2020 IT 21
Global Conference
Digital New Deal
Technology Essentials
디지털 뉴딜 기술 핵심

Session 1-2

스마트카 보안 표준화 동향 및 관련 법규

윤세욱 위원 (DNV GL Korea)

[요약문]

자동차 분야의 기술 발전이 빠르게 진행되고 있다는 것은 부인할 수 없는 사실이며, 머신러닝과 인공지능 기술을 사용하는 자율주행기능과 5G, 와이파이, 블루투스 등의 통시기술을 사용하는 커넥티드기능을 보유한 스마트카의 등장은 기존에 없던 새로운 기술에 대한 잠재적 위험 및 사이버보안 문제를 유발하게 되었다. 스마트카를 대상으로 하는 공격은 차량을 고정시키거나, 도로에서의 사고, 민감한 개인정보 공개 등의 보안문제들뿐 아니라 차량 승객과 보행자들의 안전을 위협하게 될 것이다. 따라서 관련 위협 및 사이버보안 위험을 분석하고 이러한 위험을 해결하기 위한 보안대책을 제시하는 것이 중요하다.

본 강연에서는 스마트카 개발동향을 파악하고 이와 관련된 보안 위협과 취약점을 해결하기 위한 다양한 국제적인 노력, 즉 국제 표준과 관련 법규에 대하여 분석한다. 자동차 사이버보안 최초의 국제표준인 ISO/SAE 21434 는 사이버보안경영시스템(CSMS, Cyber Security Management System)을 구축하여 사이버 보안 정책 및 프로세스를 정의하고, 사이버 보안 위험을 관리하고 사이버보안 문화를 육성함으로써, 자동차의 사이버보안 리스크를 최소화하기 위한 개발활동을 수행할 수 있도록 도움을 준다. 2020년 6월 26일, UNECE WP29는 국제 표준에서 정의한사이버보안 경영시스템의 인증을 강제하고, 국제적인 구속력이 있는 사이버보안 규제를 발표하였고, 자동차 제조사로 하여금 성능과 심사/감사 등에 대한 명확한 요구사항을 정하고 이에 대한 형식승인을 제출하도록 함으로써 사이버보안에 관한 위험을 해결하는 데 도움이 될 전망이다.

[발표자 약력]

1997년 인하대학교 전기공학 학사
1999년 인하대학교 전기공학 석사
2018년 연세대학교 정보대학원 정보시스템학 박사수료
2002년 삼성종합기술원
2003년~2012년 한국지엠 주식회사 설계품질기획팀장/안전성능통합 총괄
2013년~ 현재 DNVGL Korea 사이버보안 전문위원
관심분야 : 자동차 사이버보안 국제 표준, 국제 법규, 기능안전, 소프트웨어 프로세스

DNV·GL

BUSINESS ASSURANCE

스마트카 보안표준동향과 관련 법규

윤세욱

2020년 9월 24일

Confidential

DNV GL Group 소개

•1864년 노르웨이 오슬로 DNV 설립
•1867년 독일 함부르크 GL(독일 선급) 설립
•2013년 9월 DNV와 GL 합병, DNV GL 그룹 탄생

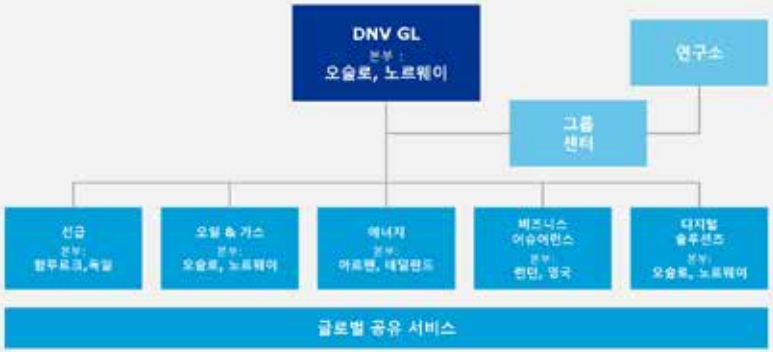
전세계 100여 개국에서

리스크 관리, 품질 보증 분야 WORLD LEADING
운송산업, 석유 및 가스, 전력 및 재생에너지

특히 자동차, 조선, 항공, 의료,식품·음료
경영시스템 분야 GLOBAL LEADER

DNV GL Group 소개

오랜 역사를 가진, 글로벌 기업



≈100,000
고객사

12000
임직원

350
개 사무소

100+
개국 지사 운영

2019년 말

목적
생명, 재산 및 환경의 보호

비전
글로벌 혁신을 위한 신뢰할 수 있는 목소리

가치
WE CARE
우리는 고객과 서로를 돌보고, 우리의 지구를 돌보고, 우리 자신을 돌봅니다.
WE DARE
우리는 과감히 탐험하고, 실험하고, 남들과 달라질 것이며, 용기있고, 호기심있고, 창의적일 것입니다.
WE SHARE
우리는 우리의 경험과 지식을 공유합니다. 우리는 서로, 그리고 고객들과 협력하고, 그 결과 지속적으로 성장하며 발전하고 있습니다.

Confidential

DNV GL KOREA 소개

- 선급, 인증, 검증, 검사, 평가 및 교육훈련 서비스를 제공

사무소	서울과 남부지역 5개 사무소
임직원	324 명
매출	1,130 억
인증 발행수	약 1,900 개

Confidential

DNV GL BUSINESS ASSURANCE KOREA 소개

- 전 산업 분야의 인증, 평가 및 교육훈련 서비스 제공
- 교육훈련 서비스 제공은 공개교육(Open Training) 및 고객 맞춤형 방문교육(Customized Training) 형태로 클라이언트 요청에 따라 선택

인증 & 검증 Certification & Verification | 평가 Assessment | **교육훈련** Training | 지속가능 자문 Sustainability Advisory | **산업별 특별서비스** Industry Specific Services

전 산업 분야의 인증, 평가 및 교육훈련 서비스를 수행

Confidential

자동차 산업 가치사슬의 변화

- 피라미드 구조에서 수평적 구조로의 자동차산업 가치사슬의 변화
  - 기존 자동차산업의 가치사슬 : 완성차업체에 부품을 납품하는 업체들(1차, 2차, 3차 티어 업체)이 수직적으로 형성한 피라미드구조
  - 티어 0.5는 완성차업체에 소프트웨어 시스템을 공급하는 IT하드웨어 혹은 소프트웨어업체로서 산업 의 경계가 모호함

Confidential

<출처 : 자동차/차부품 이슈리포트, 유진투자증권>

차세대 자동차의 새로운 생활상

① 이동 일정을 예약 ② 이동 목적에 맞는 차가 빌딩으로 옴 ③ 도로 인프라 정보를 활용한 최적의 주행경로 탐색 ④ 학교로 자녀를 데리러 감 ⑤ 부모와 자녀가 탑승 ⑥ 최적 경로 주행으로 늦지 않게 약속 장소에 도착

CASE 혁명

- **C**onnected : IT기술이 융합된 자동차에 모든 것이 **연결**
- **A**utonomous : 운전자 조작 없이 자동차가 **스스로** 판단하고 주행
- **S**hared : 한 대의 자동차를 시간단위로 **나누어** 여러 사람이 사용
- **E**lectrification : 자동차 구동방식이 내연기관에서 **전기**모터로 전환

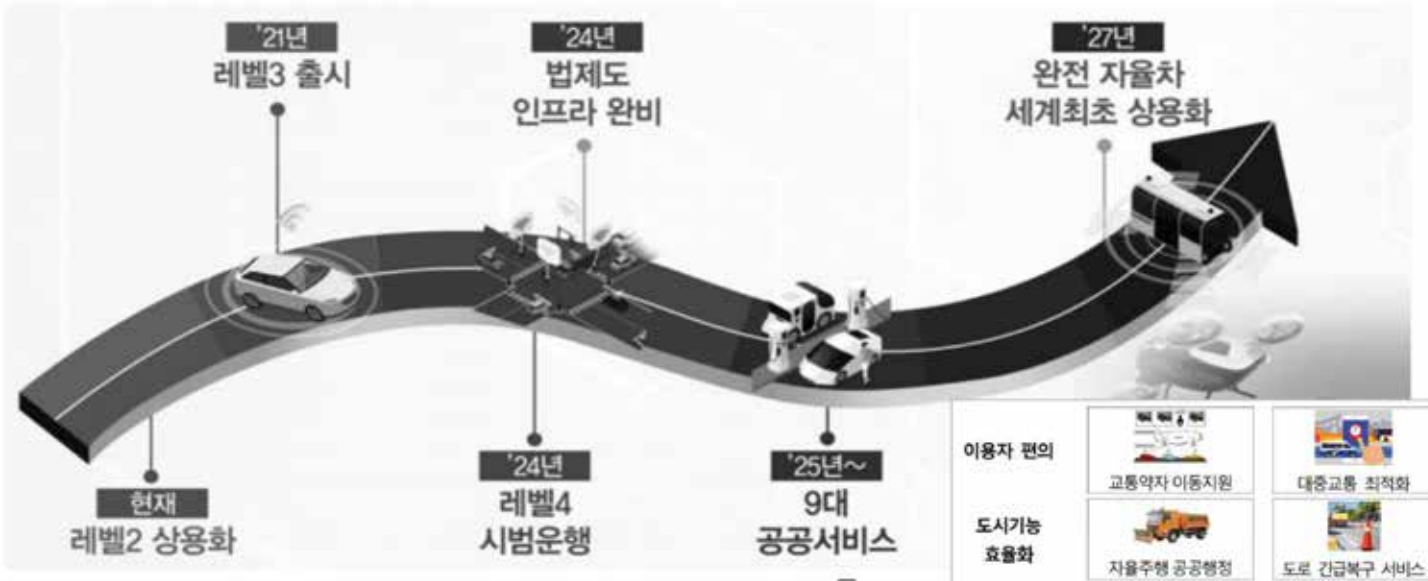
자동차 인프라의 발전 동인

- Safety : 도로 교통 안전의 확보
- Efficiency : 교통 운영의 효율적 증대
- Predictability : 교통 수요의 예측 가능성 증대

Confidential

<출처 : KPMG 교통보고서, 2020>

국내 자율주행차 로드맵



이용자 편의	교통약자 이동지원	대중교통 최적화	공유차 서비스
도시기능 효율화	자율주행 공공행정	도로 긴급복구 서비스	차량 고장시 긴급대응
국민안전 서비스	주야간 모니터링	긴급차량 통행지원	자율주행 순찰

<출처 : 미래자동차 산업 발전 전략 2030년 국가 로드맵>

차세대 자동차 주요 기술과 이슈

- **인지 및 판단** 시스템
  - 센서융합 중심 인지 및 판단시스템은 단순 규칙기반의 계산에서 **딥러닝 방식의 매우 높은 수준의 CPU/GPU /DSP 성능이 요구되는 기술**로 발전
  - 자율협력주행(C-ITS, 도로인프라)은 한계가 있는 차량용 센서의 성능(거리, 화각, 환경조건 등)을 보조하는 수단

<협동 지능형 교통시스템 도로>

- **커넥티드** 시스템
  - 다양한 내외부 연결기능의 증가로 다양한 서비스 제공
  - 외부 연결망은 다양한 공격방법에 노출가능

운전자를 위한 커넥티드 카

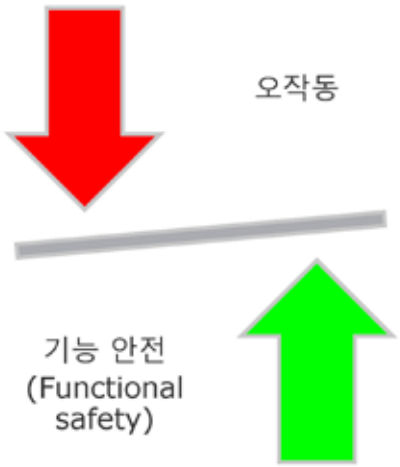
- 실시간 도로 정보
- 내비게이션
- 주차 보조 기능
- 기상 정보
- 엔터테인먼트
- 친환경 주행
- 클라우드 서비스
- 차량 앱

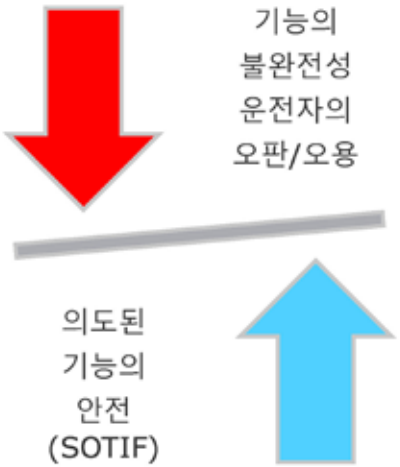
차량을 위한 커넥티드 카

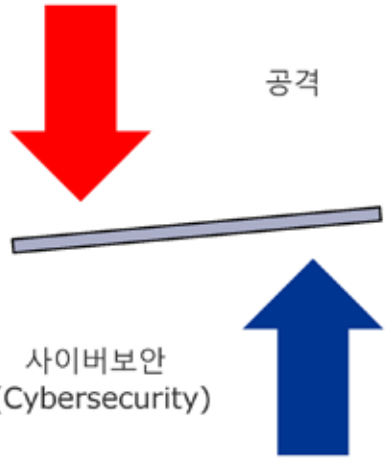
- 정비/진단
- 차량 추적
- 차량 간(V2V) 통신
- 차량과 인프라 간(V2I) 통신
- 텔레마틱스 및 보험 추적
- eCall 및 응급 서비스

<출처 : 중소기업 기술로드맵 2020-2022>

차세대 자동차 주요 기술과 이슈







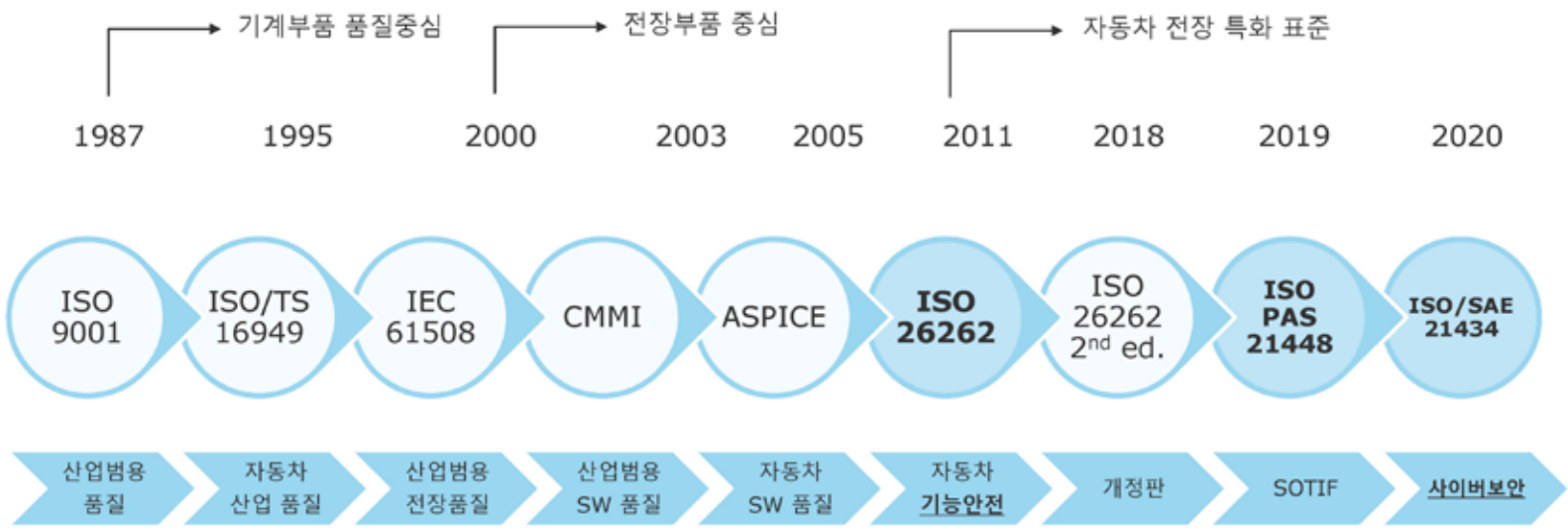
전기전자시스템의 ***오작동****으로 발생하는 위험원에 기인한 불합리한 위험을 없애는 것*

기능의 불완전성 혹은 사람에 의한 ***잘못된 사용***으로 발생할 수 있는 위험원에 기인한 불합리한 위험을 없애는 것

전기 또는 전자 부품 및 그 기능에 대한 ***위협 시나리오로부터 자산이 충분히 보호***받는 상태

Confidential

자동차 안전/품질/보안 관련 규격의 변천



CMMI : Capability Maturity Model Integration

ASPICE : Automotive Software Process Improvement Capability dEtermination

Safety of the intended functionality (의도된 기능 : 특정시스템에서 구현하는 기능

Confidential

자동차 사이버보안 규제 동향

2014. 10

NHTSA(미국 도로교통안전)
자동차 잠재적 보안위협 정의

2015

미국 상원 SPY
CAR 법안 제출

2016. 02

SAE J3061
자동차 사이버보안 가이드라인

2016. 07

AUTO-ISAC
모범 사례 배포

2016. 10

NHTSA
자동차 사이버보안
모범 사례 배포

Confidential

자동차 사이버보안 규제 동향

2017. 07

미국 하원

자율주행법안(SELF DRIVE ACT)

2017. 08

영국 정부

스마트카 보안 가이드라인 배포

2017. 09

유럽 자동차 제조사협회(ACEA)

자동차 보안 지침서

현재

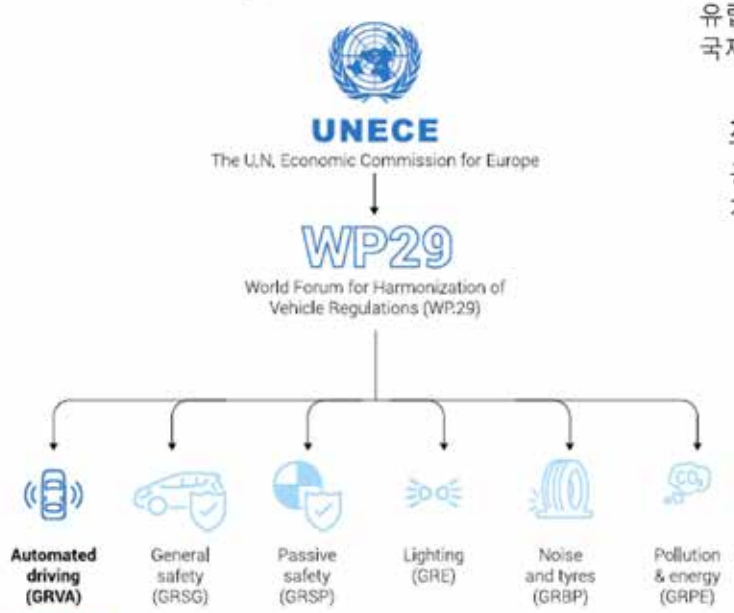
UNECE WP29 사이버보안 법규 채택

ISO/SAE DIS 21434 발간

Confidential

UNECE WP29 사이버보안 법규 - 배경

Organization of WP.29



Confidential

유럽경제위원회

유럽, 북미, 아시아의 56개 회원국을 포함하며, 지속가능한 발전과 경제적 번영, 국제 협력을 촉진하기 위한 규범, 표준 및 규약을 규정한다.

차량규정의 일치화를 위한 세계포럼

광범위한 자동차 분야에 적용되는 기술 규제를 전담하는 포럼으로, 바퀴 달린 차량과 그 서브시스템 및 부품의 안전 및 환경적 성능을 다룬다.

자동/자율 커넥티드차량 실무그룹

차량 자동화 및 연결성의 안전과 보안, ADAS, Dynamic 관련 규정 제정

UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles

Published: 25 June 2020

The automotive sector is undergoing a profound transformation with the digitalization of in-car systems that are necessary to deliver vehicle automation, connectivity and shared mobility. Today, cars contain up to 150 electronic control units and about 100 million lines of software code – four times more than a fighter jet –, projected to rise to 300 million lines of code by 2030.

This comes with significant cybersecurity risks, as hackers seek to access electronic systems and data

<그림 출처 : UNECE WP29 웹사이트>

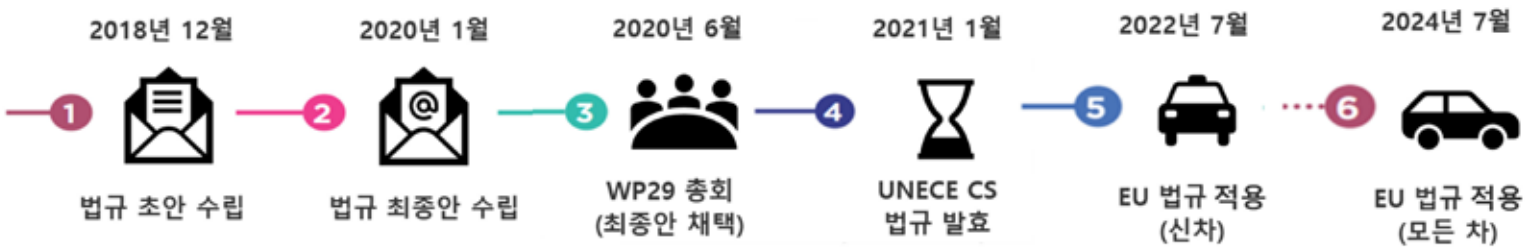
UNECE WP29 사이버보안 법규 - 개요

❑ 2개의 개별 인증으로 구성

✓ **Type Approval(형식승인)** : 차종별 보안기술의 적용과 평가결과 인증(실차, 기능 시험)

✓ **Certificate of Compliance for CSMS(사이버보안 경영시스템 인증서)** : 사이버보안 조직, R&R, 차량 수명주기에 대한 사이버보안 프로세스 인증

❑ 적용 일정



❖ 법규 채택 확정 국가 : EU 연합 참여국사, EU 법규를 따르는 일부 국가(이스라엘, 팔레스타인, 이란, 터키 등)

❖ 법규 채택 검토 국가 : 일본(2020년 발효 예정), 한국 등

UNECE WP29 사이버보안 법규 - 구조

ECE/TRANS/WP.29/2020/79 Revised

UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems

Contents

Section 1	규정 범위
Section 2	규정에 사용된 용어
Section 3-6	승인 신청, 마킹, 승인, **CSMS** 인증서
Section 7	규정의 주요 요건
Section 8	차량의 변경 및 확장
Section 9-11	생산 프로세스 상세
Section 12	승인 절차
Annex 1-4	**Section 3~6** 에 대한 상세
Annex 5	사이버 위협, 위험과 통제방안

<그림 출처 : UNECE WP29 Cybersecurity regulation>

UNECE WP29 사이버보안 법규 : Section 1~6

1. 범위(Scope)

- 차량 카테고리 M, N, O (ECU 장착시) L6, L7 (Lv.3 이상의 자율주행 기능을 장착한 경우)
  * M : 승객용 4륜차, N : 화물용 4륜차, O : 트레일러, L6 & L7 : 4륜 ATV(all terrain vehicle)

2. 정의(Definition)

- CSMS (Cybersecurity Management System) : 차량에 대한 사이버 위협과 위험을 관리하고 사이버 공격으로부터 보호하기 위한 조직적 프로세스, 책임 및 관리 시스템
- Development, Production, Post-production phase : 형식승인전 개발기간, 차량형식의 생산기간, 더 이상 생산되지 않지만 차량이 운행되는 기간
- Mitigation, Risk, Risk assessment, Risk management, Threat, Vulnerability 등 보안 용어

3. 승인 신청

- 자동차 제작사 또는 권한을 위임한 대리인이 차량 형식 승인에 대한 신청을 제출하여야 함
- **문서패키지**와 **CSMS 인증서**를 제출해야 함
  - 공식 문서 패키지는 Annex 1참조
  - 승인을 위한 적절한 점검이 이뤄질 수 있도록 충분한 정보를 제공하여야 함
  - 차량의 생산기간 종료후 최소 10년간 가용해야 함

4. 마킹

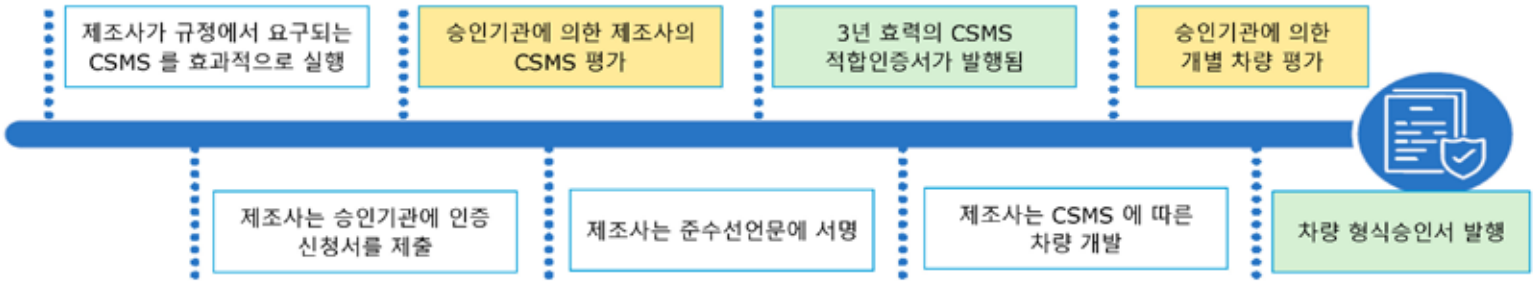
UNECE WP29 사이버보안 법규 : Section 1~6

5. 승인(Approval)

- 승인기관 혹은 기술서비스 기관은 다음 내용을 문서로 확인하고, 시험을 통해 검증하여야 함
  - Suppler 관련 위험의 식별과 관리, 위험평가, 시험결과, 완화방안 적용여부, 사이버보안 공격의 탐지와 대응, 사고조사용 데이터 포렌직 기능
  - 규정에서 언급된 보안위협에 대한 위험평가가 완전하지 않거나, 위험평가에서 고려된 위협에 대해 적절한 보안대책이 없는 경우, 혹은 보안대책의 효과성을 검증하기 위한 충분한 시험수행이 되지 않은 경우, 승인이 거부됨

6. CSMS 및 Vehicle Type 승인 프로세스

* 제조사 : 자동차 제조사



Confidential

UNECE WP29 사이버보안 법규 : Section 7

7.1 일반 사항

- 본 법규의 요구사항은 다른 UN 법규의 요구사항이나 조항을 제한하지 않음

7.2 CSMS(사이버보안 경영시스템)

* ISO 9000 정의 참조

- **경영시스템 :** 방침 및 목표를 수립하고 그 목표를 달성하기 위한 시스템)
- **사이버보안 경영시스템 : 사**이버보안에 관하여 조직을 지휘하고 관리하는 경영시스템 (품질경영시스템의 일부 혹은 독립시스템으로 구축 가능)
- **자동차 전체 수명주기(개발/생산/생산후)에 걸친 사이버보안 위험관리, 보안시험평가, 보안조치, 공격모니터링, 공급망 관리 프로세스 구축 필요**

7.3 Vehicle type(차량 형식)

* ACEA (유럽자동차제조사 협회) 참조

- 소비자용 자동차가 관련 환경, 안전 및 보안 표준을 충족하도록 보장하기 위해 사용되는 프로세스
- 자동차 제조업체와 자동차 제조업체에 관련된 부품의 공급자는 사이버보안 요건을 충족하는지 확인해야함.

UNECE WP29 사이버보안 법규 : Section 8~12

차량 형식의 변경 과 확장(Modification and extension of the vehicle type)

- 사이버보안에 영향을 미치는 모든 변경 및 관련문서가 승인기관에 제공되어야 함
- 승인기관은 기존 인증서를 유지하거나, Section 5에 따라 보완이 필요한 경우 평가 및 관련보고서를 요구할 수 있음

생산의 적합성(Conformity of production)

- 1958 협정에 따라 양산시험결과와 부속문서의 보관(생산중단후 10년을 초과하지 않음)

생산 부적합에 대한 페널티(Penalties for non-conformity of production)

- 형식승인 철회 및 그 통보와 관련된 내용

생산 중단(Production definitively discontinued)

- 생산이 단종되는 경우 계약당사자들간의 정보의 교환

승인기관과 기술서비스기관의 정보(Names and addresses of Technical Services responsible for conducting approval test, and of Type Approval Authorities)

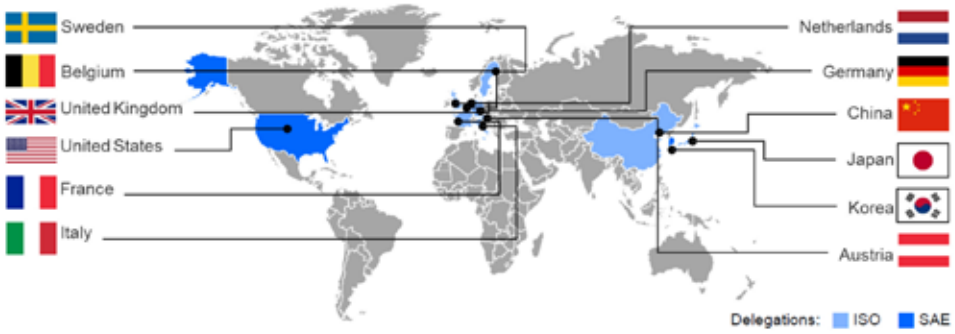
ISO/SAE 21434 : Road vehicles – Cybersecurity Engineering

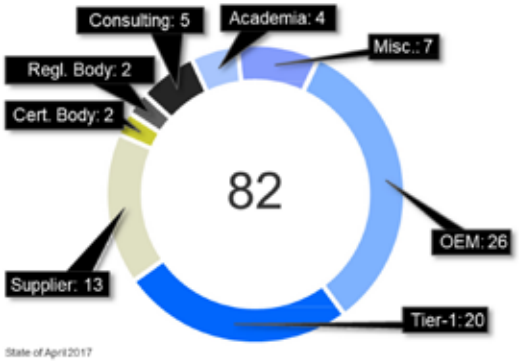
- **배경**
  - 기존의 기능안전 국제표준을 사이버보안 영역에 동일하게 적용하는데 제한이 있음
    - ✓ 모든 security critical system 이 safety critical system 은 아니며,
    - ✓ 고장이 나는 경우에도, 안전에 영향이 없는 security-critical system 이 있음

- **목표**
  - ✓ 자동차 사이어보안 엔지니어링에 대한 국제 표준 제정
  - ✓ 자동차에 적합한 사이버보안 용어를 정의
  - ✓ 자동차 사이버보안 평가에 필요한 사이버보안 프로세스 및 활동과 최소한의 요구사항을 정의
  - ✓ 자동차 산업에 적용할 수 있는 최신 수준(State of the art)의 사이버보안 엔지니어링 절차 수립
  - ✓ 추가로, 입법에 참고할 수 있을 정도의 엄격함과 법적 확실성을 보장할 것, ref. UNECE WP29 사이버보안 법규

ISO TC22/SC32/WG11 조직 구성

- **간사단**
  - ISO: Stephan Krähnert (DIN/VDA)
  - SAE: Tim Weisenberger
- **공동 의장단**
  - ISO: Dr. Gido Scharfenberger Fabian (carmeq/VW; DE)
  - SAE: Lisa Boran (Ford. Inc; US)





Confidential

ISO/SAE 21434 – 참여 기관

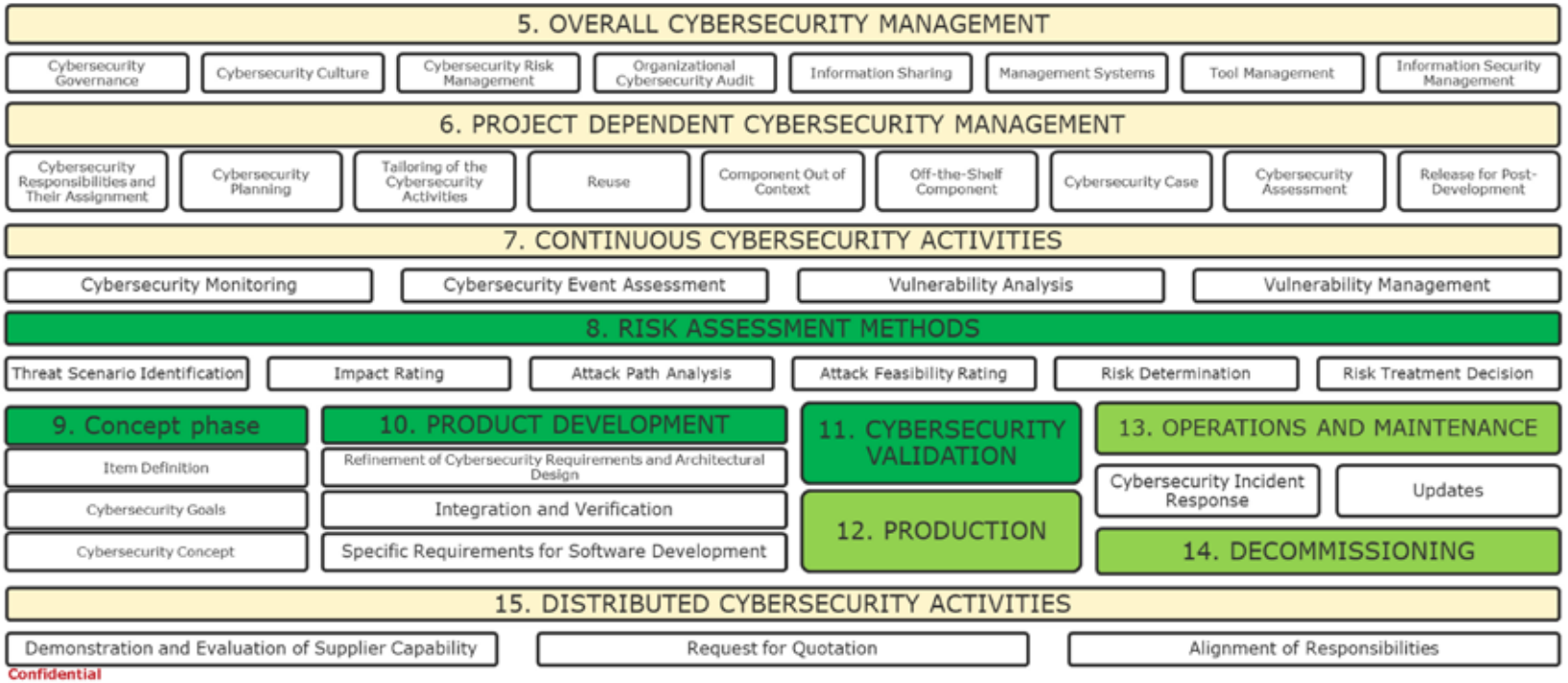
ISO/SAE 21434 – 주요 원칙

- **주요 원칙**
  - **Road vehicles** 에 적용됨
  - 합리적으로 절차에 기반하여 **안전한 자동차 시스템** 개발
  - 자동차 제조사와 부품사가 "**due diligence**" 를 보여주어야 함
  - 자동차 사이버보안 **엔지니어링**에 주안점을 둠
  - 사이어보안의 최신 기술에 **기반**
  - **위험 기반** 접근법
    - 위험 정도에 따라 우선 순위가 결정됨
    - 사이버보안 요구사항에 대한 위험 요소 분석
  - 사이버보안 **경영시스템(Management system)** 구축(관리 체계)
  - 자동차 **전체 수명주기**에 걸친 사이버보안 활동과 프로세스:
    - 설계, 구현, 생산, 운행, 정비 및 유지보수 와 폐기

- **적용 범위**
  - 도로용 자동차,
  - 도로용 자동차에 장착되는 전기전자 시스템, 부품과 소프트웨어,
  - 외부 장비/네트워크와의 연결(접속)되는 경우

- **아래의 내용은 다루지 않음**
  - 특정한 사이버보안 기술과 해법
  - 특정한 개선 방안에 대한 요구사항
  - 통신 시스템에 대한 요구사항
  - 특정 통신서비스 및 그 제공기관에 대한 요구사항
  - 전기차 충전에 대한 요구사항
  - 자율주행자동차 기술에 대한 특정한 요구사항

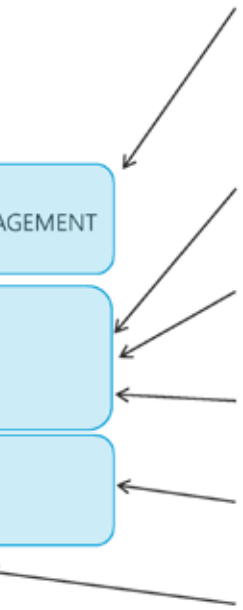
ISO/SAE DIS 21434 구조



Confidential

ISO/SAE DIS 21434 – 조항

- 1. SCOPE(범위)
- 2. NORMATIVE REFERENCES(참조규범)
- 3. TERMS AND ABBREVIATIONS(용어와 약어)
- 4. GENERAL CONSIDERATIONS(일반 사항)
- 5. OVERALL CYBERSECURITY MANAGEMENT
- 6. PROJECT DEPENDENT CYBERSECURITY MANAGEMENT
- 7. CONTINUOUS CYBERSECURITY ACTIVITIES
- 8. RISK ASSESSMENT METHODS
- 9. CONCEPT PHASE
- 10. PRODUCT DEVELOPMENT
- 11. CYBERSECURITY VALIDATION
- 12. PRODUCTION
- 13. OPERATIONS AND MAINTENANCE
- 14. DECOMMISSIONING
- 15. DISTRIBUTED CYBERSECURITY ACTIVITIES
- ANNEX A-J (참고 정보)



사이버보안 경영시스템
- 기업(회사) 레벨의 관리
- 엔지니어링 단계별 세부 활동
- 자동차 전체 수명주기에 사이버보안 활동

사이버보안 위험 분석, 평가 및 관리 방법론

사이버보안 컨셉 활동 (사이버보안 목표 수립, 설계 방안 수립)

사이버보안 엔지니어링 개발 단계(시스템, 하드웨어, 소프트웨어 수준)

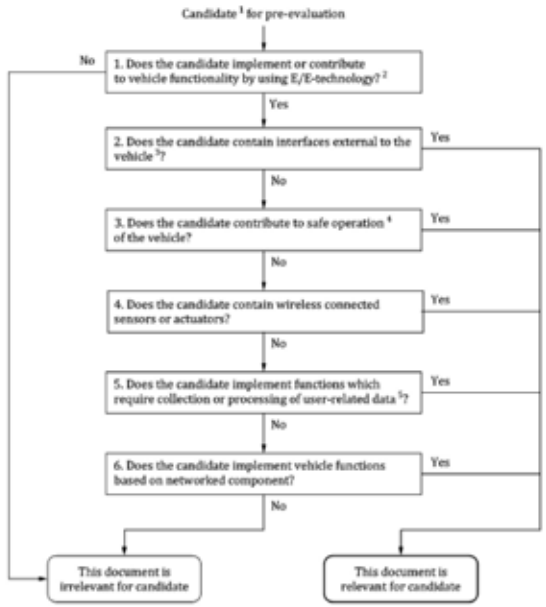
생산 및 사후 단계(생산, 운용, 사후지원, 폐기)의 사이버보안 활동

OEM 과 부품업체(TIER1,2,...)간 사이버보안과 관련된 상호협업 및 책임, 권한에 대해서 정의

ISO/SAE DIS 21434 – Annex 구성

Annex A	사이버보안 활동과 작업 산출물 요약	단계별 사이버보안 활동과 결과(작업 산출물)
Annex B	사이버보안 문화 사례	사이버보안 문화의 좋은 사례와 나쁜 사례
Annex C	사이버보안 협약서 양식 사례	제조사/부품공급사들간의 사이버보안 활동 및 각 역할
Annex D	사이버보안 적CYBERSECURITY 관련성 : 사례 및 기준	사이버보안 적용여부를 결정하기 위한 기준 질문
Annex E	사이버보안 보증 수준 (CAL)	ASIL 과 유사한 개념인 CAL 의 결정방법과 CAL 등급별 요구되는 개발방법론
Annex F	검증과 타당성확인 (V&V)	사이버보안 개발 활동에서 수행되는 검증방안(검토, 분석, 시험 등) 과 타당성확인 방안
Annex G	사용사례와 작업산출물 예시 : 헤드램프 시스템	사이버보안 엔지니어링 표준 적용 사례 : 헤드램프 시스템
Annex H	안전, 재무, 운용, 사생활 손상의 영향 등급	사이버보안 위험평가시 사용되는 영향 등급의 기준 사례
Annex I	공격 가능성 등급을 결정하기 위한 지침	공격가능성 등급의 기준
Annex J	위험 판정을 위한 기준	위험 등급을 결정하기 위한 기준표 사례

핵심 내용 1 : 사이버보안 적용여부 검토



사이버보안 적용여부 검토기준

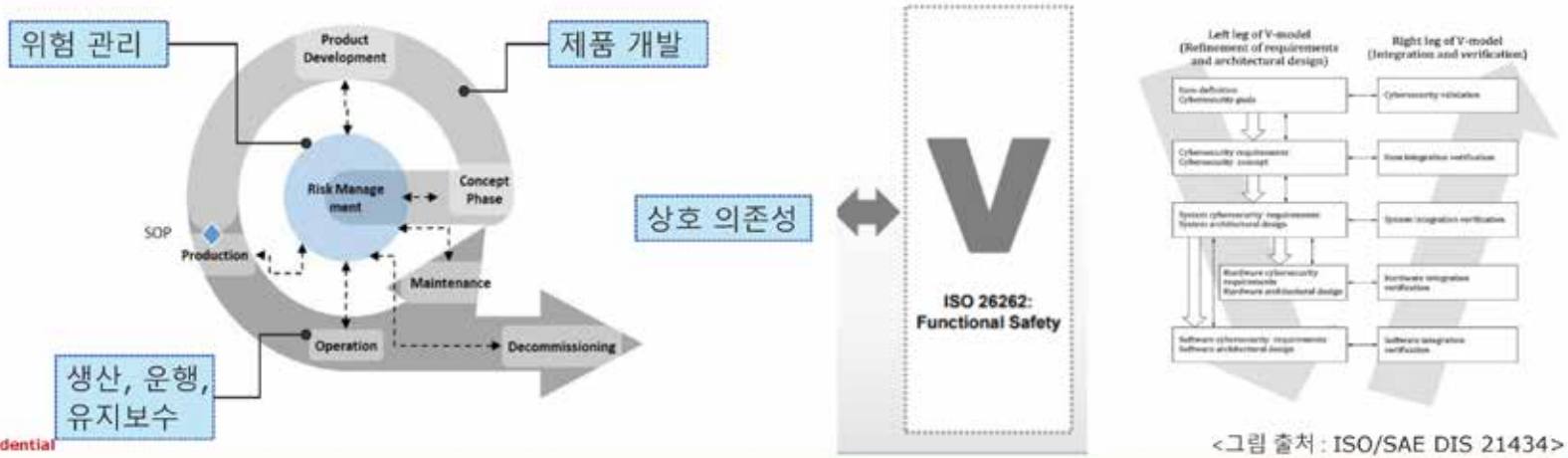
1. 전기전자 기술을 활용한 기능을 구현하는지?
2. 자동차 외부와 인터페이스를 보유하는지?
3. 자동차의 안전한 운행과 관련있는지?
4. 무선으로 연결된 센서 혹은 엑츄에이터가 있는지?
5. 사용자정보의 수집 혹은 처리를 위한 기능이 있는지?
6. 네트워크에 연결되어 기능이 구현되는지?

→ 위의 질문에 하나라도 "**예**"에 해당이 된다면 사이버보안 국제표준을 적용하여 개발해야 함

<그림 출처 : ISO/SAE DIS 21434>

핵심 내용 2 : 위험기반 엔지니어링 & 수명주기 적용

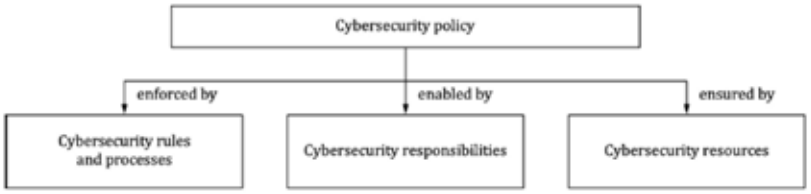
- **위험 관리**는 사이버보안 엔지니어링의 핵심 활동
  - 사이버보안 엔지니어링의 최종 목표는 사이버보안 위협 & 공격으로 인한 **위험을 최소화**, 수용가능한 수준으로 줄이는 것
  - 공격기술의 발전에 따른 지속적으로 위험을 관리하기 위한 **지속적인 프로세스**로 실행 필요
  - 제품 개발 단계별로 **Vulnerability Analysis(취약점 분석)** 을 수행함으로써 추가적인 위협이 없다는 것을 보장해야 함



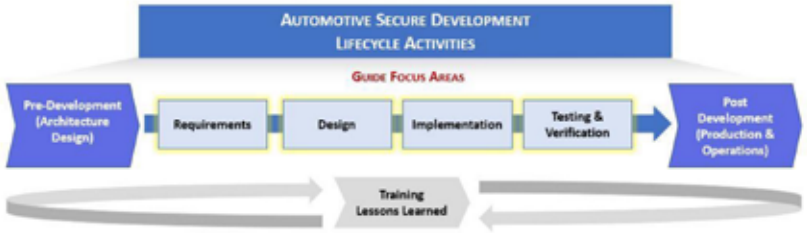
<그림 출처 : ISO/SAE DIS 21434>

핵심 내용 3 : 사이버보안 관리 체계 구축

- 사이버보안 거버넌스, 정책, 문화 및 경영시스템(Cyber Security Management System) 수립
- 정보공유, Tool 관리(시험, 플래시프로그래밍, 포렌식 등), ISMS 등 지원프로세스 구축
- 심사(Audit), 평가(Assessment), 사이버보안 최종 보고서(Cybersecurity case) 발행
- 책임과 권한 (R&R), 취약점 분석 및 관리 방안 필요
- 기능안전, 기존 IT 보안과 사이버보안의 상호 작용에 대해서 설명



<사이버보안 거버넌스 수립>



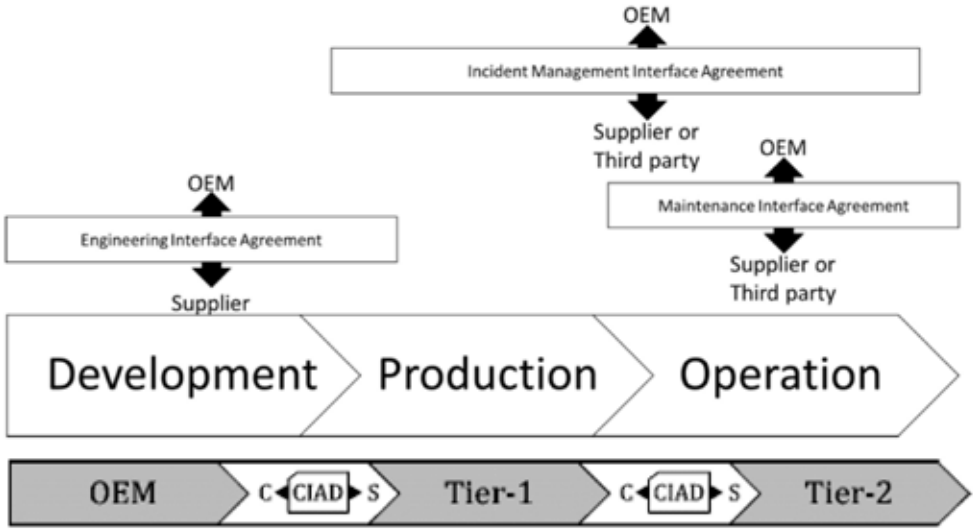
<사이버보안 적용 자동차 개발절차>

Confidential

<그림 출처 : ISO/SAE DIS 21434, AUTO-ISAC Best practices>

핵심 내용 4 : 공급망 사이버보안 관리

- "사이버보안 개발협약"을 통해 자동체 제조사 와 부품개발사 혹은 IT 서비스 제공사와의 업무 역할 정의
- 자동차 제조사뿐만 아니라, 공급업체(Tier1, 2 …)의 사이버보안 관리 체계를 요구



<그림 출처 : ISO/SAE DIS 21434>

요약

- 차량 형식

- 사이버보안 경영시스템

Confidential

감사합니다!!

윤세욱 위원
Se.wook.yoon@dnvgl.com
010-6304-2454

www.dnvgl.com

SAFER, SMARTER, GREENER

Confidential