Bedeutung und Korrektheit von C Programmen

Vorlesung vom 02.07.2008: C in sicherheitskritischen Systemen und der MISRA-Standard

Christoph Lüth & Lutz Schröder

SS 08

Fahrplan

- Software in sicherheitskritischen Systemen
- Normen und Standards
- MISRA-C

Sicherheitskritische Systeme

- Sicherheitskritisch: Ausfall bringt Gefahr für Leib und Leben
- Gesetzlich reguliert:
  - Maschinenrichtlinie (Direktive 2006/42/EC)
  - Luftfahrt (FAA, EASA)
  - Autoverkehr (Gesetzliche Regelungen)
  - Bahn (nationale Normen)

Normen und Standards

- Normen und Standards zur Einhaltung der Regularien
- Keine Vorschriften, keine Gesetzeskraft
- IEC DIN EN 61508 für Maschinenrichtlinie
  - "Functional safety of electrical / electronic / programmable electronic safety-related systems (E/E/PES)"
  - Risiko & Schadensanalyse ⟶ Safety Integrity Level 1 – 4
- Einhaltung der Norm wird zertifiziert

Zertifizierung

- Zertifizierungsbehörde als drittes Auge
- Prüft Einhaltung von Prozeduren
- Prüft Adäquatheit von Methoden
- Garantiert keine Korrektheit

IEC DIN EN 61508

Table A. 3a — Recommendations for specific programming languages

	Technique/Measure*	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
1	ADA	C1	HR	HR	R	R
2	ADA with subset	C1	HR	HR	HR	HR
3	MODULA-2	C1	HR	HR	R	R
4	MODULA -2 with subset	C1	HR	HR	HR	HR
5	PASCAL	C1	HR	HR	R	R
6	PASCAL with subset	C1	HR	HR	HR	HR
7	FORTRAN 77	C1	R	R	R	R
8	FORTRAN 77 with subset	C1	HR	HR	HR	HR
9	C	C1	R	-	NR	NR
10	C with subset and coding standard, and use of static analysis tools	C1	HR	HR	HR	HR
11	PL/M	C1	R	-	NR	NR
12	PLM with subset and coding standard	C1	HR	R	R	R
13	Assembler	C1	R	R	-	-
14	Assembler with subset and coding standard	C1	R	R	R	R

IEC DIN EN 61508

6	Dynamic reconfiguration	--- / °	NR / --	NR / --	NR / --
7a	Structured methods including for example, JSD, MASCOT, SADT and Yourdon.	HR / ++	HR / ++	HR / ++	HR / ++
7b	Semi-formal methods	R / +	R / +	HR / ++	HR / ++
7c	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	--- / °	R / +	R / +	HR / ++
8	Computer-aided specification tools	R / +	R / +	HR / ++	HR / ++

MISRA-Standard

- Beispiel für eine Codierrichtlinie
- Erste Version 1998, letzte Auflage 2004
- Kostenpflichtig (£40,-/£10,-)
- Regeln: 121 verbindlich (required), 20 empfohlen (advisory)

Zusammenfassung

- Sicherheitskritische Systeme: reguliert durch Normen und Standards
- C nur mit Richtlinie und Werkzeugunterstützung
- MISRA-C: Beispiel für anerkannte Richtlinie