

2013년 06월 27일 10시 30분 갱신

MISRA 차량 소프트웨어 인터뷰:

차량 소프트웨어의 새로운 가이드라인 “MISRA C ADC”, ISO26262 대응과 품질 확보를 동시 실현

글: 朴尚洙 | 출처: MONOist

번역: 이채원 · 카이젠컨설팅

일본 자동차 공업회와 유럽의 자동차 업계 단체인 MISRA 는 자동차 전용 기능안전규격인 ISO 26262 대응과 차량 소프트웨어의 신뢰성과 품질의 확보를 양립시키는 것을 목적으로 새로운 코딩 가이드라인이 되는 “MISRA C ADC”를 책정했다. MISRA 의 담당자에게 책정의 배경과 목적에 대해서 물었다.

자동차 전용 기능안전규격인 ISO 26262 가 정식 발행하고 1 년 반 이상이 경과했다. ISO 26262 대응으로 선행한 유럽의 자동차 제조회사나 공급자에 이어, 일본의 자동차 업계도 대응을 서두르고 있다.

ISO 26262 에서는 차량 소프트웨어의 신뢰성과 품질을 확보 가능하도록 코딩 가이드라인의 적용을 요구하고 있다. 차량 소프트웨어의 코딩 가이드라인으로서 널리 알려져 있는 것은 유럽의 자동차 업계 단체인 MISRA (Motor Industry Software Reliability Association)가 책정한 C 언어를 사용하여 프로그래밍 시에 이용하는 MISRA C 이다. MISRA C 는 유럽에서 책정된 가이드라인이지만 일본에서도 넓게 이용되고 있다.

일본 자동차 공업회와 MISRA 는 2013 년 3 월, ISO 26262 에 대응한 차량 소프트웨어의 개발 프로세스 구축에 최적화한 MISRA C 의 확장 가이드라인 “MISRA C ADC”를 책정했다. MISRA C ADC 의 책정에 참여한 영국의 자동차 기술 연구 기업 MIRA 의 기능안전 General manager 를 맡고 있는 David Ward 씨에게 확장 규격을 책정한 배경과 목적에 대해서 물었다.

MONOist MISRA C ADC란 어떠한 가이드라인 입니까?

David Ward MISRA C는 C언어를 사용한 차량 소프트웨어의 프로그래밍에 사용하는 코딩 가이드라인

2013년 06월 27일 10시 30분 갱신

입니다. 2004년에 발행된 MISRA C: 2004는 자동차뿐만 아니라 항공 우주, 군사, 의료, 프로세스 제어 등의 다양한 분야에서 이용되고 있습니다.

MISRA C에는 가이드라인에 적합하지 않은 코딩을 실시할 때의 “제어 편차 절차(Deviation Procedure)”가 존재합니다. 자동차 전장화의 추진에 따라 1개의 차량에 탑재되는 차량 소프트웨어의 규모는 급증하고 보다 복잡해지고 있기 때문에 제어 편차 시의 절차를 활용해야 하는 경우가 늘고 있습니다.

또 차량 소프트웨어의 개발 프로세스에 큰 변화를 불러일으킨 ISO 26262의 등장에 따라 편차 절차의 이용 빈도는 높아지고 있습니다. MISRA C의 편차 절차를 올바르게 운용하기 위한 가이드라인으로서 책정한 것이 MISRA C ADC (Approved Deviation Compliance)입니다.

MONOist MISRA C ADC를 일본 자동차 공업회와 공동으로 책정한 이유에 대해서 알고 싶습니다.

David Ward 일본의 자동차 업계에서는 차량 소프트웨어 개발에 MISRA C가 넓게 이용되고 있습니다. ISO 26262에 준수한 차량 소프트웨어의 개발 프로세스를 구축 시에 MISRA C를 활용하여 그 품질과 안정성을 향상 가능하도록 하여 요구사항을 만족하도록 해야겠다는 요구가 있었습니다.

하지만 차량 소프트웨어의 개발 프로세스에서 ISO 26262 대응을 추진하면 MISRA C의 제어 편차 절차를 많이 적용할 경우가 생깁니다. 제어 편차 처리라는 것은 적절한 조건으로 사용하지 않으면 차량 소프트웨어의 품질과 안정성을 향상시킬 수 없습니다. ISO 26262 대응과 MISRA C에 의한 차량 소프트웨어의 품질과 안정성의 향상을 양립할 수 있도록 제어 편차 처리를 사용하여 안전 상황 등을 명시할 필요가 있는 것입니다.

MONOist ISO 26262도 MISRA C도 유럽에서 책정되었습니다. MISRA C ADC에 대해서도 유럽에서 독자적으로 책정할 예정은 없었습니까?

David Ward 유럽의 자동차 제조회사나 공급자는 현행 MISRA C: 2004만으로도 ISO 26262의 준수는 충분히 가능하다고 생각하고 있는 것 같습니다. 이것은 유럽의 자동차 업계가 ISO 26262의 정식 발행 전부터 개발 프로세스의 기능안전규격의 도입에 적극적으로 대응하고 있기 때문에 MISRA C의 편차 절차를 사용할 때의 기준은 명확하게 이해하고 있습니다.

한편 ISO 26262 대응이 유럽보다 늦어지고 있는 일본의 자동차 업계에 대해서 MISRA C의 편차 제어를 적절히 사용하기 위한 지식이나 노하우는 부족합니다. 하지만 MISRA C ADC를 사용하면 그 문제를 해결할 수 있을 겁니다.

MONOist 그럼 MISRA C ADC는 일본의 자동차 업계에서만 운용되는 것입니까?

David Ward 차량 소프트웨어 개발의 Supply chain은 유럽이나 일본, 북미를 불문하고 중국, 아시아,

2013년 06월 27일 10시 30분 갱신

인도 등의 신흥국에도 넓어지고 있습니다. 이들 신흥국에서도 일본의 자동차 업계와 같이 MISRA C의 편차 제어 절차에 관한 과제를 안고 있어서 MISRA C ADC의 운용을 권장하고 있습니다. 최근에는 차량 소프트웨어의 개발을 신흥국 공급자에게 아웃소싱하고 있는 경향을 보면 많은 유럽의 자동차 업계도 MISRA C ADC를 운용할 필요가 있을 것입니다.

MONOist MISRA에서는 2013년 3월에 MISRA C의 최신 버전인 MISRA C: 2012를 책정했습니다. MISRA C: 2012와 MISRA C ADC에는 어떠한 관계가 있습니까?

David Ward 2004년에 발행한 MISRA C: 2004는 1990년에 발행된 C언어의 규격서 “C90”에 대응하고 있습니다. 이에 반해 MISRA C: 2012는 1999년에 발행된 것 보다 새로운 C언어의 규격서 “C99”에 대응합니다. 이 밖에 몇 가지 추가된 규칙이나 가이드라인의 이해를 향상시키기 위한 폭 넓은 개선도 이루어졌습니다.

MISRA C ADC는 MISRA C: 2004의 확장 가이드라인이기 때문에 MISRA C: 2012와 비교하여 운용하는 것은 불가능 합니다. 하지만 현재 검토중인 MISRA C ADC의 추가 문서에 의해 MISRA C: 2012에도 대응할 예정입니다.

원문 | <http://monoist.atmarkit.co.jp/mn/articles/1306/27/news034.html>