[1.5] CSMS Tool 관리 (CSMS Tool Management)

이름	E-mail	Version	Revision Date	개정 내용
송경수	aromi.song@lge.com	v1.0	2024.04.04	CSMS Tool Management 관련 사항 변경 ISO21434 기반한 CSMS Tool Management Rationale 정리
김정묵	jeongmook.kim@lge.com	v1.1	2024-07-12	Security measure, Additional Security measure, Tool Operating Environment 필드 추가
김정묵	jeongmook.kim@lge.com	v1.2	2026-01-06	공동 Flashing Tool(QFIL) 추가 JRL Diagnostic Tool(Corvus, DDAT) 추가 현대 Diagnostic Tool(DiVE), Flashing Tool(DiVEH-OTA studio) 추가

ENG

Response to CSMS Tool Management-related matters	
1) CSMS Tool Management	2) Rationale

ISO/SAE 21434:2021(E) **5.4.5 Tool management** [RQ-05-14] Tools that can influence the cybersecurity of an item or component shall be managed. Example 1 Tools used for concept or prodcut development , such as model based development , static checkers , verification tools. Example 2 Tools used during production such as a flash writer , end of line tester. Example 3 Tools used for maintenance , such as an on-board diagnostic tool or reprogramming tool. NOTE such management can be established by: – application of the user manual with errata; – protection against unintended usage or action; – access control for the tool users; and/or – authentication of the tool [RC-05-15]An appropriate environment to support remedial actions for cybersecurity incidents (see 13.3) should be reproducible until the end of cybersecurity support for the product. Example 4 testing , software build and development environments for reproducing and managing vulnerability Example 5 Toolchain and compilers used for building the software of the product **summary in TUV** "Tool management" is independent from "tool assessment" known from functional safety. ***In CS there is neither a classification nor any requirements related to development tools.*** Which tools shall be managed? Obey the user manual of the tool Assign a responsible role for each tool Make sure that only authorized/trained personnel uses the tool Is an update to the latest version meaningful? When to apply the update?	◆ ISO/SAE 21434:2021(E) states that tools that can affect the cybersecurity of items or components must be managed. ([RQ-05-14] Tools that can influence the cybersecurity of an item or component shall be managed.) ◆ Therefore, listing all tools and first identifying whether they are tools that can affect cybersecurity is tool management referred to in ISO/SAE 21434:2021(E). ◆ Such TOOLs can be distinguished through the following examples. Example 1 Tools used for concept or prodcut development , such as model based development , static checkers , verification tools. Example 2 Tools used during production such as a flash writer , end of line tester. Example 3 Tools used for maintenance , such as an on-board diagnostic tool or reprogramming tool. refer to ISO/SAE 21434:2021(E) ◆ It is stated that such management can be established by: – application of the user manual with errata; – protection against unintended usage or action; – access control for the tool users; and/or – authentication of the tool When a response request is made for each model, the response is as follows: ① Tool list up for each model based on the above-mentioned standards Example 1, Example 2, Example 3 ② Specify manual information about the tool in the manual field. ③ Protection against unintended use or behavior or access control for tool users is replaced by: ▶ https://sp.lge.com/index We are operating a new security portal system ==> Physical access authority control through ID card and visit application ==> Control technical and administrative access rights through asset export and asset management ==> Network access permission control ==> Control access rights for asset import and export through PC PLUS installation ▶ ACCESS control through TISAX and ISO27001 certification already obtained by LG Electronics ④ Please fill in the part about tool certification as it is one of them.

3) improvement plan	4) Collab updated by	5) Collab updated at
Refer to "2) Rationale "	kyungsoo Song	2024/04/04
6) Model FU History	Renault CDC , JLR Telematics EVAC	

KOR

CSMS Tool Management 관련 사항에 대한 대응	
1) CSMS Tool Management	2) Rationale

<통제 기준> **ISO/SAE 21434:2021(E)** **5.4.5 Tool management** [RQ-05-14] Tools that can influence the cybersecurity of an item or component shall be managed. ISO/SAE 21434:2021(E)에서는 품목이나 구성요소의 사이버 보안에 영향을 미칠 수 있는 Tool 은 관리해야 한다고 나와있음.. Example 1 Tools used for concept or prodcut development , such as model based development , static checkers , verification tools. Example 2 Tools used during production such as a flash writer , end of line tester. Example 3 Tools used for maintenance , such as an on-board diagnostic tool or reprogramming tool. NOTE such management can be established by: – application of the user manual with errata; – protection against unintended usage or action; – access control for the tool users; and/or – authentication of the tool [RQ-05-15]An appropriate environment to support remedial actions for cybersecurity incidents (see 13.3) should be reproducible until the end of cybersecurity support for the product. Example 4 testing , software build and development environments for reproducing and managing vulnerability Example 5 Toolchain and compilers used for building the software of the product **<발견 사실>** **summary in TUV** "Tool management" is independent from "tool assessment" known from functional safety. ***<u>In CS there is neither a classification nor any requirements related to development tools.</u>*** "Tool 관리"는 기능 안전에서 알려진 "Tool 평가"와는 별개입니다. CS에는 개발 도구와 관련된 분듀나 요구 사항이 없습니다. Which tools shall be managed? Obey the user manual of the tool Assign a responsible role for each tool Make sure that only authorized/trained personnel uses the tool Is an update to the latest version meaningful? When to apply the update?	◆ ISO/SAE 21434:2021(E)에서는 품목이나 구성요소의 사이버 보안에 영향을 미칠 수 있는 Tool 을 관리해야 한다고 나와있음 ([RQ-05-14] Tools that can influence the cybersecurity of an item or component shall be managed.) ◆ 따라서 전체 Tool 리스트업을 하고 사이버 보안에 영향을 미칠 수 있는 Tool 인지 먼저 식별하는 것이 ISO/SAE 21434:2021(E) 에서 말하는 Tool management 임 ◆ 그런 TOOL 들은 다음과 같은 예시도 구별해볼 수 있음 예 1 모델 기반 개발, 정적 검사기, 검증 도구와 같은 concept 단계 또는 제품 개발 단계에 사용되는 도구입니다. 예 2 플래시 라이터, EOL 테스터 등 생산 중에 사용되는 도구. 예 3 온보드 진단 도구 또는 재프도그래밍 도구와 같은 유지 관리에 사용되는 도구입니다. ISO/SAE 21434:2021(E) Example 1 Tools used for concept or prodcut development , such as model based development , static checkers , verification tools. Example 2 Tools used during production such as a flash writer , end of line tester. Example 3 Tools used for maintenance , such as an on-board diagnostic tool or reprogramming tool. ◆ 그러한 관리는 다음은 동해 확립될 수 있다(can be established)고 나와 있음 사용자 설명서 (user manual)의 적용 의도하지 않은 사용이나 행동에 대한 보호 도구 사용자에 대한 접근 제어 도구 인증 NOTE such management can be established by: – application of the user manual with errata; – protection against unintended usage or action; – access control for the tool users; and/or – authentication of the tool 모델별도 대응 요청이 올 경우 다음과 같이 대응함 ① 위의 언급된 기준 예1 , 예2 예3 에 의거하여 각 모델별 Tool list up 은 함 ② Tool 에 대한 manual 정보를 manual 필드에 명시함 ③ 의도하지 않은 사용이나 행동에 대한 보호 or 도구 사용자에 대한 접근 제어 는 다음으도 같음함 ▶ https://sp.lge.com/index new security portal system 은 운영하고 있음 ==> ID 카드 및 방문 신청을 동해서 물리적 촌입 권한 동제 ==> 자산 반촏 및 자산 관리를 동한 기술적 , 관리적 접근 권한 동제 ==> 네트워크 접근 권한 동제 ==> PC PLUS 설치를 동한 자산 반입촏에 대한 접근권한 동제 ▶ LG전자가 기 획득한 TISAX , ISO27001 인증은 동한 ACCESS control ④ 도구 인증 에 대한 부분은 one of them 이기 때문에 있다면 기입

3) 개선계획	4) Collab update 담당자	5) Collab update 이행 일자
Tool Management 관련 대응에 2) Rationale 를 동해서 수립	송경수	2024/04/04
6) 모델 FU 이행 이력	Renault CDC , JLR Telematics EVAC	

Tool List

정의 : 중요 보안 자산이 송수신 되는 Tool , 취약점 점검 Tool

Security Asset(중요보안 자산) : 바이너리, Key, 인증서

Criteria: Tools accessible to critical security assets

Cybersecurity Tools

Category 정의

- Qualification Test : 취약점 점검/ 개발 사이버보안 테스트 툴
- Diagnostic Tool : 진단 수행/진단 테스트 툴
- Flashing Tool : 바이너리 다운로드 툴
- Production : 생산 관련 툴

Category	Tool Name	Objectives	Version	Manufacturer	Manual	Unit (Responsible organization)	Tool Operating Environment	Security measure	additional Security measure	Result (Security measure is acceptable?)

Qualification Test	BDBA	To Scan Open source software vulnerability	2021.12.01	Sypnopsys	http://ossvs.lge.com:8080/static/docs/user-guide/index.html	CSAU	• Tool 전용 PC 사용 • 별도 CS 실험실 내 위치 • 사내 별도 공간에 서버 이용 ------- English------- • Use a PC dedicated to the tool • Located in a separate CS lab • Separate server existence	• 물리적 접근권한 통제 ==> 신분증 ID Card tagging 및 방문신청은 통한 물리적 접근 통제 • 기술 및 네트워크 접근권한 통제 ==> PC PLUS (사내 방화벽) 설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • 관리적 접근 권한통제 ==> 자산 반입 및 자산 관리를 통해 접근 통제 • ID/PW 으로 인증(등록된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import • ID/PW authentication (registered ID)		Yes

Qualification Test	PSA	To Scan Open source software vulnerability	v2.37	Cybellum	https://cybellum.my.site.com/CustomerPortal/s/	CSAU	• 사내 별도 공간에 서버 이용 • 사이트에 접속해 실행 ------- English------- • Separate server existence • Access and operate the site	• 물리적 접근권한 통제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근통제 • 기술 및 네트워크 접근권한 통제 ==> PC PLUS (사내 방화벽) 설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한은 제어 • ID/PW 으로 인증(등록된 아이디) ---------- English---------- -- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • ID/PW authentication (registered ID)		Yes

Qualification Test	Defensics	Fuzz test	2023.12.0	Sypnopsys	https://community.synopsys.com/s/article/Defensics-User-Guide-Version-2021-12-0	CSAU	• Tool 전용 PC 사용 • 별도 CS 실험실 내 위치 ------- English------- • Use a PC dedicated to the tool • Located in a separate CS lab	• 물리적 접근권한 통제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근 통제 • 기술 및 네트워크 접근권한 통제 ==> PC PLUS (사내 방화벽) 설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • 관리적 접근 권한통제 ==> 자산 반입 및 자산 관리를 통해 접근 통제 ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import		Yes

Qualification Test	Canoe	CAN signal trriger and CAN communication test	12.0	Vector	https://www.vector.com/kr/ko/search?type=%5B%22downloads%22%5D&page=1&q=VN5610&pageSize=50&sort=date&order=desc&	Validation Environment Unit	• 별도 실험실에 위치 • 장비를 등 독해 라이센스 유/무도 동작 ------- English------- • Located in a separate lab • Operating with or without a license on registered devices	• 물리적 접근권한 동제 ==> 신분증 ID Card tagging 및 방문신청은 동한 물리적 접근 동제 • 기술 및 네트워크 접근권한 동제 ==> PC PLUS (사내 방화벽) 설치를 동해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • 관리적 접근 권한동제 ==> 자산 반입 및 자산 관리를 동해 접근 동제 ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import		Yes

Qualification Test	Coverity	Static Analysis	2022.3.0	Synopsys	http://collab.lge.com/main/x/Lx7JX	DevOps Unit	• 별도 실험실에 위치 • Tool 전용 PC 사용 ------- English------- • Located in a separate lab • Use a PC dedicated to the tool	• 물리적 접근권한 통제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근 통제 • 기술 및 네트워크 접근권한 통제==> PC PLUS (사내 방화벽) 설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • 관리적 접근 권한통제 ==> 자산 반입 및 자산 관리를 통해 접근 통제 • ID/PW 으로 인증(등록된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import • ID/PW authentication (registered ID)	Z10 16 05 95863 001.pdf ==> ISO 26262 인증	Yes

Qualification Test	Protex	Scanning source code to find OSS information	7.8.6	Synopsys	protex identification guide.docx	DevOps Unit	• 별도 실험실에 위치 • Tool 전용 PC 사용 ------- English------- • Located in a separate lab • Use a PC dedicated to the tool	• 물리적 접근권한 통제 ==> 신분증 ID Card tagging 및 방문신청 은 동한 물리적 접근 동제 • 기술 및 네트워크 접근권한 통제==> PC PLUS (사내 방화벽) 설치를 동해 자산 가져오기 및 내보내기에 대한 접근 권한은 제어 • 관리적 접근 권한동제 ==> 자산 반입 및 자산 관리를 동해 접근 동제 • ID/PW 으도 인증(등독된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import • ID/PW authentication (registered ID)		Yes

Qualification Test	VulDOC Privacy and Credential Analyzer	scanning Privacy and Credential	1.6.0	LGE	http://collab.lge.com/main/x/7QlmmQ	CTO CSG TASK	• 사내 별도 공간에 서버 이용 • 사이트에 접속해 실행 ------- English------- • Separate server existence • Access and operate the site	• 물리적 접근권한 통제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근 통제 • 기술 및 네트워크 접근권한 통제 ==> PC PLUS (사내 방화벽) 설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • ID/PW 으로 인증(등록된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • ID/PW authentication (registered ID)		Yes
Flashing Tool	QFIL	Flashing device in low level	QPST 2.0.2.3	Qulaocmm	https://createpoint.qti.qualcomm.com/	Project Team	• Tool 전용 PC 사용 ------- English------- • Use a PC dedicated to the tool	• 기술 및 네트워크 접근권한 통제 ==> PC PLUS (사내 방화벽) 설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 ---------- English---------- • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall)		

Production	GMES	Production Data Management	1.0	LGE	http://gmes.lge.com/	VS Smart Factory Team	• 별도 공간에 서버 이용 • 사이트에 접속해 실행 ------- English------- • Separate server existence • Access and operate the site	• 물리적 접근권한 통제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근 통제 • 기술 및 네트워크 접근권한 통제 ==> PC PLUS (사내 방화벽) 설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • ID/PW 으로 인증(등록된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • ID/PW authentication (registered ID)		Yes
Production	Data management Software (DMS	ROM Writing	2.3.5	Data I/O	https://www.dataio.com/Support/LumenX-Release	Production Team	Tool 전용 PC 사용 SMT제조계 별도 R/W실 내 위치 사내 별도 공간에 서버 이용 ------- English------- Use a PC dedicated to the tool Located in a separate R/W area(SMT Manufacturing Section) Separate server existence	물리적 접근권한 통제 ==> SMT제조계 출입 시 신분증 ID Card tagging 및 통한 물리적 접근통제(SMT제조계 구성원) ---------- English---------- Physical access rights control ==> Physical access control (SMT Manufacturing Section) through ID card tagging (Only for SMT Manufacturing Section Member)		Yes

Production	Tasklink	ROM Writing	9.31	Data I/O	https://www.dataio.com/Support/Resources-Library	Production Team	TOOL 전용 소프트웨어 사용 별도 운용 서버(NAS)에서 Data File 관리 ------- English------- Use TOOL-only software Managing Data Files on a Separate Operational Server (NAS)	물리적 접근권한 통제 ==> TOOL 전용 소프트웨어 계정 설정으로 접근 권한 제한 기술 및 네트워크 접근권한 통제 ==> 사내망으로 접근가능한 NAS 서버에서 Data File을 사용, Tool 전용 SW 사용으로 외부 조작 불가 ---------- English---------- Physical Access Control ==> Limit access to TOOL-only software account settings Control technical and network access rights ==> Using Data File on NAS servers accessible to the in-house network, external manipulation is not possible using tool-only SW		Yes
Production	FA & FCT Inspection Program	Inspection of product	프로젝트명_날짜	Moohan tech	http://www.moohantech.biz/bbs/board.php?bo_table=02_board	Inspection Technology Team	TOOL 전용 소프트웨어 사용 별도 운용 서버(GMES SWP)에서 Data File 관리 ------- English------- Use TOOL-only software Managing Data Files on a Separate Operational Server (GMES SWP)	물리적 접근권한 통제 ==> TOOL 전용 소프트웨어 계정 설정으로 접근 권한 제한 기술 및 네트워크 접근권한 통제 ==> 사내망으로 접근가능한 GMES SWP 서버를 사용, Tool 전용 SW 사용으로 외부 조작 불가 ---------- English---------- Physical Access Control ==> Limit access to TOOL-only software account settings Control technical and network access rights ==> Using GMES SWP servers accessible to the in-house network, external manipulation is not possible using tool-only SW		Yes

Process	Tool Name	Objectives	Version	Manufacturer	Manual	Unit (Responsible organization)	Tool Operating Environment	Security measure	additional Security measure	Result (Security measure is acceptable?)

Management	Codebeamer	process management		PTC	https://codebeamer.com/cb/login.spr	IT Team	• LG 전용 Cloud 서버 이용 ------- English------- • Using LG's dedicated cloud servers	• 클라우드 네트워에서 사용자 인증 및 VPC 접근 동제 • 승인된 사용자에게만 접근권한 부여 • ID/PW 으도 인증 ---------- English---------- • User authentication and VPC access control in the cloud network • Provide access only to authorized users • ID/PW authentication	인증_CodeBeamer_TV-Zertifikat-Intland_codeBeamer_8.0.0_EN_V0_1(1).pdf	Yes
Qualification Test	BDBA	To Scan Open source software vulnerability	2021.12.01	Sypnopsys	http://ossvs.lge.com:8080/static/docs/user-guide/index.html	CSAU	• Tool 전용 PC 사용 • 볃도 CS 실험실 내 위치 • 사내 볃도 공간에 서버 이용 ------- English------- • Use a PC dedicated to the tool • Located in a separate CS lab • Separate server existence	• 뭍리적 접근권한 동제 ==> 신분증 ID Card tagging 및 방문신청을 동한 뭍리적 접근동제 • 기술 및 네트워크 접근권한 동제 ==> PC PLUS (사내 방화벽)설치를 동해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • 관리적 접근권한동제 ==> 자산 반입 및 자산 관리를 동해 접근 동제 • ID/PW 으도 인증(등독된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import • ID/PW authentication (registered ID)		Yes

Qualification Test	PSA	To Scan Open source software vulnerability	v2.31	Cybellum	https://cybellum.my.site.com/CustomerPortal/s/	CSAU	• 사내 별도 공간에 서버 이용 • 사이트에 접속해 실행 ------- English------- • Separate server existence • Access and operate the site	• 물리적 접근권한 동제 ==> 신분증 ID Card tagging 및 방문신청은 동한 물리적 접근동제 • 기술 및 네트워크 접근권한 동제 ==> PC PLUS (사내 방화벽)설치를 동해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • ID/PW 으도 인증(등독된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • ID/PW authentication (registered ID)		Yes

Qualification Test	Defensics	Fuzz test	2023.9.5	Sypnopsys	https://community.synopsys.com/s/article/Defensics-User-Guide-Version-2021-12-0	CSAU	• Tool 전용 PC 사용 • 별도 CS 실험실 내 위치 ------- English------- • Use a PC dedicated to the tool • Located in a separate CS lab	• 물리적 접근권한 동제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근동제 • 기술 및 네트워크 접근권한 동제 ==> PC PLUS (사내 방화벽)설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • 관리적 접근권한동제 ==> 자산 반입 및 자산 관리를 통해 접근 동제 ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import		Yes

Qualification Test	Canoe	CAN signal trriger and CAN communication test	12.0	Vector	https://www.vector.com/kr/ko/search?type=%5B%22downloads%22%5D&page=1&q=VN5610&pageSize=50&sort=date&order=desc&	Validation Environment Unit	• 별도 실험실에 위치 • 장비를 등록해 라이센스 유/무도 동작 ------- English------- • Located in a separate lab • Operating with or without a license on registered devices	• 물리적 접근권한 동제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근동제 • 기술 및 네트워크 접근권한 동제 ==> PC PLUS (사내 방화벽)설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • 관리적 접근권한동제 ==> 자산 반입 및 자산 관리를 통해 접근 동제 ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import		Yes

Qualification Test	Coverity	Static Analysis	2022.3.0	Synopsys	http://collab.lge.com/main/x/Lx7JX	DevOps Unit	• 별도 실험실에 위치 • Tool 전용 PC 사용 ------- English------- • Located in a separate lab • Use a PC dedicated to the tool	• 물리적 접근권한 동제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근동제 • 기술 및 네트워크 접근권한 동제==> PC PLUS (사내 방화벽)설치를 통해 자산 가져오기 및 내보내기에 대한 접근권한을 제어 • 관리적 접근권한동제 ==> 자산 반입 및 자산 관리를 통해 접근 동제 • ID/PW 으로 인증(등록된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import • ID/PW authentication (registered ID)	Z10 16 05 95863 001.pdf ==> ISO 26262 인증	Yes

Implementation	Protex	Scanning source code to find OSS information	7.8.6	Synopsys	protex identification guide.docx	DevOps Unit	• 별도 실험실에 위치 • Tool 전용 PC 사용 ------- English------- • Located in a separate lab • Use a PC dedicated to the tool	• 물리적 접근권한 동제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근동제 • 기술 및 네트워크 접근권한 동제==> PC PLUS (사내 방화벽)설치를 통해 자산 가져오기 및 내보내기에 대한 접근권한을 제어 • 관리적 접근권한동제 ==> 자산 반입 및 자산 관리를 통해 접근 동제 • ID/PW 으로 인증(등록된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • Technical and administrative access authority control ==> Access control through asset import • ID/PW authentication (registered ID)		Yes

Qualification Test	VulDOC Privacy and Credential Analyzer	scanning Privacy and Credential	1.6.0	LGE	http://collab.lge.com/main/x/7QlmmQ	CTO CSG TASK	• 사내 별도 공간에 서버 이용 • 사이트에 접속해 실행 ------- English------- • Separate server existence • Access and operate the site	• 물리적 접근권한 동제 ==> 신분증 ID Card tagging 및 방문신청을 동한 물리적 접근동제 • 기술 및 네트워크 접근권한 동제 ==> PC PLUS (사내 방화벽)설치를 동해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • ID/PW 으로 인증(등록된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • ID/PW authentication (registered ID)		Yes
Flashing Tool	QFIL	Flashing device in low level	QPST 2.0.2.3	Qulaocmm	https://createpoint.qti.qualcomm.com/	Project Team	• Tool 전용 PC 사용 ------- English------- • Use a PC dedicated to the tool	• 기술 및 네트워크 접근권한 동제 ==> PC PLUS (사내 방화벽)설치를 동해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 ---------- English---------- • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall)		

Production	GMES	Production Data Management	1.0	LGE	http://gmes.lge.com/	VS Smart Factory Team	• 별도 공간에 서버 이용 • 사이트에 접속해 실행 ------- English------- • Separate server existence • Access and operate the site	• 물리적 접근권한 동제 ==> 신분증 ID Card tagging 및 방문신청을 통한 물리적 접근동제 • 기술 및 네트워크 접근권한 동제 ==> PC PLUS (사내 방화벽)설치를 통해 자산 가져오기 및 내보내기에 대한 접근 권한을 제어 • ID/PW 으로 인증(등록된 아이디) ---------- English---------- • Physical access rights control ==> Physical access control through ID card tagging and visit application • Network access control ==> Control access to asset import and export by installing PC PLUS (in-house firewall) • ID/PW authentication (registered ID)		Yes
Production	Data management Software (DMS	ROM Writing	2.3.5	Data I/O	https://www.dataio.com/Support/LumenX-Release	Production Team	Tool 전용 PC 사용 SMT제조계 별도 R/W실 내 위치 사내 별도 공간에 서버 이용 ------- English------- Use a PC dedicated to the tool Located in a separate R/W area(SMT Manufacturing Section) Separate server existence	물리적 접근권한 동제 ==> SMT제조계 출입 시 신분증 ID Card tagging 및 동한 물리적 접근동제 (SMT제조계 구성원) ---------- English---------- Physical access rights control ==> Physical access control (SMT Manufacturing Section) through ID card tagging (Only for SMT Manufacturing Section Member)		Yes

Production	Tasklink	ROM Writing	9.31	Data I/O	https://www.dataio.com/Support/Resources-Library	Production Team	TOOL 전용 소프트웨어 사용 별도 운용 서버(NAS)에서 Data File 관리 ------- English------- Use TOOL-only software Managing Data Files on a Separate Operational Server (NAS)	물리적 접근권한 동제 ==> TOOL 전용 소프트웨어 계정 설정으로 접근 권한 제한 기술 및 네트워크 접근권한 동제 ==> 사내망으로 접근가능한 NAS 서버에서 Data File을 사용, Tool 전용 SW 사용으로 외부 조작 불가 ---------- English---------- Physical Access Control ==> Limit access to TOOL-only software account settings Control technical and network access rights ==> Using Data File on NAS servers accessible to the in-house network, external manipulation is not possible using tool-only SW		Yes
Production	FA & FCT Inspection Program	Inspection of product	프로젝트명_날짜	Moohan tech	http://www.moohantech.biz/bbs/board.php?bo_table=02_board	Inspection Technology Team	TOOL 전용 소프트웨어 사용 별도 운용 서버(GMES SWP)에서 Data File 관리 ------- English------- Use TOOL-only software Managing Data Files on a Separate Operational Server (GMES SWP)	물리적 접근권한 동제 ==> TOOL 전용 소프트웨어 계정 설정으로 접근 권한 제한 기술 및 네트워크 접근권한 동제 ==> 사내망으로 접근가능한 GMES SWP 서버를 사용, Tool 전용 SW 사용으로 외부 조작 불가 ---------- English---------- Physical Access Control ==> Limit access to TOOL-only software account settings Control technical and network access rights ==> Using GMES SWP servers accessible to the in-house network, external manipulation is not possible using tool-only SW		Yes

HKMC

Category	Tool Name	Objectives	Version	Manufacturer	Manual	Unit (Responsible organization)	Result (Security measure is acceptable?)
Diagnostic Tool	DiVE	진단 수행/진단 테스트 툴	1.33	테크웨이즈	DiVE_Manual v1_3_251203.pdf	진단사용하는 Unit (MCU, VNU)	OK
Flashing Tool	H-OTA studio	바이너리 다운로드 툴	2511N01	GIT	[kor]H-OTA Studio GEN2 Manual_20240314.pdf	OTA 사용 Unit (MCU, OTA)	OK

JLR

Category	Tool Name	Objectives	Version	Manufacturer	Manual	Unit (Responsible organization)	Result (Security measure is acceptable?)
Diagnostic Tool	Corvus	Diagnostic feature and udpate test	V2.7.0.15 RC5	JLR	http://collab.lge.com/main/display/TCUA/Util	MCU SW1 UNIT	OK
Diagnostic Tool	DDAT	Diagnostic feature management	V3.4.0.0	JLR	JLRE-ODXType1Installation-UserManual-070223-1021-1010.pdf	MCU SW1 UNIT	OK

Honda

Category	Tool Name	Objectives	Version	Manufacturer	Manual	Unit (Responsible organization)	Result (Security measure is acceptable?)