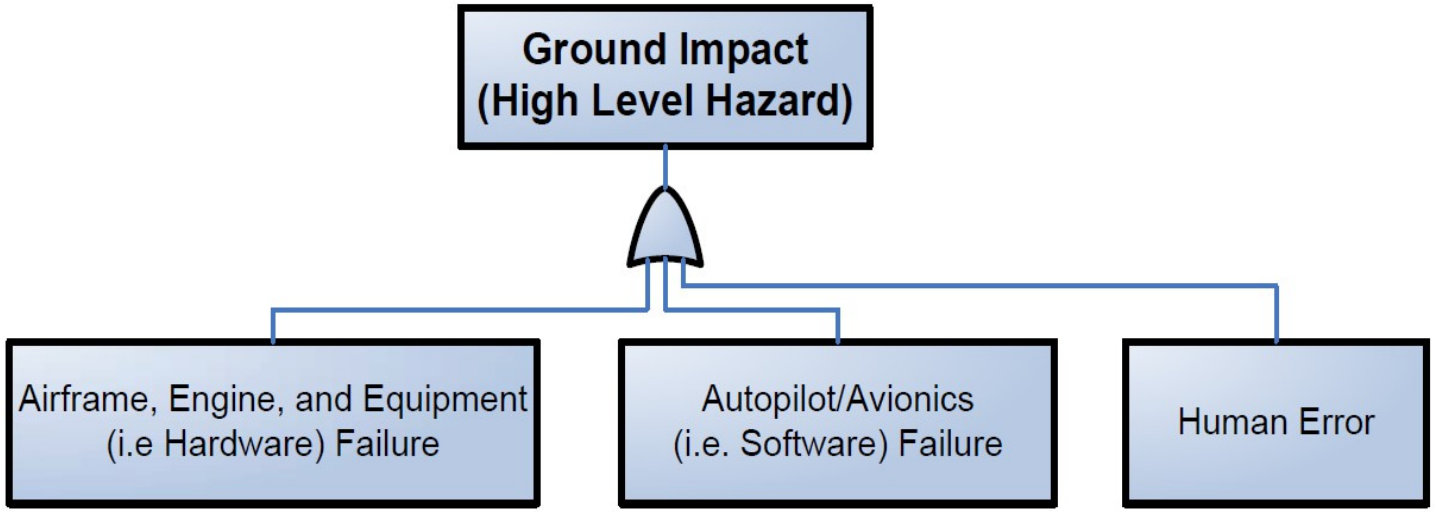
Critical Component or Stage	Operational Procedures Safeguards	Design and Setup Safeguards	Redundancy
Control Surfaces	Exercise Surfaces Pre-Flight	Secondary Fasteners on the Servo Extensions	Redundant Servo Technique
Backup Board	Check Connections	Vibration Isolated Mounting	Mux Fail to Pass Through 72 MHz
Piccolo Radio Link	Taxi Test Before Takeoff	Extensive Ground Range Checks	Backup Circuit Board
Airframe	Checklists to Verify Setup	Check C.G. and Propulsion System	None
Flight Tests	Detailed Flight Plan	Test Plan in HIL Environment	N/A

[Uhliget2006]

Forschung

Bhamidipati, K. 2007. Mitigating the UAV Ground Impact Hazard Using Fault-tree Analysis and a Fuel Consumption Model. University of Illinois at Urbana-Champaign

· Bodenstoß Hazard mildern
· Fault-tree Analysis zur Hazardbestimmung



[Bhpati2007]

Fokus

1. Einführung
2. Motivation
3. Safety-Critical Computer Systems
4. Forschung
5. Fokus
6. Quellen
7. Fragen?

Fokus

- Wie muss eine Sicherheitsarchitektur eines UAV konzipiert werden?
  - Aspekte der Safety
  - Bewertung und Auswahl technischer Komponenten
  - Welche Vor-/Nachprozesse notwendig?
    - Analysen, Testen
- Betrachtung des UAS (Unmanned Aerial System)?
- **Problem**:

  → Wenig Material zu UAV bzgl. Safety

  → Ausweichen Automobilindustrie (ISO 26262), kleine Arbeitsgruppen, NASA?

Quellen

1. Einführung
2. Motivation
3. Safety-Critical Computer Systems
4. Forschung
5. Fokus
6. Quellen
7. Fragen?

Quellen

- Literatur:
  - Storey, Neil: **Safety-Critical Computer Systems**. Addison Wesley Longman. 1996. 978-0201427875
  - Börcsök, Josef: **Funktionale Sicherheit: Grundzüge sicherheitstechnischer Systeme**. VDE Verlag GmbH. 2011. 978-3800733057
  - Newcome, Laurence R.: **Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles**. Pen & Sword Books Limited. 2004. 978-1844152018
- Konferenzen:
  - *UAV/S:*
    - ICUAS – International Conference on Unmanned Aircraft Systems
    - DASC – Digital Avionics Systems Conference
  - *Safety*:
    - SafeComp – The International Conference on Computer Safety, Reliability and Security
- Interne Arbeiten:
  - Richter, A. M., 2013. Konzept und Einführung von Safety-Analysen bei Mikrocontroller-basierten Anwendungen in UAVs. HAW Hamburg.

Fragen?

Informatik @ HAW HAMBURG

Vielen Dank für eure Aufmerksamkeit!

Auflistung der Quellen

- **[Storey96]**: Storey, Neil: Safety-Critical Computer Systems. Addison Wesley Longman. 1996. 978-0201427875
- **[Börcsök2011]**: Börcsök, Josef: Funktionale Sicherheit: Grundzüge sicherheitstechnischer Systeme. VDE Verlag GmbH. 2011. 978-3800733057
- **[NewCome2004]**: Newcome, Laurence R.: Unmanned Aviation: A Brief History of Unmanned Aerial Vehicles. Pen & Sword Books Limited. 2004. 978-1844152018
- **[DeGarmo2004]**: DeGarmo, M.T: Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace. 2004
- **[Kumaret2011]**: Kumar, S.P. & Ramaiah, P.S. & Khanaa, V. 2011 Architectural pattern to design software safety based safety-critical systems. SafeComp 2011
- **[Forsberget2007]**: Forsberg, H. & Manefjord, T. 2007. Derating concerns for microprocessors used in safety critical applications. Digital Avionics Systems Conference 2007
- **[Uhliget2006]**: Uhlig, D. & Bhamidipati, K. & Neogi, N. 2006. Safety and Reliability Within UAV Construction. DASC 2006
- **[Bhpati2007]**: Bhamidipati, K. 2007. Mitigating the UAV Ground Impact Hazard Using Fault-tree Analysis and a Fuel Consumption Model. University of Illinois at Urbana-Champaign
- **[Lions96]**: Lions, J.L. 1996. Ariane 5 Flight 501 Failure:http://www.di.unito.it/~damiani/ariane5rep.html
- **[DseWiki2013]**: Ariane5 Absturz. 2013: http://www.wikiservice.at/dse/wiki.cgi?Ariane5Absturz
- **[Wey2013]**: Weyand, C. 2003. Ariane 5 – Luftfahrt Berühmt-berüchtige Software-Fehler. Universität Koblenz – Landau:http://formal.iti.kit.edu/~beckert/teaching/Seminar-Softwarefehler-SS03/Folien/weyand.pdf
- **[Richter2013]**: Richter, A. M., 2013. Konzept und Einführung von Safety-Analysen bei Mikrocontroller-basierten Anwendungen in UAVs. HAW Hamburg.
- **[CloudCap2013]**: Cloud Cap Technology. Piccolo SL 2013: http://www.cloudcaptech.com/piccolo_system.shtm