Chapter 02

자동차 사이버 보안 및 보안 코딩 기술 동향

장대원_MDS인텔리전스 차장

I. 서론

커넥티드카, 자율주행, 사물인터넷(IoT), 가상현실(VR), 증강현실(AR) 등 새로운 융합 기술이 차량에 적용되면서 자동차 시장에 급진적인 변화가 계속되고 있다. 이에 따른 차량 내 전기전자시스템 역시도 비약적으로 증가하고 있으며, 이와 함께 차량에 대한 해킹 위협도 지속적으로 늘어나고 있다.

2015년 “지프 체로키”의 전자제어장치(Electronic Control Unit: ECU)에 대한 해킹 시연은 사이버 공격으로 차량의 직접적인 제어가 가능함을 확인시켜준 사건이었고, 2022년 초 독일의 10대 소년 데이비드 콜롬보(David Colombo)의 “테슬라 전기차” 25대 해킹 사건은 자동차 키가 없어도 원격으로 시동을 걸 수 있을 정도의 해킹이 가능함을 보여주었다[1]. 또한, 2025년까지 차량 약 4억 7,000만 대 가량이 전산화된 데이터베이스에 연결될 것으로 예상되며, 차량 해킹을 이용한 원격 제어, 차량 정보 탈취 등 각종 사이버 범죄가 늘어날 것으로 분석하고 있다.

이에 따라 차량에 대한 악의적인 사이버 보안 공격에 대한 피해와 손실에 대한 대응도 함께 요구되고 있다. 유엔 유럽경제위원회(UNECE)는 차량 사이버보안의 국제기준을 마련하기 위해 2016년부터 준비한 자동차 사이버보안 국제기준(UN Regulation No.155)을 2020년 6월 채택하고 2021년 1월 발효했다. 이 기준에 따라 2022년 7월부터 전자제어장치(Electronic Control Unit: ECU)를 장착하는 신차는 자동차 사이버보안 국제기준 인증을 받아야 한다. 이는 계속적으로 확대되며 2024년 7월에는 모든 차량으로 적용된다[2],[3].

국내에서는 이러한 사이버 보안 요구에 대한 대응을 위해 국토부가 2020년 12월 자동차

* 본 내용은 장대원(☎ 031-627-3135, daewon@hancomit.com)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

사이버 보안 가이드라인을 발행하여 UN Regulation No.155을 바탕으로 제정될 국내 기준에 사전 대비할 수 있도록 대응하고 있다. 국내 법 체계에서 사이버 보안을 적용하기 위해서는 국내의 자기인증제도와 UN 사이버 보안 기준인 형식승인제도 간을 차이를 확인하고 이를 효과적이고 올바르게 적용할 수 있는 국내기준 제정을 위한 시간이 필요하다[4]. 차량 제조사에서도 사이버 보안을 대응하기 위해 세부적인 요구사항을 체계적으로 구축해 나아가고 있으며, 보안 코딩과 관련해서는 자체적으로 적용 가능한 보안 코딩 가이드를 제작하여 협력사 및 관련 업체에 가이드 준수를 요구하고 있다.

본 고에서는 사용자가 UN Regulation No.155 준수를 위한 보안 코딩 가이드 선택 및 적용에 관한 정보를 자세히 제시하고 있다. UN Regulation No.155를 통해 보안 코딩 가이드의 필요성에 대해 구체적으로 기술하고, ISO/SAE 21434에서 언급한 보안 코딩 가이드에 대한 대응방안과 이를 준수하기 위해 제시된 2개의 보안 코딩 가이드를 서로 비교한다. 이를 통해 보안 코딩 가이드의 한계에 대해 올바르게 이해하고 현업에서 보안 코딩 가이드를 활용할 수 있도록 가이드 한다.

II. UNECE 사이버 보안 정의

UN Regulation No.155는 Cyber Security(사이버 보안)와 Cyber Security Management System(사이버 보안 관리 시스템)에 대해 다음과 같이 정의한다[3].

> 2.2 “Cyber Security(사이버 보안)”
> 차량 및 그 기능이 전기 또는 전자 부품에 대한 사이버 위협으로부터 보호되는 상태
>
> 2.3 “Cyber Security Management System(사이버 보안 관리 시스템)”
> 차량에 대한 사이버 위협과 관련된 위험을 처리하고 사이버 공격으로부터 차량을 보호하기 위해 조직 프로세스, 책임 및 거버넌스를 정의하는 체계적인 위험 기반 접근 방식
>
> 〈인용〉 UNECE, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, 2021.

Cyber Security Management System(CSMS)은 악의적인 사이버 위협으로부터 보호되는 상태를 체계적으로 대응하기 위해 차량의 전기/전자 부품에 대한 보안을 요구한다. 뿐만

아니라, 사이버 보안을 위한 효과적인 프로세스 구축과 책임 그리고 추후 관리까지 전주기 대응을 필요로 한다.

일반적으로 회사 내 S/W 품질팀이나 Q/A 등의 업무를 병행하는 것과 같은 개인이나 팀 단위의 한정적인 대응으로는 사이버 보안 준비 및 대응 범위의 한계로 인해 효과적인 결과를 기대하기 어렵다. 그렇기 때문에 조직 차원의 계획 및 프로세스 구축 그리고 이를 수행하기 위한 세부적인 실행방안을 수립해야 한다. 이를 구체화하기 위해 사내 사이버 보안 대응을 위한 차량 개발부터 판매 이후 보안 위협 대응과 관리까지 전반적인 통제가 필요하며, 이를 위한 체계적인 보안조직 관리부터 프로세스까지 갖춰야 한다.

다음은 CSMS 문서 내용 중 구축해야 할 다양한 사이버보안 프로세스 일부 내용이다[3].

- Vehicle type의 사이버 보안 테스트에 사용되는 프로세스
- Risk assessment가 최신 상태로 유지되도록 하는데 사용되는 프로세스
- Cyber attacks, Cyber threats, vehicle types에 대한 vulnerabilities 모니터링, 탐지, 대응 프로세스

위와 같이 여러 프로세스는 차량 개발, 생산 및 판매 이후까지 세부적인 계획을 반영하기 위해 사이버 보안 테스트 절차와 최신의 위험 평가 상태 관리 그리고 취약성 모니터링, 탐지, 대응에 이르기까지 체계적인 프로세스 구축을 명시한다. 또한, 사이버 위협에 체계적으로 대응할 수 있는 다양한 프로세스 이외에도 사이버 보안을 위한 보안 코딩 연관 내용도 찾아볼 수 있다.

III. 보안 코딩 가이드와 ISO/SAE 21434

UN Regulation No.155은 기본적인 개념 및 표준화된 절차 위주의 내용으로 구성되므로 현업에서 사이버 보안을 위해 적용해야 할 보안 코딩 적용사항은 문서 내 언급된 참조 내용을 통해 확인해야 한다. UN Regulation No.155의 5절 Approval을 통해 보안 코딩 관련 내용을 확인해 보면 다음과 같다[3].

5.3절 승인 당국(Approval Authorities)은 제조업체가 이 규정에서 다루는 사이버 보안 측면을 적절하게 관리하기 위해 만족스러운 조치와 절차를 마련했는지 확인하지 않고 형식 승인을 부여해서는 안 된다고 설명한다. 이러한 조치와 절차의 세부 내용을 5.3.1 (a), (b)를 통해 살펴보면, 다음과 같다.

(a) 적합한 사이버 보안 기술과 특정 자동차 위험 평가 지식[1]을 갖춘 역량 있는 인원

(b) 규정에 따른 일관된 평가를 위한 시행 절차

[1] E.g. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434

〈인용〉 UNECE, Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, 2021.

위의 주요 내용은 적합한 사이버 보안 기술과 사이버 보안 세부 활동 수립 시 참고할 수 있는 주요 국제표준으로 ISO/SAE 21434를 권장하고 있다는 점이며, ISO/SAE 21434를 통해 보안 코딩 대응방안을 마련하고 적용하는 것이 가능하다는 것이다. 때문에 사용자는 ISO/SAE 21434를 활용하여 보안 코딩에 대한 세부적인 방안을 추론하고 검토해 볼 수 있다. 참고로 ISO/SAE 21434는 2021년 상반기 DIS 버전이 출시되었으며, 2021년 8월 Final Release 되었다.

도메인별 사이버 보안 엔지니어링 표준 최신 기술 수집 및 파트너 간의 협력을 지원하는 ISO/SAE 21434는 기능 안전 관점의 사이버 보안 인터페이스만 다루는 ISO 26262: 2018을 보완하기 위해 자동차 사이버 보안 표준 개발의 필요성에 따라 작성되었다.

사이버 보안이 충분히 고려되고 이를 보장하기 위한 대응 절차를 통해 E/E(electrical and electronic) 시스템이 최첨단 기술과 진화하는 악의적인 공격 방법에 대응할 수 있도록 하는 것을 목표로 한다. 이러한 목표 달성을 위해 사이버 보안 엔지니어링과 관련된 어휘, 목표, 요구사항 및 지침을 공급망 전반에 걸쳐 이해를 위한 기반 정보와 조직이 수행해야 할 사이버 보안 정책 및 프로세스, 사이버 보안 위험 관리, 사이버 보안 문화 조성을 위한 정보를 제공한다. 이와 더불어 사이버 보안 위험 관리를 포함한 사이버 보안 관리 시스템을 구현하는데 사용할 수 있는 보안 코딩 준수 내용도 함께 기술하고 있다. 보안 코딩 준수방안에 대해 ISO/SAE 21434에서 언급된 내용은 다음과 같이 확인할 수 있다[5].

[RQ-10-05] 언어 자체로 해결되지 않는 사이버 보안에 적합한 설계, 모델링 또는 프로그래밍 언어에 대한 기준([RQ-10-04] 참조)은 설계, 모델링 및 코딩 지침 또는 개발 환경에서 다루어야 합니다.

예5〉 'C' 프로그래밍 언어의 보안코딩을 위해 MISRA C:2012 또는 CERT C 사용

〈인용〉 ISO/SAE International, ISO_SAE_21434_2021 INTERNATIONAL STANDARD, 2021.

프로그래밍 개발언어 자체 제약으로 해결되지 않은 사이버보안 이슈를 해결하기 위한 보안 코딩의 필요성을 확인할 수 있으며, 이에 대한 방안으로 MISRA C: 2012[6]과 CERT C[7]를 제안하고 있다. 이에 언급된 두 가지 보안 코딩 가이드를 비교/검토하여 사이버 보안을 위한 적합한 방안을 도출하고자 한다.

IV. 보안 코딩 가이드 비교

ISO/SAE 21434에 언급된 MISRA C: 2012과 CERT C를 비교하기 위해 가이드 목적, 가이드 항목별 정의, Coverage 순으로 정리하고 내용을 비교한다. 먼저, 보안 코딩 가이드 비교를 위해 MISRA C:2012와 CERT C:2016의 목적을 아래와 같이 정리하였다[6],[7].

- MISRA C 2012, Guidelines for the use of the C language in critical systems, 3rd Edition, 1st Revision
  - MISRA Consortium에서 개발한 C 프로그래밍 언어용 소프트웨어 개발 가이드라인
  - ISO C/C90/C99에 프로그래밍된 시스템에서 safety, security, portability, reliability 촉진하는 것
- SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems(2016 Edition)
  - 소프트웨어 시스템의 safety, reliability, security 개선을 위해 개발한 소프트웨어 코딩 표준
  - CERT C 보안 코딩 표준의 지침은 CWE(Common Weakness Enumeration) 항목 및 MISRA를 비롯한 여러 다른 표준과 상호 참조 가능

위 정의에서 보는 것과 같이 두 개의 코딩 가이드라인은 safety, security, reliability를 목적으로 한다는 점과 코딩 가이드라인 형태로 정보를 제공하고 있는 점에서 공통점을 찾을 수 있다. 또한, 가이드라인 구성에서도 CERT는 Rules와 Recommendations로 MISRA는 Rules와 Directives 로 구성되어 유사한 구조를 보인다.

좀 더 세부적으로 각 가이드 항목의 정의를 서로 비교하여 추가적인 공통 사항 또는 차이점을 확인해 볼 수 있다. [표 1]에 작성된 각 가이드 항목의 정의를 통해 코딩 가이드라인의 구성에서 Rules가 소스 코드 수행에 대한 직접적인 영향을 미치는 항목으로 구성되었다는 점과 정적 도구를 통해 검출 가능하다는 점 역시 공통점으로 볼 수 있다. 하지만, CERT의 Rules와 Recommendations는 보안을 목적으로 정의되고 설계된 보안 가이드라는 점에서 가장 큰 차이를 가진다고 볼 수 있다.

[표 1] CERT C와 MISRA C:2012 비교

구분	비교 내용
CERT Rules 정의	- 악용 가능한 취약성을 초래할 수 있는 보안 결함으로 시스템의 안전, 신뢰성 또는 보안에 부정적인 영향을 미칠 수 있는 결함 - 소스 코드 주석이나 가정에 의존하지 않으며, 지침 준수 여부는 자동화된 분석(정적 또는 동적)으로 검출되는 항목
MISRA Rules 정의	- 요구사항에 대한 완전한 설명이 제공되는 지침 - 타 정보 없이 소스 코드가 규칙을 준수하는지 확인할 수 있어야 하고 정적 분석 도구를 통해 적용되는 규칙
CERT Recommendations 정의	- 가이드라인의 적용은 소프트웨어 시스템의 안전성, 신뢰성, 보안성을 향상시킬 수 있는 항목 - 소스코드 실행에 직접적인 영향이 없는 내용이나, 추후 보안에 문제 소지가 있는 항목들로 구성
MISRA Directives 정의	- Compliance 확인을 수행하는데 필요한 전체 설명을 제공할 수 없는 가이드라인 - 검사를 수행하려면 설계 문서 또는 요구사항 사양에 제공될 수 있는 것과 같은 추가 정보 필요

〈자료〉 MISRA C 2012, Guidelines for the use of the C language in critical systems, 3rd Edition, 1st Revision, February 2019. ISBN (print/electronic): 978-1-906400-21-7/978-1-906400-22-4
SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems(2016 Edition), Pennsylvania: Software Engineering Institue, Carnegie Mellon University, 2016 [viewed 2021-02-12].

CERT는 소프트웨어의 Safety, Reliability, Security를 개선하기 위한 코딩 가이드라인으로 Carnegie Mellon University의 Software Engineering Institute에서 유지 관리하는 보안 코딩 표준이다. 프로그래밍 언어(C, C++, Java, Android, Perl)별로 룰에 대한 설명 및 위험 평가를 제공하며, 최신 Rule 및 Recommendation은 보안 코딩 표준 웹 사이트에 게시한다. 또한, 사용자에게 보안 위협에 대한 명확한 우선순위와 레벨을 제공하기 위해 [표 2]와 같이 Rule 항목별 Severity(심각도), Likelihood(침해발생 가능성), Remediation

[표 2] 보안 항목별 의미

구분	의미
Severity (심각도)	규칙을 무시하면 얼마나 심각한 결과를 초래합니까?
Likelihood (침해발생 가능성)	규칙을 무시함으로써 생긴 결함이 악용 가능한 취약점으로 이어질 가능성은 얼마나 됩니까?
Remediation Cost (사후처리 비용)	규칙을 준수하는데 비용이 얼마입니까?

〈자료〉 Software Engineering Institute, “Trademarks and Servicemarks,” Software Engineering Institute website, 2012.

Cost(사후처리 비용)와 같은 보안 관련 정보를 제공한다.

이는 각 항목에 따라 다시 3개의 레벨로 재구분되어 우선순위를 도출하는 데 사용된다. Severity와 Remediation은 high, medium, low로 등급이 구분되며, Likelihood는 unlikely, probable, likely로 구분된다. 각 등급은 1~3점으로 치환되고 각 등급의 점수를 곱한 값을 통해 Priority 포인트를 산출해 낸다. 이를 통해 각 항목에 대한 등급은 [표 3]과 같이 정리할 수 있다.

[표 3] 위험 평가

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
FIO30-C	High	Unlikely	Medium	P18	L1
FIO32-C	Medium	Unlikely	Medium	P4	L3
FIO34-C	High	Probable	Medium	P12	L1
FIO37-C	High	Probable	Medium	P12	L1

〈자료〉 Software Engineering Institute, "Trademarks and Servicemarks." Software Engineering Institute website, 2012.

하지만, MISRA C:2012는 CERT C와는 다른 보안 접근 관점을 찾아볼 수 있으며, 보안 관련하여 MISRA C 2012 Amendment 1 문서의 머리말에 다음과 같이 적어 놓고 있다. 문서의 내용에 따르면 “안타깝게도 많은 사람들이 MISRA는 오직 safety에만 적용 가능하다는 생각을 가지고 있어 security에는 많이 연관되지 않는다는 인식이 있다”라고 언급한다[9]. 이에 대한 근거로 “MISRA 버전이 Release된 이후 security coding standard 인 17961가 Release됨에 따라 이러한 인식이 존재하는 것이라며, MISRA가 security와 연관이 아주 없지 않다”라고 언급하고 있다[9].

MISRA도 safety에 목적을 두고 개발되어 security에 대한 연관성 및 대응방안이 부족하

다는 인식을 알 수 있으며, MISRA C:2012의 근본적인 목적이 security가 아닌 safety에 근거함을 추론할 수 있다. MISRA는 이에 대한 보완책으로 MISRA는 Amendment 1, 2와 Addendem 1, 2, 3을 추가적으로 Release함으로써 security에 대한 coverage를 확보하고자 지속적으로 노력하고 있다.

마지막으로, MISRA에서 제공하고 있는 "MISRA C 2012 Addendum 3 Coverage of MISRA C 2012 against CERT C 2016 Edition"을 통해서 CERT와 MISRA의 룰 구성 및 지원율에 대한 차이를 확인해 볼 수 있다.

[표 4]는 CERT C:2016에 대한 MISRA C:2012 지원 룰을 매칭한 테이블로 정적도구를 통해 검출할 수 있는 부분만 한정하여 MISRA와 CERT를 비교하기 위해서 작성된 표이다. 해당 내용 보면 CERT C:2016의 총 99개 룰에 대한 MISRA C:2012 지원율은 88%로 공통의 룰이 존재하지만, 19개의 미지원 항목이 존재하여 실제 룰 구성 내용에서도 차이가 발생하고 있음을 알 수 있다. 결과적으로 ISO/SAE 21434에서 언급하는 코딩 가이드라인을 적용하기 위해서는 security에 대한 각각의 가이드라인의 목적, 구성 그리고 보안취약점에 대한 지원 내용을 종합적으로 고려하여 보안 코딩 가이드라인을 선정하고 적용해야 한다.

[표 4] CERT C 2016에 대한 MISRA C:2012의 커버리지

Classification	Strength	Number
Explicit	Strong	39
	Weak	5
Implicit	Strong	1
	Weak	13
Restrictive	Strong	22
	Weak	0
Partial	Strong/Weak	0
Out of Scope	None	15
Nome	None	4
합계		99

〈자료〉 HORIBA MIRA Limited, Coverage of MISRA C 2012 against CERT C 2016 Edition, 2018.

V. 결론

자동차 사이버 보안에 관한 국제기준 UNECE Regulation No.155 채택과 이로 인한 시장의 변화 그리고 보안 코딩 가이드 선택과 적용을 위해 MISRA와 CERT를 비교하여 보안 코딩 대응방안에 대해 기술하였다. 각 항목 비교를 통해 CERT와 MISRA의 개발 목적부터 룰 구성 내용까지 보안 코딩 가이드 적용을 위해 고려해야 할 사항들을 확인했으며, 이를 바탕으로 보안 코딩 가이드의 목적과 차이점을 검토하여 사내 프로세스 및 프로젝트의 보안 코딩 목적을 충족할 수 있도록 가이드 했다. 다양한 사용자의 요구사항과 상황에 따라 보안 코딩 가이드를 적용 및 활용할 수 있도록 함과 동시에 사용자가 효율적이고 효과적인 방법으로 보안 코딩 가이드를 선택할 수 있도록 했다.

현재 보안 코딩 가이드 적용하기 위한 구체적인 기준과 명확한 정책이 수립되지 않은 상황이다. 일부 차량 제조사는 명시적인 요구사항을 지정하여 보안 코딩 가이드 준수를 요구하기도 하지만 국내 이외의 제조사는 별도의 보안 코딩 가이드 요구가 지정되지 않고 있다. 이에 사용자는 역으로 보안 코딩 가이드 준수를 위한 계획을 제안하고 이를 위한 방안을 마련할 수 있어야 한다. 이를 위해 사용자는 보안 코딩 가이드의 목적, 구성, 내용을 올바르게 이해하고 다양한 프로젝트에 보안 코딩 가이드를 적용할 수 있는 역량을 확보해야 한다. 더불어, 보안 코딩 가이드 검토 및 선정, 룰에 대한 세부 분석 그리고 추가적인 자원 확보 노력과 구체화된 세부 진행 절차를 실용적으로 준비해 나아감으로써, 다양한 사이버 보안 시장의 요구에 적절하게 대응해 나가야 할 것이다.

참고문헌

[1] NYP, “19-year-old claims he hacked into over 25 Teslas in 13 countries,” 2022.
[2] UNECE, “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system,” 2021.
[3] UNECE, “Proposals for Interpretation Documents for UN Regulation No.155(Cyber security and cyber security management system),” 2021.
[4] 국토교통부, 한국교통안전공단, “자동차 사이버보안 가이드라인”, 2020.
[5] ISO/SAE International, ISO_SAE_21434_2021 INTERNATIONAL STANDARD, 2021.
[6] HORIBA MIRA Limited, MISRA C 2012, Guidelines for the use of the C language in critical systems, 3rd Edition, 1st Revision, Feb. 2019.

[7] Software Engineering Institue, SEI CERT C Coding Standard: Rules for Developing Safe, Reliable, and Secure Systems(2016 Edition), Carnegie Mellon University, 2016
[8] Software Engineering Institute, “Trademarks and Servicemarks,” Software Engineering Institute website, 2012.
[9] HORIBA MIRA Limited, MISRA C:2012 Amendment 1, 2016.
[10] HORIBA MIRA Limited, Coverage of MISRA C 2012 against CERT C 2016 Edition, 2018.
[11] Pitchford Mark, Software Engineering for Embedded Systems || Embedded Software Quality, Integration, and Testing Techniques, 2019.
[12] Salvi, Sayali; Kaestner, Daniel; Ferdinand, Christian; Bienmueller, Tom, [IEEE 2015 11th European Dependable Computing Conference(EDCC) - Paris, France(2015.9.7-2015.9.11)] 2015 11th European Dependable Computing Conference(EDCC) - Exploiting Synergies betweenStatic Analysis and Model-Based Testing, 2015.
[13] Roberto Bagnara, Michael Barr, Patricia M. Hill, BARR-C:2018 and MISRA C:2012:Synergy Between the Two Most Widely Used C Coding Standards, 2020.
[14] Podelski, Andreas, [Lecture Notes in Computer Science] Static Analysis Volume 11002(25th International Symposium, SAS 2018, Freiburg, Germany, August 29-31, 2018, Proceedings), 2018.
[15] Bagnara, Roberto, Bagnara, Abramo, Hill, Patricia M. The MISRA C Coding Standard and its Role in the Development and Analysis of Safety- and *Security-Critical* Embedded Software, 2018.