

# MISRA von Anfang an

Von Carsten Neumann, Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS

Automatisierte Modell-Reviews

sichern MISRA-Konformität auf ETAS ASCET-Modellebene

Der Softwaredienstleister Match Technologies hat für ASCET eine innovative automatisierte Review-Lösung für die formale Verifikation der MISRA-Richtlinien auf Modellebene entwickelt: MISRA CHECK 4 ASCET ermöglicht dem ASCET-Entwickler die frühzeitige Richtlinienprüfung mit integriertem MISRA-Prüfkatalog.

**Gerade bei immer** komplexeren Projekten und globaler Entwicklungszusammenarbeit ist das Risiko bei der Modellierung hoch, dass sich Fehler einschleichen und so nichtkonforme Softwaredesigns und -modelle entstehen. Code-Checker sind prozessbedingt erst spät im Einsatz, erschweren die Traceability und erfordern hohe Roundtrip-Zeiten für Korrekturen. Die Qualität der Software kann jedoch bereits in frühen Entwurfsphasen auf Modellebene durch konsequentes Frontloading abgesichert werden.

## MISRA-Konformität im Modell durch MISRA CHECK 4 ASCET

MISRA hat sich als allgemeingültiger Standard bei der Entwicklung zuverlässiger Software für Automotive-Steuergeräte etabliert. ETAS hat MISRA-Codierichtlinien erarbeitet, welche die Anwendbarkeit der MISRA-Regeln bei der modellbasierten automatischen Codegenerierung mit ASCET standardisieren. Match Technologies hat diese in ausführbare Regeln überführt und bietet sie als integrierte Lösung an. Der Entwickler kann MISRA CHECK 4 ASCET problemlos direkt in ASCET integrieren – sei es direkt am Arbeitsplatz oder als

Prüfserver im Hintergrund. Hierdurch lässt sich die Einhaltung der die Code-Syntax betreffenden MISRA-Regeln vor den statischen Code-Analysen bereits im Modell überprüfen und so Fehler frühzeitig korrigieren.

## Formale Verifikation mit MISRA CHECK 4 ASCET

Mit dem neuen ASCET-Release 6.1.3 können Software-Modellkomponenten auf physikalischer Ebene anhand von Blockdiagrammen und Zustandsautomaten noch effizienter spezifiziert und gleichzeitig mit dem MISRA CHECK 4 ASCET überprüft werden. Aktuell geltende MISRA-Richtlinien sind im MISRA-C:2004 Compliance Guide für die jeweils eingesetzte ASCET-Version verfügbar.

## Vorteile der automatisierten MISRA-Prüfung

Mit einem Mausklick werden alle Entwurfsregeln, Modellierungsrichtlinien, Codekonventionen und Qualitätsmetriken bereits im Modell geprüft. Dabei werden sowohl Anforderungen nach dem MISRA-C:2004 Compliance Guide von ETAS als auch unternehmensspezifische Richtlinien geprüft. Die Traceability-Ansicht (siehe Abbildung) zeigt die Fehlerstelle

direkt auf, erstellt ein Traceability-Protokoll zur Dokumentation und kann zusätzlich durch den Anwender kommentiert oder in begründeten Ausnahmefällen verworfen werden. Gegenüber herkömmlichen Code-Checkern ergeben sich durch Modell-Reviews zusätzliche Möglichkeiten zur Prüfung von:

- konformen Codegenerator-Optionen für effizienten Code
- einheitlichen Programmeinstellungen bei verteilter Projektentwicklung
- Modelllayout- und Design-Konventionen
- Namenskonventionen (Semantikprüfung gegen Glossar)
- Codierregeln (Datentypen, Wertebereiche, Initialisierungen)
- Strukturregeln für Architekturen und Verhaltensmodelle
- Konsistenz gegenüber relevanten MS Office®-Dokumenten

Mit diesen Möglichkeiten können qualitätssichernde Maßnahmen, wie Inspektionen und Reviews, genauer auf die potentiell kritischen Stellen eines Modellentwurfs gerichtet werden, die sonst unter Umständen Zuverlässigkeits- oder Wartbarkeitsprobleme verursachen können.

# Checklist

Mit einem Klick wurde die Verletzung der MISRA-Regel „Floating-point expressions shall not be tested for equality or inequality“ erkannt.

## Ziel erreicht

Mit dem MISRA CHECK 4 ASCET kann die Erfüllung der MISRA-Anforderungen präziser nachgewiesen werden. Auch Problemsituationen im Verbund mit anderen elektronischen Systemen oder Lieferanten werden schneller erkannt. Schließlich verbessert sich die Datenqualität bei allen Stakeholdern, da nicht nur stichprobenhaft, sondern durch die automatisierte Verifikation nahezu vollständig geprüft wird – einschließlich übergreifender Konsistenzbeziehungen der Modelle mit geltenden Dokumenten. Weitere Infos zu MISRA CHECK 4 ASCET finden Sie unter [www.match-technologies.com](http://www.match-technologies.com).

## HERAUSFORDERUNG

Mit zunehmend komplexen Modellierungsumgebungen wird die formale MISRA-Prüfung von Daten und Modellen zur zeitaufwändigen Herausforderung.

## LÖSUNG

Automatische Modell-Reviews mit MISRA CHECK 4 ASCET unterstützen die frühzeitige Absicherung der MISRA-Konformität auf Modellebene und sorgen so für weniger Beanstandungen bei den nachfolgenden Code-Checks und Reviews.

## NUTZEN

Implementierungsorientierte Modell-Reviews bringen insbesondere bei komplexen Modellen einen Zeitgewinn durch schnelleren Roundtrip (Modell/Code) und die leichtere Wartbarkeit – auch durch Dritte. Erfahrungswerte von Experten können als (Best Practices) Richtlinien weitergegeben werden, wodurch schließlich die Effizienz und Qualität der generierten Software ansteigt.