자동차 업계의 DevSecOps

자동차 보안, 안전성과 고객 신뢰 확보를 위한 필수 요소

WNDRVR

차량에서도 소프트웨어가 보편적인 존재가 되면서 보안의 중요성 증대

볼트 온(Bolt-on) 솔루션은 이제 차량 보안을 확보하는 데 역부족입니다. 요즘의 모범 사례에서는 DevSecOps의 원칙을 받아들여 개발 초기부터 보호를 포함하고 장기적인 자동 테스트를 제공합니다.

차량 제조업체와 자동차 솔루션을 개발하는 독립형 소프트웨어 공급업체에서 보안 보호 기능을 한 단계 끌어올리고 차량 작동의 안전성을 배가하기 위해 DevSecOps를 도입하는 사례가 늘어나고 있습니다. 개발 초기 단계에 잠재적인 취약점을 평가하여 제거하는 것은 설계의 핵심적인 부분이며, 이를 통해 더욱 안전한 솔루션을 릴리스하고 코드를 더욱 효과적으로 유지할 수 있습니다.

DevSecOps는 친숙한 DevOps를 자연스럽게 확장한 것으로, 작업을 자동화하여 코드 개발에 일관성과 구조를 부여합니다. 코드를 자주 릴리스 및 리뷰하고 보안 모니터링 및 시뮬레이션을 활용하여 위험 요소를 파악하고 개발 과정 중에 이를 시정하며 지속적인 유지 관리의 일부분으로 계속 시행합니다. 도로에 자율주행 및 반자율주행 차량이 출현하기 시작하면서 보안을 강화한 DevSecOps가 고객의 신뢰를 얻고, 새롭게 출현하는 사이버 보안 문제점에 대응하며 주행 안전을 개선하는 데 필수적인 역할을 하고 있습니다.

2025년까지 사이버 범죄로 인해 발생하는 연간 비용[1]

– Cybercrime Magazine

1 *cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016*

DevSecOps란 무엇인가요?

DevSecOps 프로세스는 DevOps에서 발전한 형태로, 소프트웨어 개발과 운영을 순환형 흐름을 포함한 하나의 통합형 프로세스로 합쳤습니다.

이러한 순환 주기는 코드를 신속하게 릴리스하고 엄격한 테스트와 피드백을 거쳐 소프트웨어 제품의 전체 수명 주기를 인식하는 것이 무엇보다 중요합니다. DevOps는 대다수 기업에서 소프트웨어 빌드 및 업데이트 지침으로 삼을 근본적이고 유용한 실무로 도입되었으며, 이것이 발전하여 DevSecOps가 되면서 순환 주기 흐름에 보안 프로비저닝을 추가했습니다(그림 1 참고). 코드 계획, 빌드, 테스트 프로세스와 보안 문제(위협 완화, 스캐닝, 분석, 시정 및 각 코드 릴리스의 지속적인 모니터링 포함) 등을 순환 주기의 일부로 검사합니다.

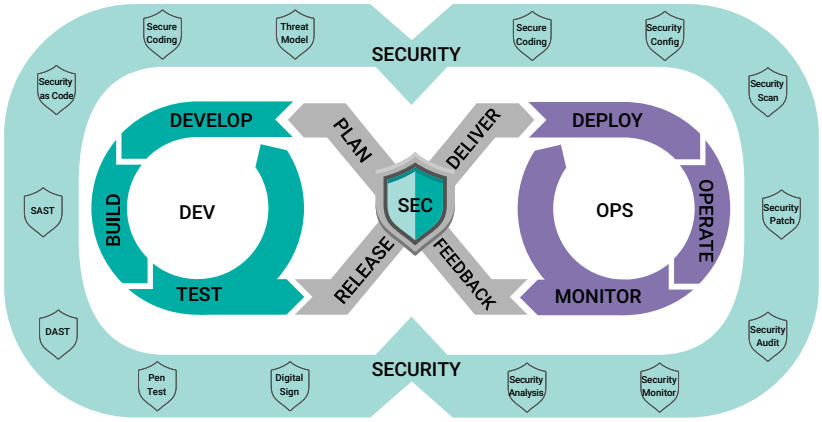
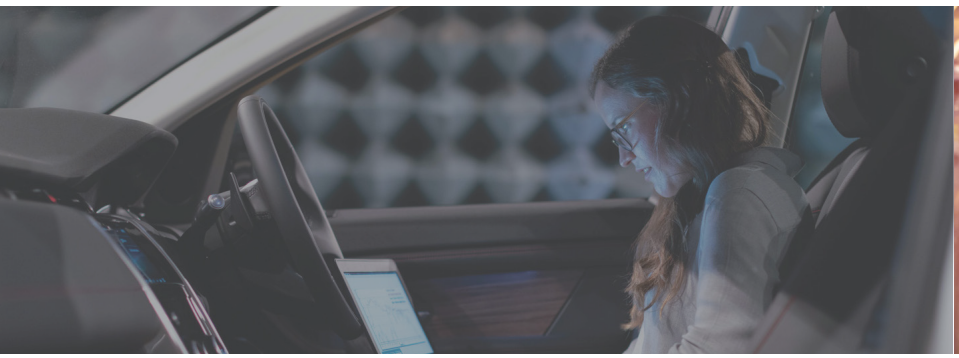


그림 1. DevSecOps는 친숙한 DevOps에 보안을 추가한 형식

차량 보안 보호는 특히 크게 두 가지 영역에서 중요합니다. 하나는 전자 제어 장치(Electronic Control Units, ECU)의 설계와 사용이고, 다른 하나는 자동화된 운전자 지원 시스템(Automated Driver Assistance Systems, ADAS)입니다. 차량의 ECU나 ADAS가 해킹되거나 운전자 외의 다른 외부 사람에게 주도권을 빼앗기면 안전 면에서나 개인정보 면에서나 엄청난 결과를 초래할 수 있습니다.

> "첨단 자동차의 주요 사이버 보안 우려 사항이 대두되면서, 유럽경제위원회(UNECE)에서 최근 사이버 보안과 소프트웨어 보안에 관한 새로운 규정을 두 가지 고안하여 제조업체와 소비자 모두 앞으로 고려해야 할 위험 요소를 관리하는 데 도움이 되도록 조처하였습니다."
>
> – SecurityBoulevard.com



교통수단 시스템과 공공복지를 보호할 책임을 맡은 기관에서는 선제적으로 위험 요소를 해결하기 위해 서두르는 태세입니다. 예를 들어 Stephen Gates는 Security Boulevard에 이렇게 기고했습니다.

"첨단 자동차의 주요 사이버 보안 우려 사항이 대두되면서 유럽경제위원회(UNECE)에서 최근 사이버 보안과 소프트웨어 보안에 관한 새로운 규정을 두 가지 고안하여 제조업체와 소비자 모두 앞으로 고려해야 할 위험 요소를 관리하는 데 도움이 되도록 조처하였습니다. 이러한 규정은 법적으로 효력이 있고, 자동차 보안이라는 분야에서 사상 최초로 세계적으로 여러 기관이 협력하여 이뤄낸 결과입니다. 이 규정은 승용차, 밴, 트럭과 버스에 적용되며 2021년 1월부터 효력이 발생합니다. 이러한 규정은 주로 오늘날 자동차 한 대에 신형 전투기보다 약 4배 많은 것으로 추산되는 약 150여 종의 전자 제어 장치(ECU)와 대략 1억 줄의 소프트웨어 코드를 포함할 수 있다는 사실 때문에 생겨납니다."[2]

자동차, 트럭과 기타 차량은 결국 바퀴가 있는 소프트웨어 플랫폼이 될 것으로, 국가 차원에서나 국제적인 수준에서도 이와 비슷한 규정 명령이 출현할 것으로 전망됩니다. Wind River®는 차량 보안 강화를 위해 나선 초창기 주역 중 하나였으며, 지금도 사이버 공격에 대응해 광범위한 임베디드 보안 솔루션 레코드를 제공하는 믿음직한 솔루션 제공업체입니다.

미국에서는 고속도로 안전관리국(National Highway Traffic Safety Administration)에서 자동차 업계 제조업체와 시스템 개발업체에 지침을 제공하여 자율주행 시스템을 제작하는 과정을 지원하고(안전 표준 포함), 권장 연구소 테스트, 시뮬레이션과 교육 활용법 등을 안내하고 있습니다. 이 기관의 관점을 설명한 보고서 자율주행 차량 기술 분야에서 미국의 리더십 보장(Ensuring American Leadership in Automated Vehicle Technologies)이 지난 2020년 1월에 발행된 바 있습니다.

> "2023년까지 텔레매틱스나 차량 내 앱을 통해 연결된 차량 수가 7억 7,500만 대를 넘을 것으로 전망됩니다(2018년 3억 3천만 대 대비)."[3]
>
> – Juniper Research

2 *securityboulevard.com/2020/07/on-the-road-to-devsecops-securing-the-software-driving-mobility*

3 *www.juniperresearch.com/press/press-releases/in-vehicle-commerce-opportunities-exceed-775mn*

시장을 변화시키는 자율주행 자동차

자율주행 차량이 보급되는 속도에 맞춰 안전 시스템과 보안 보호 기능도 발달해야 합니다.

세계 자율주행 차량 시장은 2019년부터 2026년까지 39.5%[4]의 성장률로 규모를 키울 것으로 전망됩니다. 이와 같은 정도로 자동차의 복잡성도 훌쩍 증가할 것이므로, 이에 상응하는 임베디드 안전성 및 보안 메커니즘의 필요성이 대두됩니다. 이러한 조건에 환경까지 급속히 변화하는 상황이므로, DevSecOps의 가치가 크게 증폭됩니다. 기술에 적합한 시스템이 마련되어 체계적으로 소프트웨어 업데이트와 패치를 제공하고 취약점을 일상적으로 모니터링해야 하며, 중요 소프트웨어 구성요소의 수명 주기를 유지해야 합니다.

566억 7천만

2026년까지 세계 자율주행 차량 시장의 규모[5]
— Allied Market Research

ADAS에서 제공되는 지원 기능은 다섯 가지 레벨로 정의됩니다. 완전한 자율주행 차량 운행 시대로 나아가는 지금은 레벨 2에 해당합니다(그림 2 참조). 인공 지능, 특히 딥 러닝이 발달해야 완전 자율주행으로 전환을 마칠 수 있습니다. 이 분야에서 더 진전을 이루려면 안전성을 고려하고 해킹 시도에 맞서 여러 시스템을 보호하는 등 한층 정교한 제어 시스템을 갖춰야 합니다.

> "심각한 교통사고의 94%는 인간적인 실수 탓에 일어납니다. 2018년 미국에서 차량 충돌과 관련하여 발생한 사망자 수는 36,560명에 달했으며, 이는 운전자 보조 기술로 사람의 생명을 구할 수 있다는 장점을 적극 활용해야 한다는 점을 보여줍니다."[6]
>
> – 미국 교통부

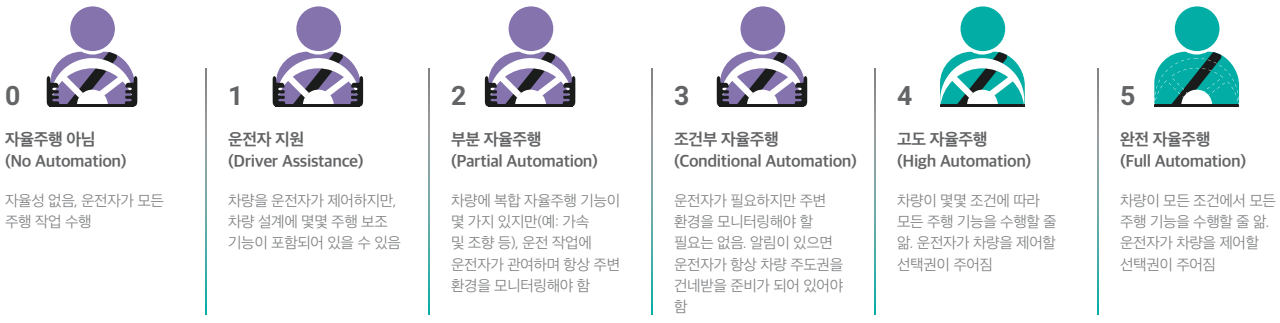


그림 2. 완전 자율주행 차량 작동으로 가는 자율주행 레벨[7]

4 www.alliedmarketresearch.com/autonomous-vehicle-market
5 www.alliedmarketresearch.com/autonomous-vehicle-market
6 www.nhtsa.gov/technology-innovation/automated-vehicles-safety#topic-road-self-driving
7 www.nhtsa.gov/technology-innovation/automated-vehicles-safety#topic-road-self-driving

DevSecOps 기본 모범 사례

DevSecOps를 도입한 기업이 점차 늘어나면서, 모범 사례도 공통성을 갖게 되었습니다.

이러한 모범 사례는 워크플로에 보안이 포함된 소프트웨어를 구현하는 데 적합한 구성 프레임워크를 제시합니다. 권장 지침에 포함되는 원칙은 다음과 같습니다.

1. 개발 단계 중 최대한 이른 시기에 자동 보안 제어 및 테스트 시퀀스를 포함합니다.
2. 업그레이드, 패치, 발전하는 취약점 테스트와 코드의 수명 종료 조항 등을 고려하여 소프트웨어 수명 주기 전체를 중심으로 계획을 수립합니다.
3. 코드를 개발하면서 동시에 스캔할 수 있는 툴을 사용하여 각종 보안 약점을 탐지해 해결합니다.
4. 오픈 소스 구성요소와 관련된 각종 코드 종속성을 자주 검사하여 알려진 취약점을 파악합니다.
5. 정적 애플리케이션 보안 테스트(SAST) 툴을 적용하여 오픈 소스 코드와 컴파일링한 코드 양쪽 모두의 보안 결함을 확인합니다.
6. 동적 애플리케이션 보안 테스트(DAST) 시퀀스를 구현하여 시스템 내 침입을 시뮬레이션합니다.
7. 광범위한 위협 모델링을 수행하여 취약점 위치를 찾고 보안 제어의 간극(있는 경우)을 완화합니다.

이처럼 잘 정립되고 철저한 자동 방식으로 보안 설계와 테스트에 접근하면 소프트웨어 솔루션에서 위협 식별과 제거를 핵심적인 부분으로 다루도록 보장할 수 있습니다. 그림 3에 표시한 것과 같이, 파이프라인이 코드 선택과 분석부터 릴리스와 수명 주기 관리까지 모든 단계를 아우릅니다. 코드 업데이트, 패치 및 지속적인 취약점 테스트 면에서 360도 보안을 유지하는 데 최적의 결과를 보장하려면 AI 구성요소를 사용해 업데이트 예약과 배포를 관리하는 경우가 많으며, 이전에 발견되지 않은 위협을 탐지하기 위해 테스트를 자주 수행하는 것이 좋습니다. 클라우드를 통해 소프트웨어를 배포하는 사례가 보편적으로 자리 잡고 있으며, 이와 함께 차량 내 안전한 소프트웨어 환경을 안전하고 효율적으로 유지 관리하기 위해 컨테이너를 사용하는 경우가 늘어나는 추세입니다.

발전하는 자동차 기술 분야에서 Wind River의 역할

Wind River에서 제공하는 솔루션은 높은 수준의 안정성, 보안과 안전성이 요구되는 까다로운 업계에서 오래전부터 신뢰할 수 있는 구성요소로 여겨져 왔습니다. 여기에는 중요 인프라의 구축과 유지 관리, 산업 제조 및 장비 프로세스, 항공우주 산업, 방위 산업 등 여러 업종을 포함합니다. VxWorks®는 세간의 이목을 끄는 우주 비행 임무를 비롯한 중요 업무용 배포에 최대한의 안정성을 보장하기 위해 종종 선정되는 실시간 운영 체제(RTOS)입니다. Wind River는 5G 통신으로 강화되는 지능형 에지 컴퓨팅 개발과 구체화에도 우수한 성과를 내어 정교한 지능형 에지 설치를 지원하였습니다. 이는 자율주행 차량과 스마트 시티 교통수단의 앞날에 점점 중요한 의미가 있는 요소입니다. 차량에 컨테이너화한 소프트웨어 구성요소를 제공하기 위해 개발된 클라우드 기술 또한 Wind River의 전문 분야입니다.

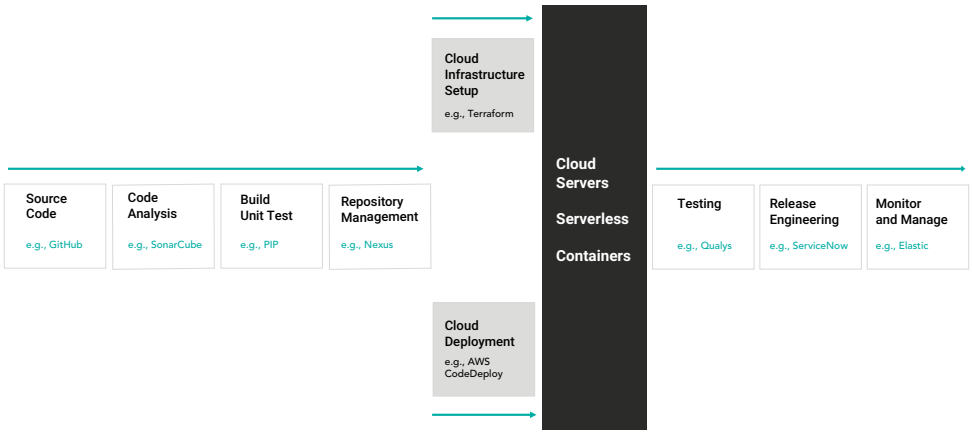


그림 3. DevSecOps 파이프라인은 개발 주기 전체에 걸친 자동 테스트 강조

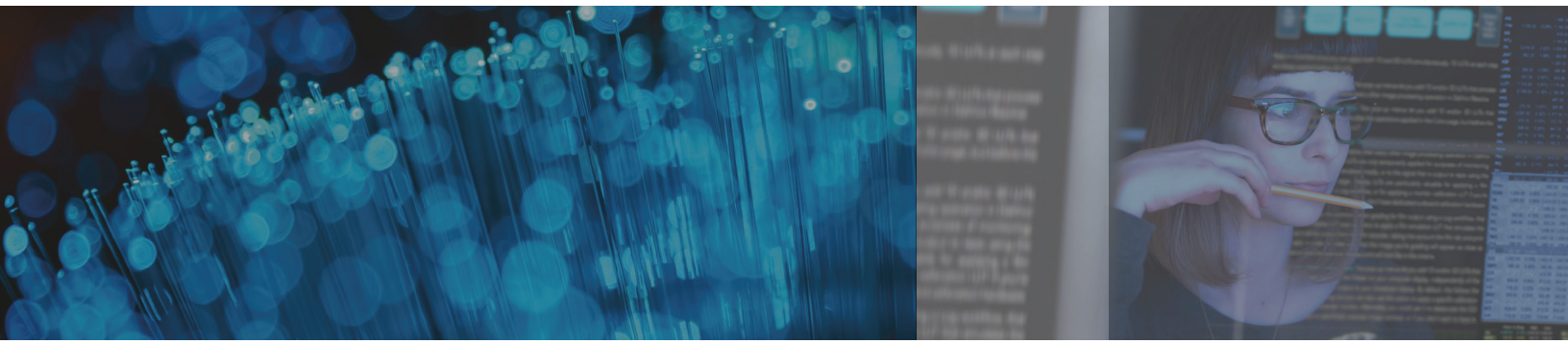
여러 파생 제품이 있는 경우, 소프트웨어 무결성을 보장하기 위해 DevSecOps 툴을 사용하여 가능한 각 사례의 전체 범위를 자동으로 테스트할 수 있습니다. 이것은 AI를 활용해 프로세스를 감독하고 인간의 잘못된 의사 결정으로 인한 잠재적인 오류가 발생할 가능성을 줄이는 또 다른 영역입니다.

차량과 차량 작동을 위한 데이터를 일상적으로 수집하여 클라우드로 보내는 과정에서 머신 러닝을 적용하여 소프트웨어 내에서 발생 가능한 안전성 문제를 지속해서 분석하고, 예측형 유지 관리 검사를 수행하여 운전자나 정비팀에 구성요소 오류가 해결을 대기 중이라는 사실을 알릴 수도 있고, 프로그래밍을 변용하여 안정성 문제에 좀 더 효율적으로, 개선된 방식으로 대응하도록 할 수도 있습니다.

" 전형적인 차세대 차량에는 다섯 가지 이상의 영역으로 구성된 소프트웨어 아키텍처가 포함될 가능성이 큽니다. 여기에 차량 내부와 클라우드 내에 존재하는 수백 가지 기능적인 구성요소까지 더해집니다. 이런 것들이 인포테인먼트와 ADAS부터 매핑, 텔레매틱스, 타사 애플리케이션까지 모든 작업을 담당합니다. 이런 아키텍처를 구축하는 일반적인 OEM은 다양한 소프트웨어 제공업체와 교류하며 다양한 기능을 빌드합니다. 이 과정에서 차량에 광범위한 개발 언어, 운영 체제와 소프트웨어 구조가 채워지게 됩니다. 업계를 대표하는 기업에서도 시중에 있는 어떤 소프트웨어 플랫폼도 시스템 요구사항 모두에 단독으로 부응할 수는 없기 때문에 이런 단편적인 방식이 흔합니다."[8]

– **McKinsey & Company,**
2020년 1월

8 *https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-case-for-an-end-to-end-automotive-software-platform*



DEVSECOPS의 핵심은 시뮬레이션

DevSecOps 모델에서 효과적인 성과를 내려면 일관된 테스트를 자주 수행해야 하며 잘 정의된 파이프라인 내에서 이를 되풀이해야 합니다. 애자일 개발을 효과적으로 지원하려면 하드웨어, 운영 체제, 네트워크, 주변 기기와 보드의 기능성을 모델링하는 시스템 전체 시뮬레이터가 있어야 합니다. Wind River Simics®는 강력한 프레임워크를 제안하여 이 안에서 구성요소 작업을 정확하게 재현함으로써 새 코드를 고안, 실행할 테스트베드를 제공합니다. 여기에서 취약점을 검사하고 탐지된 문제에 대한 해결 방법을 생각해내며 차량 시스템의 전반적인 무결성을 평가할 수 있습니다.

그림 4에 표시한 것과 같이 침투 테스트는 소프트웨어 구성요소를 최신 버전으로 유지하고 새로운 해킹 기법을 식별하여 위협을 완화하면서 소프트웨어를 침입으로부터 보호해주는 데 꼭 필요합니다. 시뮬레이션 방식 침투 테스트는 공격적으로 보호 기능을 뚫고, 실제 운행 중이거나 도로에 나와 있는 차량을 실시간 테스트하는 위험한 작업을 수행하지 않고도 기존의 알려진 위협에 맞설 방법을 모색하기 위해 개발된 방식입니다. 그림에 표시된 것과 같이 이 테스트는 여러 단계를 거치는 지속적인 주기의 일부분이며, 단계를 마치면 처음부터 다시 시작하게 되어 있습니다. 이 프로세스 전체를 자동화하여 필요한 만큼 자주 수행함으로써 소프트웨어 무결성과 보안을 최고 수준으로 유지하는 것입니다.

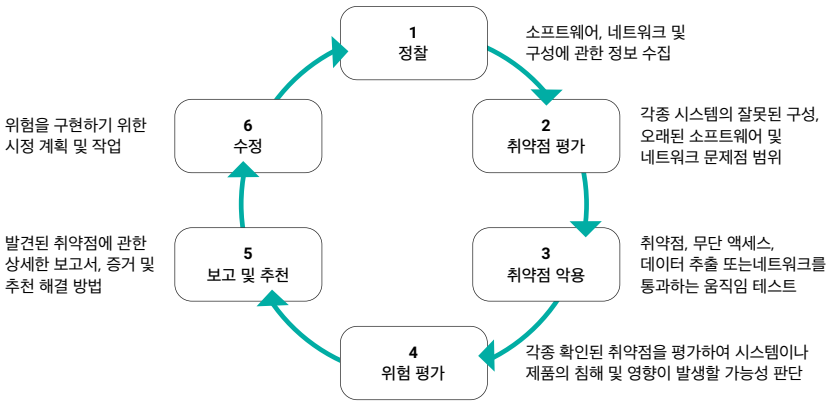


그림 4. 보안 프레임워크 내 약한 지점을 파악하는 침투 테스트

Wind River 솔루션

소프트웨어 정의 차량(Software-Defined Vehicle) 운행이 점차 대세로 자리 잡으면서 발생한 문제점을 Wind River의 솔루션 포트폴리오를 활용해 유능하게 대처할 수 있습니다. VxWorks, Wind River Linux, Wind River Helix™ Virtualization Platform과 Simics 등은 모두 자동차 업계에서 사용되어온 솔루션입니다. Wind River Studio는 새로 나온 통합형 클라우드 플랫폼으로, 이 포트폴리오에 최근 추가되었습니다. 이들 솔루션은 그간 조정을 거쳐 광범위한 중요 업무용 배포에 맞춰졌으며, 여기에는 에너지, 항공우주, 국방, 의료 및 제조 등의 분야가 포함됩니다. 이들 구성요소는 플랫폼 솔루션의 부분으로나 인프라 요소와 합쳐서 인증 요구 사항에 부합하는 데 시간을 절약해주는 경우가 많습니다.

- **VxWorks**: 세계를 선도하는 상용 실시간 운영 체제(RTOS)인 VxWorks는 지능형 차량 애플리케이션을 구축하는 데 유리한 DevSecOps 워크플로를 탄탄히 지원합니다. VxWorks는 개발 단계에서 소스 코드 작성, 코드 분석, 빌드 및 유닛 테스트와 리포지토리 관리를 담당합니다. VxWorks는 AUTOSAR(Adaptive AUTomotive Open System ARchitecture)도 지원합니다. 이는 자동차 법인에서 자동차 ECU 표준을 정립하기 위해 협력하여 개발한 아키텍처입니다.

- **Wind River Linux**: Wind River는 Yocto 프로젝트의 창립 멤버사이자 최고의 기여자로서 Yocto와 호환되는 Wind River Linux를 제공합니다. Wind River Linux는 임베디드 개발에 사용할 수 있는 상용급 기능과 다양한 종류의 사전 검증 된 오픈소스 소프트웨어로 차량 애플리케이션에 활용할 수 있는 유용한 기능을 비롯해, 컨테이너 기술을 통한 마이크로서비스 형태의 빠른 배포와 업데이트를 제공합니다.

- **Wind River Studio**: Wind River Studio에는 개발자 기능이 통합되어 있어 디지털 규모로 지능형 시스템에 수명 주기 전체를 관리하는 플랫폼을 제공하는 유일한 솔루션입니다. Studio가 개발 워크플로를 솔루션에 재설계하여 개발 비용을 절감하고 에지에서의 빌드, 테스트와 배포 기능 속도를 빠르게 해줍니다.

> "Wind River Professional Services 팀은 임베디드 디바이스 보안 강화 분야에서 쌓은 수십 년의 경험을 활용하여 사이버 보안 위협으로부터 디바이스를 보호합니다."[9]

9 *blogs.windriver.com/wind_river_blog/2020/03/tools-for-agile-development*

- **Wind River Helix Virtualization Platform:** 이 소프트웨어 플랫폼은 가상 프레임워크를 지원하고, DevSecOps 워크플로우의 일부로 코드를 제품화하는 입증된 기법을 제공합니다. Helix Platform은 안전 필수 어플리케이션과 일반적인 어플리케이션을 나란히 구동 시킬 수 있는 혼합중요(mixed-criticality) OS들을 지원하는 것과 동시에 ISO26262 안정성 표준의 엄격한 요구사항을 충족합니다.

- **Wind River Simics:** 무수히 많은 종류의 하드웨어와 운영 체제의 기능을 재현하는 전체 시스템 시뮬레이터로, 복잡한 자동차 시스템의 설계, 개발과 테스트 속도를 빠르게 해주면서도 안전성과 보안을 보장할 메커니즘을 제공합니다. Simics는 애자일 및 DevSecOps 소프트웨어를 수용하여 담당 팀에서 개발 주기를 단축하고, 실물 하드웨어 없이도 임베디드 시스템 설계를 철저하게 테스트할 수 있게 합니다.

Wind River는 인텔리전트 에지를 위한 글로벌 소프트웨어 리더입니다. Wind River의 기술은 1981년부터 가장 안심할 수 있고 안전한 장치를 만드는 데 기여해 왔으며, 수십억 개의 제품에 사용되고 있습니다. Wind River는 최고 수준의 안전과 보안, 신뢰도를 필요로 하는 필수적인 에지 시스템의 디지털 변혁을 가속화하고 있습니다.

향후 방향성

여러 가지 검증된 기술이 서로 융합되어야 차량의 안전성과 보안의 발전에 기여하며, 상호운용성을 완비하여 차량 간 통신(V2V)과 차량 사물 간 통신(V2X) 연결을 지원할 수 있습니다. DevSecOps를 포함하는 자동차 솔루션은 대개 가상화, 클라우드 컴퓨팅, 정교한 시뮬레이션, 반응성이 뛰어난 RTOS, 5G 통신이 좌우하며 이외에 중복성, 안정성과 성능을 위한 멀티코어 애플리케이션을 지원하는 하드웨어 플랫폼도 중요한 역할을 합니다. Wind River는 반자율 및 자율주행 자동차의 개발과 이용에 적합한 안전하고 보안이 보장되는 미래를 만들기 위해 역동적인 전 세계적 생태계 전반에 걸쳐 같은 생각을 가진 파트너들을 한데 모으고 있습니다.

Wind River Korea
3F, Sambo building, 638, Yeongdong-daero,
Gangnam-gu, Seoul, 06080, Korea

Contact
scott.kim@windriver.com