MISRA-Konformität von ASCET-Autocode

Von Mathias Mackh, ETAS

Unterstützung der Automobilindustrie durch Entwicklung und Anwendung von sicherer und zuverlässiger Software

Durch den steigenden Anteil von Elektronik und Software im Fahrzeug hat die Softwarequalität maßgeblichen Einfluss auf die Qualität des Endprodukts und trägt somit entscheidend zum Geschäftserfolg bei. Daher fordern immer mehr Automobilhersteller standardisierte, nachvollziehbare Prüfkriterien für den gesamten Code, wie z. B. den Nachweis der MISRA-Konformität.

Das MISRA-Konsortium

Das MISRA-Konsortium (Motor and Industry Software Reliability Association) wurde von Automobilzulieferern und Herstellern mit dem Ziel gegründet, die Automobilindustrie in der Anwendung und Entwicklung von sicherer und zuverlässiger Software im Automobil zu unterstützen.

Die Notwendigkeit dazu ergibt sich aus der in der Automobilindustrie üblichen Verwendung der Programmiersprache C und deren teilweise lückenhafter Spezifikation. Diese Lücken führen häufig zu einem Fehlverhalten des Gesamtsystems, obwohl der implementierte C-Code durchaus der C-Spezifikation genügt (s. Beispiel unten).

Beispiel zur Abhängigkeit einer C-codierten Rechenoperation von der Zielplattform.

```
short x, y;
long z; x = 30000; y = 40000;
z = x+y;

z-Wert in einem 16-Bit-System:
x+y = (30000+40000) % 32768 = 4464

z-Wert in einem 32-Bit-System:
x+y = (30000+40000) % 2147483648 = 70000
```

Werden zwei Zahlen addiert, so kann auf einem 32-Bit-Zielsystem ein korrekter Wert errechnet werden, auf einem 16-Bit-System jedoch ein Überlauf entstehen, der nicht erkannt wird. Das Ergebnis entspricht dann nicht dem erwarteten Wert.

Wesentliche Gründe für eine fehleranfällige C-Code Programmierung sind:

- eine unterschiedliche Interpretation der Sprache durch den Compiler,
- Plattformabhängigkeiten,
- die Mehrdeutigkeit der Sprache,
- unverständliche, komplexe Konstrukte sowie
- Tippfehler.

Um diese Fehlerquellen im Quellcode möglichst auszuschließen, definierte das MISRA-Konsortium eine Empfehlung mit 141 Regeln zu neun Themengebieten, die als MISRA-C:2004 (MISRA-C 2.0) Standard bezeichnet wird.
Diese Regeln werden in zwei Gütestufen unterteilt:

- benötigte Regeln, die vom Programmierer verpflichtend einzuhalten sind und
- empfohlene Regeln, die im Normalfall eingehalten werden sollen.

Prüfung der MISRA-Konformität von ASCET-Autocode

Um die Integratoren von Code, der von ASCET automatisch generiert wird, bei der Absicherung der Gesamtsoftware zu unterstützen, wurde der ASCET-Codegenerator auf MISRA-Konformität hin untersucht und weiterentwickelt. Die Konformität wurde durch eine Matrix dokumentiert, welche die Einhaltung der MISRA-Regeln und begründete Abweichungen darstellt. Die Konformitätsuntersuchung fokussiert auf Aussagen zu ASCET-Autocode für Produktivsysteme mit und ohne Einbindung von Betriebssystemen.

Die Einhaltung von Regeln, welche die Code-Syntax betreffen, können über statische Code-Analysen im Entwicklungsprozess überprüft werden. Regeln, deren Einhaltung im Zuge der Implementierung nicht von ASCET beeinflusst werden kann, wie z. B. solche, die von der Compilerauswahl abhängen, haben keinen Einfluss auf die Qualifizierung des ASCET-Autocodes. Entsprechende Regeln wurden in der Konformitätsbetrachtung von ASCET-Autocode als „nicht anwendbar" bezeichnet. Code, der vom Anwender manuell hinzugefügt wird, unterliegt ebenfalls nicht der Kontrolle von ASCET und muss fallweise geprüft werden.

Als Referenz zur Prüfung der MISRA-Konformität setzt ETAS zur statischen Analyse des Sourcecodes QA-C von Programm Research ein. Die vorliegenden Auswertungen von ASCET V5.2 wurden mit QA-C V6.2.1 und dem Add-On zur MISRA-Überprüfung M2CM Version 1.5 durchgeführt.

Eine besondere Stellung nimmt der Mechanismus zur Adressberechnung für die ASAM MCD 2MC-Beschreibungsdateien ein. ASCET stellt sicher, dass die Maßnahmen zur Adressberechnung keinerlei Einfluss auf das Zielsystem haben. Dies ist in der Konformitätsbeschreibung entsprechend dokumentiert.

Darstellung der Einhaltung der MISRA-Regeln und begründeten Abweichungen.

Regel	konform	benutzerabhängig	nicht konform	nicht anwendbar
Regel 1.1		X		
Regel 1.2		X		
Regel 1.3				X
Regel 1.4				X
Regel 1.5				X
Regel 2.1	X			
Regel 2.2	X			
Regel 2.3	X			
Regel 2.4	X			
Regel 3.1			X	
Regel 3.2	X			
Regel 3.3				X

Eine weitere Kategorie stellen Regelverletzungen dar, die aufgrund der Konfiguration oder des Modelldesigns entstehen können. Da ASCET als Softwarewerkzeug nicht beurteilen kann, ob die Regelverletzung beabsichtigt ist oder nicht, wurde die Klasse der „benutzerabhängigen" Regeln eingeführt. Um Anwender bei einer MISRA-konformen Modellierung zu unterstützen, stellt ETAS entsprechende Modellierungsrichtlinien bereit.

Konformitätserfüllung

Die Implementierung des ASCET-Codegenerators stellt sicher, dass 59 % aller MISRA-Regeln grundsätzlich erfüllt werden. Die Konformität von ASCET-Autocode ist bis zu 31 % von der Modellierung und den Einstellungen in ASCET abhängig. Weitere 4 % können von ASCET nicht verletzt werden, da sie die C-Codegenerierung nicht betreffen. Hier muss der Anwender anderweitige Maßnahmen ergreifen, um die Konformität sicherzustellen. Somit kann mit ASCET generierter Code bei entsprechender Beachtung der Richtlinien 90 % aller Regeln erfüllen. Aufgrund der Tatsache, dass Regelverletzungen MISRA-konform dokumentiert sind, kann bei der ASCET-Codegenerierung 100 % MISRA-Konformität eingehalten werden.

Sicherstellen der Konformität für die Zukunft

Um die Konformität von ASCET-generiertem Code bezogen auf die MISRA-Regeln sicherzustellen, wird bei allen Weiterentwicklungen des Codegenerators deren MISRA-Relevanz überprüft. Zum Test werden geeignete Modelle erzeugt. Um die Codegenerierung kontinuierlich zu verbessern, werden Referenzmodelle aus der Praxis eingesetzt. Die Konformitätsmatrix für den ASCET-Codegenerator und die Modellierungsrichtlinien werden kontinuierlich überarbeitet sind seit ASCET V5.1.3 bei ETAS erhältlich.

MISRA für ASCET-Modelle

In der Zukunft wird die modellbasierte Software-Entwicklung für Steuergeräte immer mehr an Bedeutung gewinnen. Wohl können MISRA-Regeln prinzipbedingt durch nichtkonforme Softwaremodelle und -designs verletzt werden. Allerdings werden Regeln, die sich auf Fehleingaben bei der manuellen Codierung beziehen, durch die automatische Codegenerierung niemals verletzt. Implementierungsbedingte Regelverletzungen wiederum können dann nicht vermieden werden, wenn die Implementierung durch die Zielplattform vorgegeben ist. Das MISRA-Konsortium hat Arbeitsgruppen eingerichtet, welche die Sonderfälle, die im Zusammenhang mit der automatischen Codegenerierung auftreten, genauer untersuchen. Im Rahmen dieser Arbeitsgruppen wird in Zusammenarbeit mit ETAS ein Regelwerk erarbeitet, das die Anwendbarkeit der MISRA-Regeln bei der modellbasierten automatischen Codegenerierung mit ASCET standardisiert.

Literaturhinweise:

MISRA-C:2004 Guidelines for the Use of the C Language in Critical Systems, 2004, Mira Ltd. www.misra.org.uk

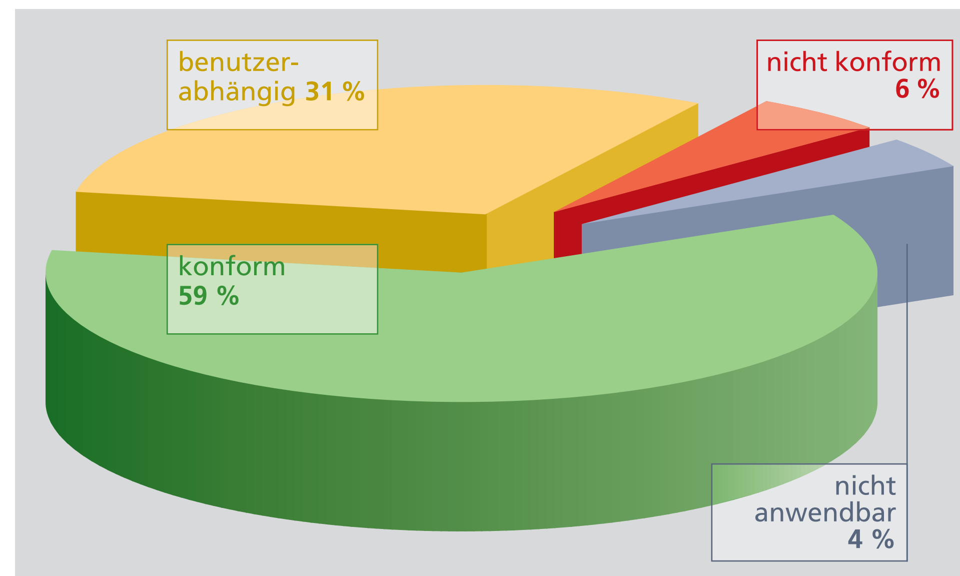
Emerging Software Best Practice and how to be Compliant, Roger S. Rivett (Rover Group Ltd.). Proceedings of the 6th International EAEC Congress, July 97. www.misra.org.uk

Definition und Dokumentation von Designregeln für ASCET zur Generierung von MISRA-C konformem Code, ETAS GmbH, A. Rolew, 2006.

Styleguide für ASCET-Modelle zur Generierung von MISRA-C konformem Code, ETAS GmbH, A. Rolew, M. Mackh, 2006.

ASCET V5.1.3 MISRA-C:2004, Compliance Document, ETAS GmbH, 2006.

QA-C: Users Guide, Programming Research Ltd. www.qa-systems.de



Konformität von ASCET generiertem Code bezogen auf die MISRA-Regeln.