bitkom VDMA ZVEI: Die Elektroindustrie

인더스트리 4.0 실현 전략

「플랫폼 인더스트리 4.0」의 결과보고서

2017년 9월

간행 요목

「플랫홈 인더스트리 4.0」(2013~2015)은 BITKOM e.V,와 VDMA e.V. 및 ZVEI e.V 3개 단체의 공동 프로젝트이다.

발행인 그룹

BITKOM e.V.
연방 정보·통신 및 뉴미디어 산업협회
Albrechtstraße 10
10117 Berlin–Mitte

Tel.: (030) 27576–0
bitkom@bitkom.org
www.bitkom.org

VDMA e.V.
독일 기계 및 장비제작협회
Lyoner Straße 18
60528 Frankfurt am Main

Tel.: (069) 6603–0
zvei@zvei.org
www.vdma.org

ZVEI e.V.
독일 전기 및 전자산업협회
Lyoner Straße 9
60528 Frankfurt am Main

Tel.: (069) 6302–0
kommunikation@vdma.org
www.zvei.org

조정, 편집 및 교정

볼프강 돌스트(Wolfgang Dorst), BITKOM e.V.

레이아웃, 조판

아스트리드 샤이베(Astrid Scheibe) BITKOM E.v.

도 표

아스트리드 샤이베(Astrid Scheibe) BITKOM E.v.

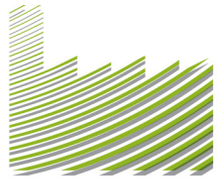
인 쇄

Kehrberg Druck Produktion Service

사진제공

그림 17 : (사진) 가치창조 지휘자로서의 인간, FESTO AG & Co. KG ; 그림 22 : (사진) 기계, FESTO AG & Co. KG ; (사진) 연결단자, PHOENIX CONTACT GmbH & Co. KG ; (사진) 전동축 (좌) (우), FESTO AG & Co. KG ; 그림 24 및 그림 31 : (사진) 기계 1 및 기계 2, FESTO AG & Co. KG ; (사진) 연결단자, PHOENIX CONTACT GmbH ; 그림 25 : (사진) 전동축 (좌) (우), FESTO AG & Co. KG ; 그림 26 : (사진) 센서, Pepperl+Fuchs GmbH ; (사진) 제어장치, Bosch Rextoth AG ; (사진) 전동축 (좌, 우), FESTO AG & Co. KG ; 그림 27 : (사진) 해석, FESTO AG & Co. KG ; (사진) 사용지침서 (좌), FESTO AG & Co. KG ; (사진) 사용지침서 (우), FESTO AG & Co. KG ; (사진) 전동축 (중단 1), FESTO AG & Co. KG ; (사진) 전동축 (중단 2), FESTO AG & Co. KG ; (사진) 전동축 (중단 3), FESTO AG & Co. KG ; (사진) 전동축 (중단 4), FESTO AG & Co. KG ; (사진) 전동축 (하단 1), Pepperl+Fuchs GmbH ; (사진) 전동축 (하단 2), FESTO AG & Co. KG ; 그림 28 : (사진) 기계, FESTO AG & Co. KG ; (사진) 연결단자, PHOENIX CONTACT GmbH & Co. KG ; (사진) 전동축(좌), FESTO AG & Co. KG ; (사진) 전동축우) : FESTO AG & Co. KG

2015년 4월 간행


플랫폼
인더스트리 4.0

인더스트리 4.0 실현 전략

「플랫폼 인더스트리 4.0」 결과보고서

Umsetzungsstrategie Industrie 4.0

Ergebnisbericht der Plattform Industrie 4.0

(번 역 판)

전문번역 I Vollständige Übersetzung

원어: 독일어 I Ausgangssprache: Deutsch

원판 발행일자 및 장소: 2015년 4월 베를린
Erscheinungsdatum und Ort in der Originalsprache: April 2015, Berlin

번역: 신창선 전남대학교 명예교수 I Übersetzung: Prof. Dr. Shin, Changseon em.

번역판 편집: 도서출판 피데스 I Layout und Satz der Übersetzung: Verlag Fides

ISBN 978-89-6479-317-6

2017년 9월 I September 2017

번역 및 출판 후원 I Sponsor der Übersetzung und Veröffentlichung

Dongwon 동원F&B

차 례

머리말

1. 머리말

물리적 세계와 가상 세계가 갈수록 서로 가까워지고 있다. 점점 더 많은 물리적 대상들이 지능형 센서 및 작동 기술로 장착되고 사물인터넷(IoT)의 발달을 통해 네트워크화 되고 있다. 가치창조에 참여하는 모든 작업자들의 관련 정보가 네트워크를 통하여 실시간으로 이용가능해지고, 아울러 이 데이터들로부터 어느 시점에서나 최적의 가치창출 흐름을 이끌어낼 수 있게 됨에 따라 산업혁명의 새로운 단계에 돌입하게 되었는데, 이것을 「인더스트리 4.0」이라 명명하고 있다. 이는 기술 분야에 진화적 영향을 미치게 되겠지만, 기존의 사업과정에 대한 영향은 혁명적이며 아울러 새로운 사업모델도 생기게 할 것이다. 여기에서 초점이 되는 것은 개발, 생산, 물류, 서비스라고 하는 산업의 핵심 과정들을 최적화시키는 것이다.

이 「인더스트리 4.0 실현전략」은 (BITKOM, VDMA, ZVEI 3개 단체에 의하여 조직된) 「플랫폼 인더스트리 4.0」(Plattform Industire 4.0)이 독일 산업계의 기업들 및 여타 단체들의 협력을 받아 작성한 것이다. 이 전략은 산업국가 독일 및 그 산업의 미래 대처 능력을 확고하게 하기 위한 것이다.

인더스트리 4.0의 근간이 되는 핵심 요소들에 대한 설명은 제4장에서 이루어진다. 이를 바탕으로 제5장 “연구와 혁신”에서는 연구가 필요한 중요 분야들을 도출하여 연구 로드맵과 개요 작성의 형식으로 기술된다. 연구 로드맵에서는 정치권과 기업들에 의한 적절한 조치 및 지원기구들(최상위 클러스터, 데모 실험실, 데모 시설, 데모 공장 등)을 통해 인더스트리 4.0의 주제를 의미 있게 계속 발전시켜나가기 위한 전향적인 방향을 제시하였다.
인더스트리 4.0에 대한 「참조구조 모델」(약칭하여 RAMI 4.0)은 제6장에서 소개된다. 거기에서는 인더스트리 4.0을 구성하는 요소들의 구축 과정과 작업방식이 설명된다. 의미가 있는 경우에는, 실행능력을 더 빠르게 갖출 수 있도록 「참조구조 모델」과 인더스트리 4.0 구성요소들의 일부분에 대하여 기존의 관련된 규범을 적용시키고 있다. 그러나 꼭 필요한 경우에는 추가적인 특정 표준규범의 작성 필요성에 대하여 언급하고 있다.

사물의 네트워크화가 진전되고 그 조정이 용이하게 되는 한편, 해커나 정보기관 또는 스파이 등에 의한 위협도 증대하게 됨에 따라 특히 안전성에 대한 요구가 대두된다. 이에 대하여는 제7장에서 다루어진다.

이 「실현전략」은 독일의 산업계, 기술지향적 업종, 연구소 및 정치권에 종사하는 사람들을 대상으로 하고 있다. 특히 경영간부나 전문가, 컨설턴트를 비롯하여 독일 인더스트리 4.0의 미래상에 관심을 갖고 있거나 그 형성에 참여하기를 원하는 사람들이 일독하기를 바란다.

인더스트리 4.0에 대한 포괄적 설명

2. 인더스트리 4.0에 대한 포괄적 설명

2.1 인더스트리 4.0의 개념 정의

인더스트리 4.0은 제4차 산업혁명을 가리키는 개념으로서, 이는 제품의 생애주기에 대한 전반적인 가치창출흐름의 조직과 제어가 새로운 단계에 들어서게 되는 것을 의미한다. 이 생애주기는 점점 더 개별화되는 고객의 요망을 충족시키는 것으로, 아이디어단계로부터 개발 및 제품의 완성을 거쳐 최종 고객에 대한 제품의 인도와 리사이클링(재활용)에 이르기까지 모든 단계에 미치며, 여기에는 관련된 제반 서비스들을 포함한다.

그것은 가치창출에 참여하는 모든 단계의 관련자들의 네트워크화를 통하여 관련 정보들을 실시간 사용할 수 있게 되고 나아가 그런 데이터들로부터 언제 어느 시점에서나 최적의 가치창출 흐름을 이끌어낼 수 있는 능력에 바탕을 두고 있다. 사람, 대상, 체계 등을 네트워크로 연결함으로써 기업들을 모두 아우르는 가치창출 네트워크가 역동성을 띠고 실시간으로 최적화되며 자율적으로 조직화된다. 그 결과 가치창출 네트워크는 가격, 효용성, 자원소비 등 다양한 기준에 맞추어 최적화가 가능해진다.

2.2 전략과 목표

BITKOM, VDMA, ZVEI 3개 산업단체는 「경제-학술연구연맹」의 활동을 계속 진행시키며, 상호 협력하고 여러 산업 분야를 포괄하는 대응방안을 확보하기 위해 「플랫폼 인더스트리 4.0」이라는 공동의 이니시아티브를 만들었다. 「플랫폼-인더스트리-4.0」의 핵심 목표는 BITKOM, VDMA, ZVEI 등 산업단체들을 통해 산업계 현장에서 인더스트리 4.0 비전의 실현을 촉진하는 것이다. 그렇게 함으로써 생산거점국가로서의 독일의 미래를 확고히 하고 더 나아가 확장하자는 것이다.
인더스트리 4.0에 대한 「경제-학술연구연맹」의 2013년 4월자 결과 보고서에서는 비전의 실현을 위한 제안[3]을 기술하고, 연구의 필요가 있는 분야를 상세히 지적하는 한편 8가지 작업 분야를 제시하였다. 여기서는 다음과 같이 – 효용성 측면을 보충하여 – 초기 현황을 설명하는 정도로 간략히 정리한다.

1. 표준화, 「참조구조」를 위한 규격표준의 개방
   가치창출 네트워크를 통하여 기업들을 포괄하는 네트워크와 통합을 가능케 한다.
2. 복합 시스템의 완벽한 제어
   작업의 자동화 및 디지털세계와 현실세계와의 통합을 위한 모델을 활용한다.
3. 산업을 위한 전국적인 광대역 고속통신망 사회기반시설의 구축
   인더스트리 4.0에서 요구되는 데이터 교환의 용량, 품질 및 속도의 확보
4. 보 안
   여기서의 목표는 기업경영의 안전(영어 Safety), 개인 정보 보호(영어 Privacy) 및 정보기술(IT)의 보안(영어 Security)을 보장하는 것
5. 작업 조직과 작업 현장의 조정
   인더스트리 4.0-시나리오에 있어서 기획자 및 의사결정자로서의 인간 내지 근로자가 연루되어 있다는 사실을 명확하게 하는 것
6. 직무 교육과 추가 교육(연수, 평생교육)
   직무 교육과 추가 교육의 내용 및 혁신적 접근방법들에 대한 설계
7. 법적, 제도적 기반의 정립
   이는 인더스트리 4.0을 위해 필요한 법적 환경과 조건(디지털 재화의 보호, 시스템간에 체결된 계약에 관한 계약법, 배상책임문제 등)의 – 가급적 유럽 통합적 - 정립을 목표로 한다.
8. 자원의 효율적 활용
   모든 자원(인적자원, 금융자원 및 원료, 첨가제, 연료 등)을 책임감 있게 활용하는 것이야말로 미래의 산업 생산을 성공적으로 이끄는 요인이다.

산업생산시스템을 인더스트리 4.0으로 성공적으로 전환시키기 위해서 독일에서는 다음과 같은 이중전략이 추진된다.

- 독일 설비산업의 고전적 장점인 첨단 산업적 특징에 정보통신 기술을 유기적으로 통합하여 스마트 생산기술 분야의 선도적 공급자 지위에 오르면서 독일설비산업이 앞으로도 계속해서 세계 시장에서 선도적인 자리를 지키도록 한다. CPS(사이버물리시스템)기술(1)[1] 및 해당 제품들을 위한 새로운 선도시장을 형성하여 키워나가야 한다.
- 동시에 효율적이고 자원 절약적 생산기술을 통해 독일 내의 제품 생산을 매력적이고 경쟁력 있게 더욱 발전시켜가는 것이 중요하다. 인터넷을 통해 생산자와 사용자 사이의 적극적인 네트워크를 이룩하고 공간적 거리의 가까움을 활용하여 독일 기업들의 경쟁력 우위를 키워가는 것이 목표다. 이 전략은 독일의 자동화기술, 프로세스기술 및 생산기술 모두에게 다 같이 장점으로 작용한다.
- 인더스트리 4.0에 다가가는 길은 진화적인 과정이다. 전체 가치창조사슬의 최적화에 관한 경험과 특수 조건을 축적하기 위하여 기존의 기초기술들을 더욱 발전시킬 필요가 있다. 인터넷 서비스를 통해 새로운 사업모델을 실현시키는 일은 파괴적 성격을 띤다. 판매시장에서 양질의 제품이나 서비스를 제공하여 그 수요가 늘어나는 성공적인 기업이 되기 위하여는 파괴적인 변화들에 대한 고도의 대비책을 강구해야 한다. 그것도 다름 아닌 기업 내 기존 프로세스를 더욱 더 발전시키는 한편 새로운 사업모델을 개발하는 과정을 통해서 말이다.

1) 「실현제안」[3]에서의 정의는 다음과 같다 : Cyber-Physical Systems (CPS – 사이버 물리 시스템): CPS는 구축된 시스템들, 생산, 물류, 엔지니어링, 조정 및 매니지먼트 등 제반 프로세스와 인터넷 서비스를 모두 포괄한다. 이들은 센서들을 통해 물리적 데이터와 직접 연결되어 있고, 구동장치를 통해 물리적 프로세스에 작용한다. 아울러 디지털 네트워크를 통해 서로 연결되어 있고, 전 세계 차원에서 이용가능한 데이터와 서비스를 이용하고 인간-기계-인터페이스라는 멀티모드를 사용한다. 사이버물리 시스템이란 개방적 사회기술 시스템이며 일련의 새로운 양식의 기능, 서비스, 특성들을 가능하게 한다.

2.3 유용성

가치창조사슬의 흐름에 참여하는 자에게 주어지는 유용성은 다양하다. 개별화된 고객의 요망을 충족시켜줄 수 있는 역량이 개선되고 낱개 제품이나 최소 물량 생산의 수익성이 커진다. 인터넷을 통해 여러 차원에서 사업 과정들과 민첩한 엔지니어링 프로세스들을 동적으로 조합하여 구성함으로써 유연화가 진척된다. 이를테면 빅데이터, 소셜미디어, 클라우드 컴퓨팅 등과 함께 인더스트리 4.0에 의해 마련된 정보들을 바탕으로 최적의 결정을 찾아내 조기에 계획안을 확정하며, 발생하는 장애에 대한 유연한 반응과 모든 자원들에 대한 지역적 입지를 초월하는 글로벌 차원의 최적화 등이 가능해진다.

생산 효율성이 증대되는데, 이는 한편으로는 생산성 향상을 통해서고, 다른 한편으로는 자원(기계, 에너지 등)의 효율적 이용을 높임으로써 이루어진다.

새로운 형식의 가치창출과 사업 활동을 통한 새로운 잠재력이 생겨난다. 예컨대 제품이 생산시설을 떠나고 난 뒤 사용자에게 본래의 제품 대신에 제공할 수 있는 서비스, 즉 후속 서비스의 제공이 이런 경우에 해당한다.

인구통계학적 변화를 고려한 일자리의 형성을 위해서도 장점이 된다. 따라서 신체적 능력 및 인지 역량에 대한 지원이야말로 인더스트리 4.0 구상의 결정적인 부가가치가 된다. 교육수준이 .높은 사람을 요구하는 지식 기반 기업이 근로자들의 지식과 경험 수준을 유지시키기 위해서는 인더스트리 4.0을 통해 인재, 즉 경영간부 외에 특히 전문인력의 육성을 위한 유연하고 다양한 경력 모델이 가능해진다. 소셜 미디어를 통해 생산계획과 근무 시간이 더욱 유연해진다. 생산프로세스의 점유율이 최적화되고 자원이 더 잘 활용된다. 게다가 단기적인 면에서도 고객의 바람에 맞춰 반응할 수 있다. 무엇보다 근로자들은 인력배치 계획을 더 충실하게 따름으로써 맡은 작업과 가족 및 여가를 더 잘 조화시킬 수 있다.

인더스트리 4.0은 고임금 국가인 독일의 경쟁력을 강화하고 독일 기업들의 선도적인 공급자 위상을 가능케 하며, 독일이 인더스트리 4.0 솔루션의 선도 시장이 되도록 한다.

독일 산업계의 노하우는 매우 앞서 있다. 몇 가지 예를 들면, 선도적인 기업들이 있고, 확고한 기반을 갖추고 있는 중소기업분야도 그러하며, 산업 자동화 기술 공급자나 IT-기업들 및 공구 및 기계제작 기업 등이 그러하다.

2.4 경 쟁

인더스트리 4.0의 구상은 참여자들 모두가 제품의 전 생애주기에 걸쳐 실시간으로 안전한 소통과 협조를 할 수 있는 것을 전제로 한다. 이는 인터넷 베이스의 플랫폼으로 가능하다. 이 디지털 플랫폼에 새로운, 혁신적인 가치창조사슬이 구축되고, 이것이 인더스트리 4.0의 효용성을 가져다 준다.

이와 같이 기업들을 망라하는 확실한 "수평적" 소통 및 협조 플랫폼에 관하여 경쟁 이전의 단계에서 공동으로 정의하고, 모든 환경·조건들과 계속해서 연구가 필요한 분야를 확정하기 위하여 「플랫폼 인더스트리 4.0」이라는 협의체를 발족한 것이다.

그러나 이것이 전부가 아니다. 물리 세계의 가상 디스플레이 및 그 시뮬레이션에 의하여 시종일관하는 제품-생산-서비스가 가능해지기 때문에 새로운 기술의 개발도 촉진된다.

더 나아가 수직적 소통이 개선됨에 따라 생산과정에 "사물 인터넷" 기술을 의미 있고 안전하게 이용할 새로운 가능성이 생겨난다.

「플랫폼 인더스트리 4.0」에 참여한 기업체와 학술 고문단 그리고 BITKOM, VDMA, VDMA, ZVEI 등의 사업자 단체들은 기술중심적인 작업그룹 안에서 공동으로 하나나 소수의 「참조 아키텍처 모델」에 필요하거나 적합한 표준들을 평가하고, 필수적인 환경 조건들을 찾아 제시하고, 연구할 가치가 있는 분야를 특정하였다. 개별 기업들은「플랫폼 인더스트리4.0」에서 제시한 방향정립지식을 기반으로 하여 자체 결정에 의해 위 단체들의 플랫폼 밖에서 새로운 가치창조사슬과 혁신적 사업모델을 제공함으로써 시장에서 서로 경쟁 관계에 설 수 있다.

「플랫폼 인더스트리 4.0」은 비슷한 주제에 참여하고 이 플랫폼의 자체 활동과 관련된 각종 협회 및 단체들과 정기적으로 의견을 교환한다. 이러한 조율은 지명되고 해당 임무의 위임을 받은 회원을 통해 이루어진다.

학술 고문단의 가설

3. 학술 고문단의 가설

학술 고문단은 모든 학술적 연구 및 프로그램에 관하여 부수적 연구사업과도 긴밀한 연락을 취하면서 「플랫폼 인더스트리 4.0」에 조언한다. 고문단에는 생산, 자동화, 전산학, 법학, 노동사회학 등 전공분야 남녀 교수 16명이 활동 중이다.

2014년 하노버 박람회 (2014년 4월 3일 시점)에서 학술 자문단은 자체적으로 설정한 가설을 발표하였는데 [12], 이는 플랫폼의 웹사이트에서 열람할 수 있다. 이하에서 인용되는 이 가설은 인간, 기술, 조직 이라는 3개의 항목으로 구성되어있다.

인 간

1. 작업조직을 인간 중심으로 구성할 가능성이 다양하게 생겨나는데, 자체조직화와 자율성의 의미에서도 마찬가지다. 특히 고령화나 연령에 적합한 근로조직을 실현할 기회가 생긴다.
2. 사회기술시스템으로서의 인더스트리 4.0에서는 근로자들이 처리하는 업무범위를 확장시키고, 근로자의 자격(자질)과 활동영역을 고양시키며 지식습득에 대한 접근성을 뚜렷하게 개선할 기회를 제공한다.
3. 학습을 촉진시키는 작업수단(Learnstruments)과 소통가능한 근로형태(Community of Practice)는 교육 및 학습 생산성을 고양시키고, IT 관련 기능의 점유비중이 점점 더 높아짐에 따라 새로운 교육내용이 생겨난다.
4. 학습수단(사용하기 편하고, 학습을 촉진하는 인공물)은 이용자들에게 그 기능을 자동으로 익히게 해준다.

기 술

5. 인더스트리 4.0-시스템들은 사용자들이 이해하기 쉽고, 이용하기 쉬우며, 학습을 촉진시키고 반응이 신뢰할 만하다.
6. 일반적으로 접근이 가능한 솔루션 모델들은 그 누구에게도 인더스트리 4.0 시스템을 설계하고, 실현시키고 운영하는 것을 가능하게 해준다(디자인에 의한 인더스트리 4.0).
7. 제품 및 사업프로세스의 네트워크화와 개별화로 인하여 상황이 복잡해지는데, 이는, 예컨대 모델링, 시뮬레이션, 자기 조직화 등을 통해 관리된다. 보다 큰 솔루션 영역의 분석과 다양한 솔루션을 찾는 일이 더 빨라진다.
8. 자원의 효용성과 효율성은 지속적으로 계획, 실현, 감독되면서 자동으로 최적화된다.
9. 스마트 제품들은 능동적인 정보매체이며 생애주기 전체에 걸쳐 소재지의 지정이 가능하고 식별이 가능하다.
10. 시스템 구성요소들은 생산수단 내부에서도 주소지정과 식별이 가능하다. 이들 요소들은 생산시스템과 프로세스의 가상 계획(디자인, 엔지니어링)을 지원한다.
11. 새로 도입되는 시스템 구성요소들은 최소한 대체 가능한 요소들의 역량을 사용할 수 있고 그 기능을 호환성 있게 넘겨받을 수 있다.
12. 시스템 요소들은 자체 기능들을 다른 사람들이 이용할 수 있는 서비스로 제공한다.
13. 새로운 보안문화의 조성으로 인더스트리 4.0-시스템은 신뢰성이 높고 탄력적이며 사회적으로 수용될 수 있게 된다.

조 직

14. 부가가치가 있는 새로운 가치창출 네트워크와 기존에 확립된 가치창출 네트워크는 제품, 생산, 서비스를 통합하여 역동적으로 다양한 유형의 분업을 가능케 한다.

15. 협력과 경쟁(competition)에 의하여 경영구조적이나 법적으로 새로운 구조가 형성된다.

16. 시스템 구조와 사업프로세스는 각각의 유효한 법규내에서 가시화될 수 있다; 새로운 법적 실마리가 생기면 새로운 계약 모델을 가능케 한다.

17. 지역적인 가치창출진흥의 기회가 생겨나는데, 이는 발달도상의 시장들에서도 마찬가지다.

2014년 하노버 박람회를 맞아 플랫폼에서 발표한 “연구개발 주제 백서”(Whitepaper FuE Themen)에서도 이 가설들의 실현에 꼭 필요한, 여러 가지 주제 영역들의 내용과 목표들이 소개되었다. 이 주제영역들에 대한 개략적인 작업의 일정이 제시되고 있다. 주제영역과 주요일정(제4장 및 제5장 참조)은 플랫폼 작업팀의 활동에 포함되어 있다.

인더스트리 4.0의 실현 전략

4. 인더스트리 4.0의 실현 전략

경제 거점국가로서의 독일의 입지를 강화하기 위해 "플랫폼 인더스트리 4.0"은 인더스트리 4.0의 실현전략을 수립하는 것을 그 목표로 하고 있다. 이를 위해 한편으로는 기술과 표준, 그리고 사업 및 조직 모델을 위한 개념들에 대해 산업 분야들을 아우르는 접근방법 속에서 실천전략을 수립하고, 다른 한편으로는 대학, 연구시설과 중소기업 및 산업계 기업들 사이의 협력체계를 구성하고, 이를 통해서도 현장 실천을 가속화한다.

인더스트리 4.0을 통해 새롭게 생겨나는 가치창출사슬과 네트워크들은 점점 더 진행되는 디지털화를 통해 자동화된다. 중요한 핵심 요소들(그림 참조)로는 다음 분야들이 해당한다.

- 연구와 혁신
- 참조 아키텍처, 표준화, 규격 통일 및
- 네트워크화된 체계들의 보안 등

이 분야들은 「플랫폼 인더스트리 4.0」의 특별 작업그룹들에서 다루어진다. 여기에는 다음 사항이 포함된다.

- 법-제도적 기본조건들의 마련

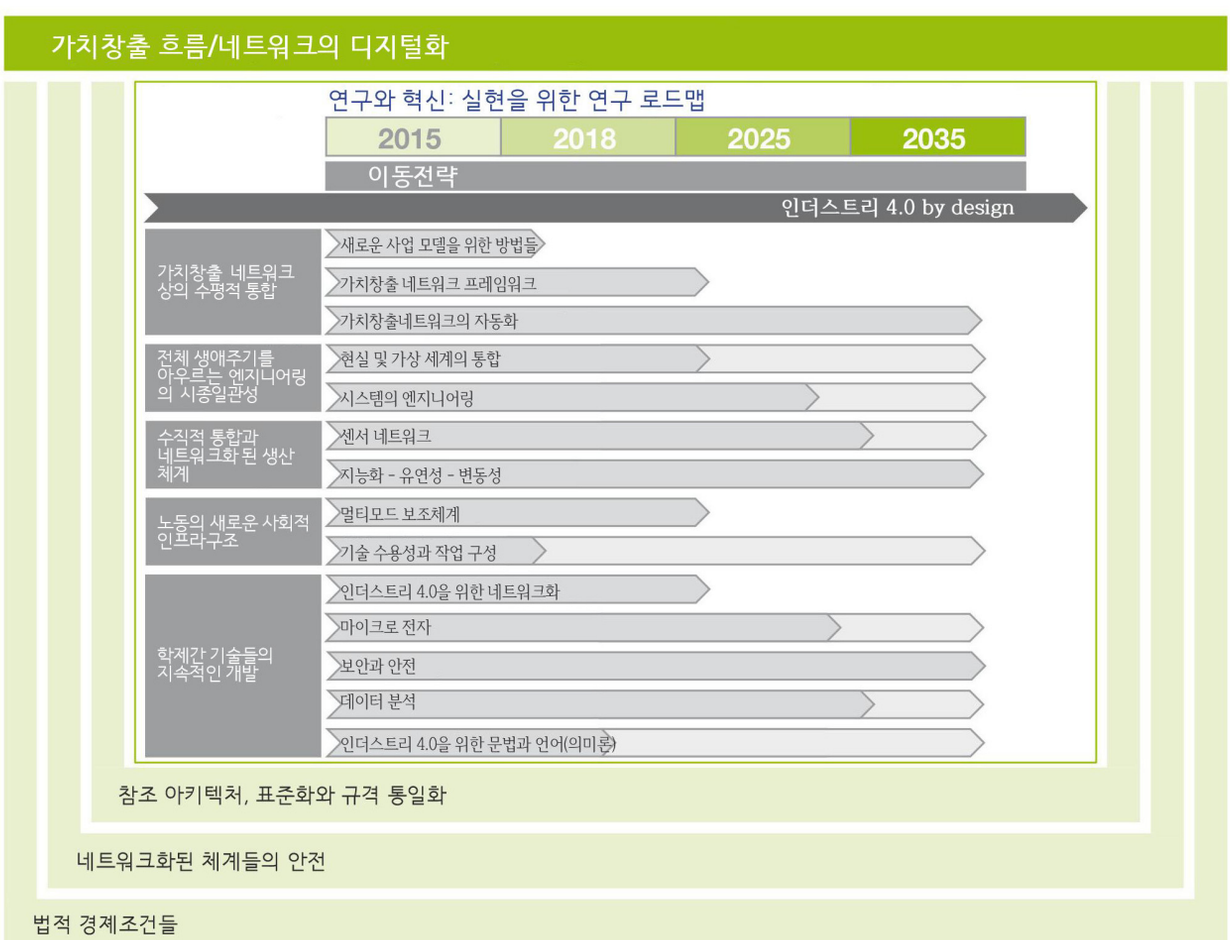


그림 1: 인더스트리 4.0의 핵심요소들

이 주제는 「플랫폼 인더스트리 4.0」에서 다루지 않고 BDI(독일연방산업연맹: Bundesverband der Deutschen Industrie)의 작업팀에서 특별하게 다룬다.

연구와 혁신 분야에서는 학술자문단과 조율하여 인더스트리 4.0의 실현에 필요한 연구 및 혁신 로드맵을 작성하고 필요한 혁신 및 연구 활동과 그에 대한 지원을 산업적 시각에서 조율하고 조정한다. 여기서 가장 중요한 주제 영역들은 다음과 같다(제5장 참조).

- 가치창출 네트워크들의 수평적 통합
  핵심은 기업들을 아우르는 협력체계(몇 가지 예를 들면 공급자, 중소기업들, 생산 기업)를 결성하는 것이다. 여기에는 새로운 사업모델을 위한 관점들과 방법들이 포함된다.
- 생애주기 전체에 걸쳐 시종일관하는 엔지니어링(생애주기 전체에 걸쳐 언제 어디서나 가능한 엔지니어링)
  여기서 핵심 주제는 제품 생애 주기 관리(PLM Product Lifecycle Management)기반의 엔지니어링인데, 이를 통해 제품 디자인과 생산디자인이 결합되어 가치창출 과정 전반에 걸쳐 언제 어디서나 지원이 이루어질 수 있다. 여기에서는 시스템 엔지니어링, 모델링 및 시뮬레이션에 대한 통합된 고찰과 같은 기술적이고 전문적인 사안들을 대상으로 하고 있다.
- 수직적 통합과 네트워크화된 생산시스템
  여기서 핵심 주제는 생산의 네트워크화인데, 이는 여러 면에서 실시간 요구사항들의 조건이기도 하다. 여기서 중요한 점들이라면, 요구되는 변화 능력과 생산기술상의 안전성 요구(예컨대 과잉과 결함허용범위 fault tolerance)를 확보, 보장하는 일이다. 여기에 요구되는 것이 센서 네트워크처럼 포함되는 요소들과 체계들은 물론이고 예측 분석과 같은 방법론들의 지속적인 개발과 발전이다.
- 작업에 요구되는 새로운 노동인프라
  결정적인 성공요인은 역시 사람이고 그것은 앞으로도 마찬가지다. 이에 따라 참여자들(특히 노동조합과 사용자연합들)의 지원과 추진을 받아 작업세계가 긍정적으로 발전할 수 있도록 보장하는 것이 핵심적으로 중요하다. 여기에는 직업교육과 계속교육의 변화와 개선 외에도 새로운 인간-기계(Human-to-Machine) 시스템들의 도입이라든가 일반적으로는 보조체계의 도입이 포함된다.
- 크로스오버 기술의 지속적인 발전
  인더스트리 4.0의 실현을 위해서는 다양한 기술적 전제들이 마련되어 산업적으로 적용되도록 해야 한다. 중요한 기술로 네트워크 통신, 광역 통신망, 클라우드 컴퓨팅, 데이터 분석, 사이버 보안, 안전한 단말기기 및 사물통신(Machine-to-Machine) 솔루션(의미론 Semantik 포함) 등이다.

참조 아키텍처, 표준화와 규격 통일화 등의 주제그룹에 있어서는 통일규격과 표준 및 그 확립(제6장 참조)을 활용하여 솔류션에 제약을 주지 않는 참조 아키텍처를 구축하는 것이 중요하다.

네트워크 시스템의 안전성에 관한 영역에서는 전형적인 가치창출 사슬의 베이스로 수평적(고객/공급자) 및 수직적(기업 내부의) 네트워크 내부에서의 IT-보안을 위한 개념들이 협력 차원에서 연구되고 있다. 이는 일반적인 요구들과 보안-원리들(제7장 참조)의 확인에 도움이 된다. 그 다음 배치는 반복 과정 속에서 이루어지는데, 이 과정 역시 연구 시각과 표준화 측면을 내포하며, 그에 따라 인더스트리 4.0 참조 아키텍처 창출에 기여한다.

법-제도적 기본조건이라는 주제는 새로운 생산 프로세스와 수평적 사업네트워크의 합법적 형성에 대해 다룬다. 여기서 제기되는 문제에는 계약법(자동화된 가치창출 사슬에서 이루어지는 동적인 계약 체결), 기업 데이터 보호, 디지털 상품 취급, 배상책임 문제 및 개인 관련 정보들의 처리 같은 것들이 포함된다.

연구와 혁신

5. 연구와 혁신

5.1 머리말

「플랫폼 인더스트리 4.0」에서는 인더스트리 4.0에 관한 여러 연구 활동을 지금까지보다 더 명확하게 구획하고, 이 연구 활동들이 구조화되며 연구 과제에 우선순위가 부여되는 방식으로 이루어져야 한다는 데에 찬성한다. 이 장에서 그 토대로 사용하는 것은 산업단체 플랫폼에서 설명한 연구-로드맵이다. 더 나아가 당면한 연구과제들의 실행을 위해 이 주제의 잠재적 범위에 부합하고 국제 비교에서 경쟁력 있게 하는 지원 예산이 연방에서 마련되어야 한다. 연방의 지원예산은 참여한 기업들이 이미 의미 있는 규모로 투입한 재원을 보충하고, 인더스트리 4.0의 조속한 실현을 위해 당면한 과제들을 목표에 따라 완수하기 위한 중요한 전제조건이기도 하다.

그 밖에도 정책적으로 적절한 조치들과 지원수단들(최상위 클러스터, 시험demo-실험실, 시험-시설들, 시험-공장들 등등)을 통해 기업들과 학계 및 상이한 분야의 상이한 규모의 기업들 사이의 네트워크 연결 확장을 지속적으로 지원하고 투자하고 요구해야 한다.

인더스트리 4.0은 궁극적으로 국가 차원에서 주어진 로드맵을 통제하여 실현시킬 수는 없고, 게다가 여러 기업들의 서로 다른 이해와 시각 때문에 인더스트리 4.0의 정확한 버전을 정하기도 어렵다. 그보다 인더스트리 4.0은 구체적인 적용 사례들(이용 잠재력과 가치창출 잠재력에 대한 분석 포함)을 점진적으로 발전시킨 결과물이 될 것이다. 이처럼 실무(현장)지향적인 성격이 오히려 강한 프로젝트에도 연방정부 차원의 지원을 고려하는 것이 바람직하다. 그 지원은 새로운 방법론과 기술의 연구로부터 대학 부설의 시험용 시설과 산업계의 파일럿 공장들에 대한 해당 기술도입에 이르기까지 혁신과정 전체를 대상으로 하는 방식이 되어야 한다.

이 장에서는 인더스트리 4.0에 대한 연구 및 혁신 관련 주제들을 설명하는데, 무엇보다 학술자문단의 가설들을 바탕으로 한다. 첫 성과들은 이미 2014년 하노버 박람회에서 발표된 "연구개발 주제 백서"에 나타나 있다. 그 이후 중요한 주제들에 대해 계속해서 자세한 설명이 이루어졌다. 이제부터는 2015년 2월 현재의 개정 작업이 설명된다(이 주제 영역들에 대해서는 개별적으로 프로파일이 있는데, 이 프로파일은 이 문서에 기술된 내용을 넘어서며 「플랫폼 인더스트리 4.0」 작업그룹 안에서 실행된다.). 2015년 전반기에 "연구개발 주제 백서"의 새 버전도 나란히 발표되었는데, 이는 상술한 주제들에 대하여 더욱 상세하게 파고든 것이다.

이하에서 이들 주제영역에 대하여 (1) 연구와 혁신의 내용들에 대한 설명, (2) 추구하였던 성과들 및 (3) 핵심 사안들과 주요 일정으로 나누어 간략히 다루고자 한다.

5.2 주제영역 : 가치창출 네트워크를 아우르는 수평적 통합

여기서 말하는 수평적 통합이란 여러 가지 가치창출 프로세스(예컨대 제조, 물류, 마케팅, 엔지니어링, 서비스)의 지원과 운영을 위한 여러 IT-시스템들과 제조업체내에서의 통합은 물론, 기업의 경계를 넘는 통합을 포함하여 시종일관하는 솔루션의 통합을 의미한다.

5.2.1 새로운 사업모델을 위한 방법들

5.2.1.1 연구 및 혁신 내용

사업모델이란 어느 기업 내에서 사업과 가치창조가 어떻게 이루어지는지에 대한 간략한 설명이다. 이는 어느 파트너와 어느 시장에서 어느 고객을 대상으로 수익을 올릴 것인지 대한 추상적인 명세서인 셈이다. 인더스트리 4.0의 맥락에서 보면 기업 내부에서 새로운 가치창조 프로세스가 생기고 가치창조 네트워크에서 스스로 역할 분담이 변화함에 따라 새로운 사업모델들이 생겨난다.

여기서 고려해 보아야 할 관점들은 다음과 같다.

- Go-To-Market(GTMs) 전략
- 수요 분석과 수요창출 및 잠재력 조사를 위한 방법론
- 지불 및 결제 모델
- 네트워크 내에서 활동하는 개별 행위자 각각에 대한 효용 및 위험 평가
- 법적, 제도적 측면
- 자극 및 수용 체계

5.2.1.2 연구 및 혁신에서 추구한 결과들

기업들을 아우르는 네트워크의 잠재력을 지속적으로 활용하기 위하여서는 사업모델에 대한 공통적인 이해가 전제되어야 한다. 방법론적 접근방법들이 통합되어 확립되어야 한다. 모범경영(Best Practice)과 경험들을 – 특히 각기 다른 분야에서 나온 것을 포함하여 – 체계적으로 수집, 파악해야 한다. 그러면 생산 과정에 적용하여 거기서 나오는 결과들에 대한 분석이 뒤따르게 된다. 이때 가치창출 네트워크 내부의 다양한 역할들이 고려되어야 한다.

다음과 같은 결과들을 기대할 수 있다.

- 어느 한 네트워크 내부에서 역할이 다른 공급자를 위한 모범적인 Go-To-Market(GTMs)전략을 모범경영에서 도출
- 인더스트리 4.0의 필요성에 맞춘 가치창조 네트워크의 측면을 고려한 사업모델 전략
- 지불, 정산 및 라이센스를 위한 모범적 모델
- 인더스트리 4.0 고유의 활용 및 그에 따른 위험의 평가를 위한 가이드라인
- 법적 가이드라인 – 무엇보다 서비스로서의 소프트웨어(SaaS)와 서비스로서의 플랫폼(PaaS)을 위한 서비스 수준 협약(SLAs)에서의 배상책임문제에 대한 가이드라인

5.2.1.3 핵심 사안들과 주요 일정들

방법론
1.4 인더스트리 4.0 고유의 활용과 위험의 평가방법에 대한 가이드라인 1.5 법적 측면에 대한 가이드라인
솔루션
1.1 모범 경영과 경험 및 생산에의 적용 1.2 모범적 Go-to-Market 전략 1.3 모범적인 지불, 정산 및 라이센스 모델 1.6 인더스트리 4.0에 조율된 사업모델 – “가치창조 네트워크” 측면을 고려 1.7 (새로운) 사업전략, 사업모델 및 사업 프로세스의 시험실행(pilot run)
전제조건
2.3 여러 가지 조직형태를 위한 가치창출 네트워크로서의 참조아키텍처

그림 2: 새로운 사업 모델을 위한 방법론 연구의 이정표

5.2.2 가치창출 네트워크의 프레임워크

5.2.2.1 연구와 혁신 내용

가치창출 네트워크라고 하는 것은 개별 가치창출 프로세스와 그 프로세스 기술의 상호의존성으로 이루어진 하나의 시스템을 말한다. 개별 가치창출은 자율적이고 법적으로 독립적인 행위자들에 의해 실현된다. 이들은 가치창출 네트워크를 통해 복잡하고 상호의존적인 관계들에 의해 서로 결합되어 지속가능한 경제적 부가가치를 추구하는 가치창출 파트너들로서 일종의 이해공동체를 형성한다.

여기서 고려해야 할 관점들은 다음과 같다.

- 새로운 가치창출 네트워크의 성립을 위한 전제조건, 추진 요인, 결과물들
- 여러 가치창출 네트워크 통합자로서의 CPS-플랫폼의 경제적 역할
- 사업상 가능한 위험들과 그 결과들
- 가치창출 네트워크의 조직형태들 – 그들의 상이한 요소, 역할 및 법적 구체화 방법

5.2.2.2 연구와 혁신에서 기대되는 성과

가치창출 네트워크의 구현을 위한 개념들이 세워져야 하고 파일럿 프로젝트들에 적용하여 (새로운) 사업 전략과 모델과 프로세스와 같은 주제들을 고객, 공급자, 파트너, 시장 등을 더 강력히 포함시켜 조명해야 한다. 그러기 위해서는 구체적인 사례들을 위한 사업-계획들을 세우고 “통합 편성 조율(orchestration)”과 관련한 경험들을 취합해야 한다. 이 경험들은 가치창출 네트워크 지원을 위한 CPS-플랫폼에 대한 미래의 요구로서도 공개되어야 한다.

기대되는 성과들은 다음과 같다.

- 가치창출 네트워크들을 생산에 유연하게 통합
- (네트워크 파트너와 그 고객들의 시각에서 본) 경제 및 기술상의 잠재력 분석과 평가 방법들 –
- 네트워크 내의 협조를 위한 특히 중소기업들 간의 제휴

- 새로운 사업 가능성들의 개시
- Win-Win-가치창출 파트너십과 그것을 통한 지속 가능한 "통합형" 사업모델

5.2.2.3 핵심 사안들과 주요 일정

방법론
2.1 하나로 통일된 모델 안의 개별 프로세스 단계들의 형식적 기술과 표준(의미론) 2.2 하나로 통일된 모델 안에 있는 인터페이스와 전체 네트워크에 대한 형식적 기술과 표준(의미론) 2.3 여러 가지 조직형태들을 위한 참조 아키텍처 – 가치창출 네트워크 2.4 연결된 가치창출 네트워크의 경제 및 기술적 잠재력에 대한 분석과 평가 2.5 구현을 위한 전제, 추동요인, 결과 및 절차 등에 대한 가이드라인 2.6 가치창출 네트워크 지원을 위한 CPS-플랫폼에 대한 요구들
솔루션
2.7 보편타당하고 통일된 모델 2.8 연결 관계(맥락), 모델, 전제, 구동요인, 결과들에 대한 기본 이해
전제조건
1.6 인더스트리 4.0에 조율된 사업모델 – "가치창출 네트워크" 관점을 고려하여

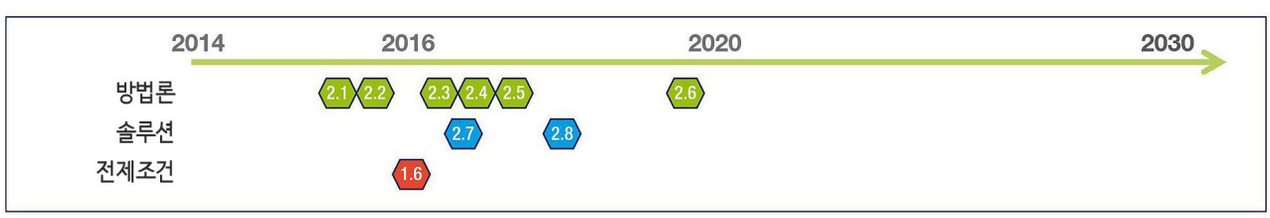


그림 3: "프레임워크 가치창출 네트워크"라는 주제에 대한 핵심 사안과 주요 일정

5.2.3 가치창출 네트워크의 자동화

5.2.3.1 연구와 혁신 내용

가치창조의 각 단계가 자동화되어 진행되면서 수평적 통합의 자동화 정도가 향상된다. 이때 가치창조가 자동적으로 이루어지거나 순수한 "디지털" 세계에서 가치창조가 이루어지는 그런 단계들이 전면에 부각된다.
고려되어야 할 관점들은 다음과 같다.

- 정보흐름의 시종일관성(언제, 어디서나 접근 가능함)
- 모델링, 계산(computation), 시뮬레이션, 최적화를 위한 절차의 도입
- PLM(제품 생애주기 관리 Product Life-cycle Management), APS(앞선 생산 및 일정계획 advanced Planning and Scheduling), MES(제조실행 시스템 Manufacturing Execution System), SCM(공급망 관리 Supply Chain Management), ERP(전사적 자원관리 Enterprise Resource Planning) 등 적용분야들의 통합
- 사람을 창의적 관계자로 글로벌 가치흐름에 통합
- 인간-기계-인터페이스 형성
- 자격취득대책과 이행과정의 의존성

5.2.3.2 연구와 혁신에서 추구한 결과들

가치창출은 더 효율적이고 더 유연하게 이루어져야 하며 확실하게 예측이 가능해야 한다. 사람들은 창조성을 필요로 하지 않는 활동의 부담으로부터 벗어난다. 생산성 향상, 자원 효율성 및 자동화가 핵심이다. 복합적 계획 프로세스 개별 단계들의 계속된 자동화를 통해 상위의 가치창출 흐름과 네트워크 및 글로벌 차원에서 정의될

수 있는 목표치와 관련하여 공장 운영이 최적화된다. 이 때 상호 종속성(연계성)을 고려해야 하고, 시너지효과를 추구해야 한다. 그것은 그 전까지 위계적-순차적으로 조직된 프로세스가 통합되어 부분적 동기화 내지 자율화로 실행되면서 가능해진다.

기대되는 성과는 다음과 같다.

- 모든 사업프로젝트의 직·간접적 상관관계와 의존관계(예컨대 PLM, ERP, APS, MES 등)를 기술하는 방법론
- 모든 활동과 프로세스들이 미치는 효과를 글로벌 차원의 목표에 미치는 영향과 연결시키는 공통의 목표계층
- 상술한 상관관계 및 의존관계를 고려한 최적의 글로벌한 목표를 구성하고 조직화할 수 있는 프로세스 및 활동
- 간단히 적용 가능하고 통합 가능하며 자동 기술되는 모듈
- 간단하고 창의적인 설명과 계속적으로 시뮬레이션할 수 있는 가능성으로 사용자를 지원하는 도구와 프로그램들

5.2.3.3 핵심 사안들과 주요 일정들

방법론
3.1 최적화 방법론 3.2 전략적 요건 – 목표 위계 시스템 – 프로세스 모델링 3.3 복잡성의 극복과 적용 가능성 3.4 프로세스의 모든 단계에 걸쳐 현시점의 상태와 계획한 상태에 대해 시종일관 확인 가능한 투명성
솔루션
3.5 고객, 공급자, 파트너 및 시장을 모두 포함하는 파일럿 사업전략, 사업모델, 사업프로세스 3.6 가치창출 네트워크의 시종일관한 통합과 유연한 연결 및 최적화된 의사 결정
전제조건들
2.1 통합된 단일 모델 내 개별 프로세스 단계들에 대한 양식에 따른 설명과 표준(semantic) 2.2 통합된 단일 모델 내 인터페이스와 가치창출 네트워크들의 편재한 통합과 유연한 연결 2.3 여러 가지 조직형태들을 위한 참조 아키텍처와 가치창출 네트워크 2.8. 연결맥락, 모델, 전제조건, 구동자 및 결과들에 대한 기본적 이해

그림 4: "가치창출 네트워크"의 자동화에 관한 연구의 핵심 사안과 주요 일정

5.3 주제 영역 : 생애주기 전체에 걸쳐 시종일관한 엔지니어링

제품의 생애주기란 제품의 개발과 그에 부수적인 생산체계의 엔지니어링, 그 생산체계를 통한 제품의 생산, 수요자에 의한 생산 제품의 사용 및 사용된 제품의 리사이클링 내지 재생(복원 renaturation) 등을 말한다. 이 생애주기 전반에 걸쳐 생겨나는 모든 정보들은 언제 어디서나 서로 접근이 가능하게 연계되어야 한다.

5.3.1 현실세계와 가상세계의 통합

5.3.1.1 연구와 혁신 내용

현실세계와 가상/디지털 세계의 상호작용은 인더스트리 4.0에서 훨씬 더 두드러지게 핵심 위치를 차지한다. 대상들에게는 모두 디지털 복사 내지 모델이 있다. 현실세계는 이런 맥락에서 보통 해결되어야 할 문제설정이나 의사결정과정으로 특징지어진다. 이에 대하여 가상/디지털 세계의 근본 요소는 시뮬레이션, 계획모델, 기술모델 등이다. Co-modelling은 그밖에도 이 두 세계 사이의 인터페이스를 다양한 규모(scale)로 고찰한다.

복잡한 시스템들을 만들어 세울 수 있으려면 그 토대는 계획모델들이 된다. 설명모델들은 복잡한 시스템들의 분석을 가능케 하며, 그럼으로써 인간에 의한 전송 프로세스를 거쳐 솔루션이나 의사결정으로 이어진다. 그런 점에서 가상세계는 이 두 가지 모델의 접근방법 모두에서 실제 세계의 설계(디자인)에 의미 있는 영향을 미친다. 그와 동시에 모델들이 가리키는 사태들과 계산해야 할 요구사항이며 목표설정은 현실 세계에 위치하기 때문에, 현실세계 역시 가상 세계에 영향을 미친다.

이를 위해서는 기계 및 장비 제작을 위한 생산기술 모델링 이론이라는 의미에서의 학술적 기반이 필요하다. 확립된 이론과 기술(記述) 수단 및 방법들은 그와 연계되는 전산학의 기초 기술들과 함께 엔지니어공학분야에서의 폭넓은 사용을 고려하여 적절한 적응, 확장 및 병합을 통해 더욱 강화되어야 한다. 여기서 핵심적인 역할을 하는 것은 널리 알려진 그 분야의 독특한 작업원칙과 소프트웨어 도구를 수용자에게 적합하게 통합하는 것이다.

고려해야 할 중요한 관점들은 다음과 같다.

- "훌륭한 모델이란 무엇인가?"(불확실성 편가 포함) "적합한 모델을 어떻게 찾나?" "디지털 세계에서 내가 실현하고자 하는 게 무엇이고, 현실 세계에서는 무엇인가" "가상세계와 현실세계 사이의 인터페이스는 어떻게 설정할 수 있는가?" 와 같은 문제들에 대하여 제대로 대답할 수 있도록 하기 위하여 모델링 이론이 그 기초를 제공해야 한다. 이때 기존 모델들에 대해서도 고려해야만 한다.
- 모델링 이론에서는 추상화, 편재성(pervasiveness), 조사(inspection), 종속성, 유형 대 사례(type vs. instance), 모듈화, 모델링의 깊이, 모델베이스 테스팅(MDT: model-driven testing) 아키텍처 등과 같은 개념들이 정의된 의미론 기반에서 확정되어야 한다.
- 모델링의 학술적 성격: 모델 제작을 위한 비용 외에도 생애주기 전체에 걸친 이용을 지원하는 모델-사용도 고려해야만 한다. 여기서 커다란 관심거리라면 생애주기 동안 모델들이 어떻게 "함께 성장"할 수 있느냐 하는 것이다. 나중에 항구적으로 편입시키기 위한 참조(references)를 지키면서 기존 데이터 소스로부터 받아 증식시키는 것도 역시 중요한 관점이 된다.

구체적으로 다음과 같은 성과들이 기대된다.

- 모델링 이론과 거기서 도출되는 도구, 데이터 내지 정보흐름(자동화 피라미드의 모든 단계 포함)
- 경제성 검증 절차 및 사례연구에 대한 신뢰
- 실제 효용성 있는 모델링 규정
- 보편적이고 도구지원이 되는 메타-모델

5.3.1.2 연구와 혁신에서 추구한 결과들

없어서는 안 될 토대라면 생산 주변 환경에서 기계 제작, 전자공학, 전산학 등에서의 모델에 대한 이해의 통일이다. 장기적인 목표는 생산을 담당하는 기업들이 경제적이고, 편익을 키우며 양방향의 모델링을 할 수 있는 역량을 갖도록 하는 것이다. 그렇게 럼으로써 가상세계의 요소들이 현실 세계와 함께 의미론적으로 높은 수준에서 여러 전문 분야를 함께 아우르도록 연결하여 내적 주문 이행의 효용과 의사결정의 안전성을 유의미하게 향상시킬 수 있다.

기대할 수 있는 결과들은 다음과 같다.

- 모델링 이론과 거기서 도출되는 도구, 데이터 내지 정보 흐름(자동화 피라미드의 모든 단계 포함)
- 경제성 검증 절차 및 사례연구에 대한 신뢰
- 실제 효용성 있는 모델링 규정
- 보편적이고 도구지원이 되는 메타-모델

5.3.1.3 핵심 사안들과 주요 일정

방법론
4.1 도구에 대한 요구를 포함한 복잡한 시스템에 대한 모델링 이론 제1차 버전 4.3 현실적 유용성 있는 적용사례와 모델링 규정 4.4 개별 사례 내지 적용 사례들에 대한 경제성 검증 절차
솔루션
4.2 “최우수 등급(Best in Class)” 기업들 찾아 확인하기(identification) 4.5 모델링 프레임워크의 제1차 버전 4.6 보편하고 도구 지원되는 메타-모델
전제조건들
4.a 산업 분야들을 아우르는 공동체(community) 확립 4.b 메인스트림에서 모델링을 받아들이는 분위기 창출 4.c 모델링 깊이의 척도화, 수직 및 수평적 일관성 확보를 위한 도구와 방법론 4.d 현실세계와의 조화 속에서 1차 참조아키텍처 이용에서 도구지원을 위한 개념

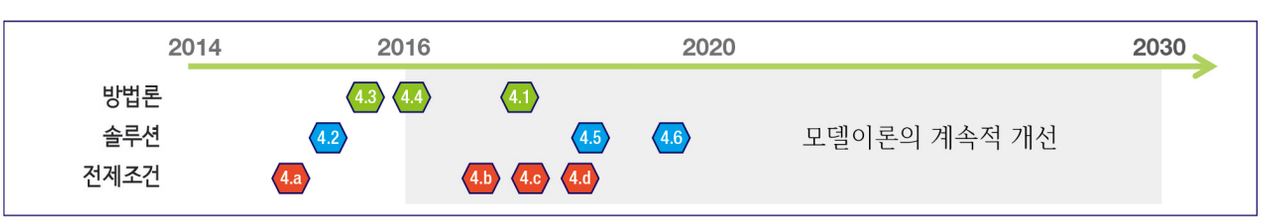


그림 5: 생애주기 전체에 걸쳐 시종일관하는 엔지니어링의 연구를 위한 핵심 사안과 주요 일정

5.3.2 시스템 엔지니어링

5.3.2.1 연구와 혁신 내용

시스템 엔지니어링은 여러 전문분야를 아우르며 언제 어디서든 접근할 수 있는, 모든 관점을 다 고려하는 기술 체계 개발 원칙이다. 학제간 원칙의 시스템을 핵심에 두고 개발활동 전체를 포괄한다.

고려해야 할 사항들은 다음과 같다.

- 제품, 프로세스, 생산체계 등의 통합 개발. 처음부터 하나의 긴밀한 상호작용 속에서 모든 관점들을 개발하고 제품의 시장주기를 벗어나 지속적으로 계속 개발해 나가도록 해야 한다.
- "초기" 국면에 계획의 결정에 대한 검증과 확인이 이루어져야 하는데, 의도했던 기능들 중 어느 것들이 나중에 기계적, 전기적으로 펌웨어와 소프트웨어 혹은 서비스로 대체될 수 있는가 하는 관점에서도 마찬가지다.
- 시스템 경계(부분시스템, 기계/프로레스, 생산시설, 공장)와 기업 경계를 넘어 중요한 데이터들과 프로세스 모두의 사용 가능성 확장 및 축소 가능한(scalable) 시스템 안에 그 모든 것 갖춰 두기.
- 점증하는 복잡성과 확장 및 축소 가능성(scalability) 극복을 위한 시설과 시스템의 모듈화와 재사용
- 시설과 시스템 개발 내지 엔지니어링과 운영 단계로 투입하며 얻은 경험들의 피드백
- 이용된 방법들로 상호 정보교환이 가능한(interoperable) 엔지니어링-사슬이 생겨나는데, 이 사슬은 엔지니어링, 시뮬레이션 체계와 운영을 위해 이용된 시스템들의 안전한 이용(데이터 교환, 롤모델, 액세스 절차)과 사업모델(이를테면 라이센스, 정산 시스템들)에 이들을 버전에 맞춰 사용하는 것을 가능하게 한다.

5.3.2.2 연구와 혁신에서 추구한 결과들

목표는 계속 구체화되어 가는 경향 속에서 복합 시스템 전체를 아우르며 학제간의 계획이 확립된 개발 방법과 기계역학, 전자공학, 소프트웨어기술, 설비 및 프로세스 기술 등과 같은 해당 도메인에 상응하는 도구 환경들로 이어지도록 하는 것이어야만 한다.
시스템 엔지니어링은 – 특히 중소기업에서 – 더 많이 수용되고 점점 더 협조적으로 이용될 수 있어야 한다. 그렇게 함으로써 인더스트리 4.0 시스템의 복잡성이 점점 커가는 것을 극복하고, 프로젝트가 엔지니어링 그룹과 생산 그룹 안에서 효율적이고 효과적으로 처리될 수 있다.

기대할 수 있는 결과들은 다음과 같다.

- 서로 조율된 방법들과 조율된 툴키트 및 개발환경
- 시스템 및 지역과 무관한 도구의 독립적 이용
- 실용적인 인터페이스의 의미론(semantic)
- 복잡계 안에서 전문분야들을 아우르고 요구사항들에 대하여 시종일관하는 매니지먼트

5.3.2.3 핵심 사안들과 주요 일정들

방법론
5.2 실용성 있는 가이드라인과 직업교육 및 계속교육 프로그램 5.3 복잡계 안에서 수직적 통합을 따라 편재하는 요구 매니지먼트 5.6 스마트 기술 체계 개발을 위한 업종들을 아우르는 참조모델
솔루션
5.1 제1차 서로 조율된 방법세트; 제1차 상호 조율된 툴키트 5.4 시스템, 클라이언트, 지역 등과 무관한 도구-사용 5.5 실용적인 인터페이스 의미론
전제조건
5.a 초기 개발단계에 기술 및 생산 기술상의 요구들 수용 4.1 복잡하고 자동화된 생산기술 체계들의 개발을 위한 제1차 모델링 이론 5.c 기술 체계들에 대한 전문분야들을 아우르는 모듈화 5.d 제품에 대한 생산중심 기술(서술)을 위한 기존 표준들의 확장

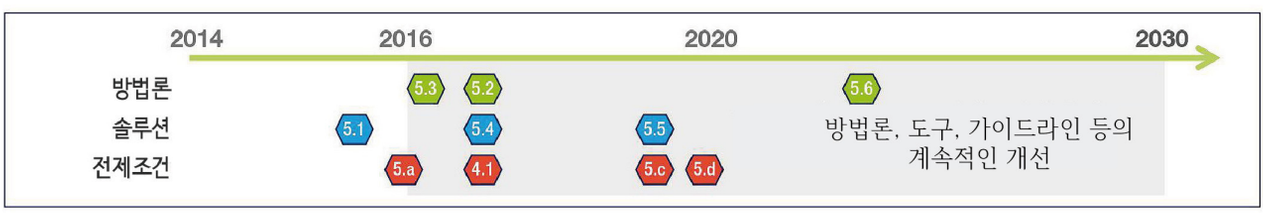


그림 6: 주제 "시스템 엔지니어링" 연구를 위한 핵심 사안들과 주요 일정

5.4 주제 영역 : 수직적 통합과 네트워크화된 생산 시스템들

수직적 통합이란 어떤 생산 시스템의 여러 계층 단계(예컨대, 작동장치와 센서단계, 조종단계, 생산단계, 매뉴팩처링과 실행 단계, 기업계획 단계 등)에 있는 여러 가지 IT-시스템들을 하나의 편재한 솔루션으로 통합하는 것을 말한다.

5.4.1 센서 네트워크

5.4.1.1 연구와 혁신 내용

센서 데이터 분석의 배경에 있는 핵심 동기는 어느 (기술) 프로세스를 통해 그 프로세스의 조종, 제어, 진단, 경고발동 등을 위한 베이스로서 정보들을 끊임없이 모아 파악하자는 것이다. 그렇게 함으로써 이를테면 반응성 개입(reactive intervention)을 할 때 프로세스 파라미터를 조절할 수 있거나 진단할 때 기계결함을 신호로 알릴 수 있다.

다양한 센서들과 (경우에 따라 엄밀한 실시간 조건으로) 그 활용을 연계시키는 것(부분적으로 위험에 처한 실시간 조건으로)이 최대의 과제이다.

고려해야 할 문제들은 다음과 같다.

- 실제 현장에서 센서의 수가 매우 많을 때 데이터 수집은 어떻게 이루어질 수 있는가?
- 어디에서 중요한 데이터 조작(manipulation)이 실행되는가?
- 측정한 값과 나타나는 효과들 사이의 질적 및 양적 관계는 어떻게 인식하고, (상태)모델로 변환시킬 수 있는가?

5.4.1.2 연구와 혁신에서 추구한 결과들

인더스트리 4.0의 각종 시나리오에서는 현 상태와 결부된 감시와 통제의 실현 토대를 개발해야 한다. 센서데이터를 처리하는 중심요소[층위(layer)]에 대한 접근은 가능한 한 표준화되어야 한다. 물리적인 센서 층위에 대한 지식을 가질 필요 없이 센서의 데이터에 대한 접근을 허용하는 소프트웨어 아키텍처가 생겨난다[캡슐화 (encapsulation) ; 통신에 잠시 장애가 있어도 핵심 기능을 유지하는 능력]. 특히 무선 센서의 포함에 대해 고려해야 한다. 작동과 구성은 그래픽으로 그리고 플럭-앤-플레이(Plug-and-play) 장치를 이용하여 쌍방향으로 실현되도록 해야 한다. 여러 센서 데이터 흐름을 데이터융합(data fusion)의 의미에서 평가하는 일이 적용 사례마다 개별적으로 개발될 필요 없이 가능해야 한다. 센서 네트워크의 자율성 정도를 가급적 높게 하려면 센서들에 의미론적 기술(description)을 가미해야 한다(Semantic Sensor Network Technologie).

기대되는 성과들은 다음과 같다.

- 신뢰할 수 있는 가이드라인의 유도를 가능케 하는, 시스템상태/제품상태의 확인을 위한 정교한 확장형 모델
- 프로세스 및 프로세스 아웃풋의 품질에 기반을 두고 실시간 데이터들에 따른 제작프로세스의 온라인-제어
- 사례 특정적이고, 수용적인 측정전략을 품질관리에 도입
- 업종들을 아우르는 공동체(community) 구축

5.4.1.3 핵심 사안들과 주요 일정들

방법론
6.1 보편적 인터페이스/메타 데이터를 이용한 센서의 기술(description)을 통한 센서 데이터들에 대한 투명한 접근 6.3 자체 조직화하는 통신개념(communications concept)
솔루션
6.2 플럭-앤-플레이 장치를 이용한 양방향(interactive) 작동 프로세스 6.4 분산 데이터 분석(Fog-Computing) 알고리즘, 클라우드-컴퓨팅-원리를 이용한 융합(Amalgamation) 6.5 복합 제작 프로세스에 대한 동적(dynamic) 제어, 경영학적 프로세스들을 이용한 수직적 통합
전제조건들
6.a 지역 데이터 수집-파악, 가공 및 분산 센서 그룹(knot)에 저장 6.b 네트워크화된 생산시스템들(사물인터넷과 서비스) 6.c 에너지를 자체 조달하는 센서들의 사용 가능성

그림 7: 센서 네트워크 연구를 위한 핵심 사안들과 주요 일정

5.4.2 지능형 – 유연성 – 가변성

5.4.2.1 연구와 혁신 내용

스마트 생산 시스템들은 조정이 가능하다. 이는 다시 말해 통합된 모델 지식을 바탕으로 그 환경과 상호작용하며 스스로 환경에 적응한다는 뜻이다. 스마트 생산 시스템은 탄력적이다. 끊임없이 변화해가는 환경에서 기대치 않았던, 개발자가 고려하지 않았던 상황까지도 성능 수준을 저하시키는 일 없이 해결한다. 뿐만 아니라 예측까지도 한다. 경험지식을 바탕으로 여러 가지 영향들이 미치는 효과들을 예측하는 것이다. 게다가 궁극적으로는 사용 친화적이기도 하다. 사용자의 여러 가지 행태들뿐만 아니라 여러 가지 정보의 수요까지도 고려하고 그에 따라 스스로 적응하는 것이다. 유연성이란 제한된 통로 안에 있는 프로세스 내지는 시스템들이 가능한 폭넓은 스펙트럼의 요구들을 충족시키도록 계획되었다는 말이다. 생산 환경에서 이것은 인간과 기계와 생산시스템 및 가치창출 네트워크들이 여러 가지 제품들 혹은 그 변형제품의 제작과 관련하여 유연하게 상호작용한다는 뜻이다. 가변성이란 유연성 통로의 한계를 연장시킨다는 뜻이다. 그렇게 함으로써 프로세스와 시스템들이 건설적인 단계를 거치면서 변화되거나 수정될 수 있다. 생산 주변 환경에서 기계와 관련하여 이는 새로운 제품과 변형제품들 제작을 위한 '단순한' 개조를 뜻하고, 생산체계와 관련하여서는 구조물의 '단순한' 변경을 의미한다.

고려해야 할 사항으로는 다음과 같은 것들이 있다.

- 글로벌 목표에 직·간접적으로 영향을 미치는 유연화 및 가변 가능성들에 대한 확인(identification), 형식화(formalization) 및 기술(description)
- 유연하고 가변적인 생산 구축을 위한 단위(모듈)의 인터페이스와 성능(능력)의 표준화
- 사회적, 윤리적, 생태적, 인체공학적(ergonomic)으로 미치는 영향

생산 환경에서 자율 시스템들의 엔지니어링과 테스트. 자율 체계 개발자는 그에 상응한 교육과 훈련을 받아야만 한다.

5.4.2.2 연구와 혁신에서 추구한 결과들

지능화(스마트화)를 통해 제품과 생산체계들은 새로운 기능을 발휘하여 이용자들의 부담을 덜어준다. 개발, 엔지니어링, 유지-보수 및 생애주기 매니지먼트를 개선하고 제품과 생산체계들의 신뢰성, 안전성, 사용성 등을 향상시킨다. 더 나아가 에너지와 재료와 같은 자원들을 더 효율적으로 투입함으로써 극도로 유연하면서도 쉽게 가변 가능한 생산프로세스와 생산체계들을 가능하게 만든다.

기대할 수 있는 성과들은 다음과 같다.

- 생산 과정 내에서 자율적이고 재사용이 가능한 단위(모듈)의 확인과 작업 모델을 위한 요구들과 잠재력의 유도
- 중앙 집중 지능과 분산 지능을 위한 탄력적이고 신뢰성 있는 알고리즘
- 생산 주변 환경 속에서 스마트 체계들 사이의 교섭을 위한 전략
- 직감적인 인간-기계-상호작용을 위한 기술과 적용 사례
- 유연하고 가변적인 생산체제로의 이동전략

5.4.2.3 핵심 사안들과 주요 일정들

방법론
7.1 유연화 가능성과 가변 변형 가능성 및 작업 모델에 미치는 그 영향 분석 7.2 유연하고 변형 가능한 생산의 방향으로 이동 전략 7.3 자율 체계의 엔지니어링과 테스트를 위한 방법들과 기술(description) 수단
솔루션
7.4 창의적인 인간–기계–상호작용을 위한 기술과 적용 사례 7.5 생산 환경에서 스마트 시스템들 사이의 협조 표준화 7.6 중앙집중적 및 분산적 지능을 위한 탄력적이고 신뢰성 있는 알고리즘
전제조건들
3.2 전략적 목표 – 목표위계 체계 – 프로세스 모델링 9.5 인더스트리 4.0 실행에 해당 직원들과 노사 협의회의 노동자 측 대표의 참여를 위한 모델 3.3 복잡성의 극복과 적용 가능성

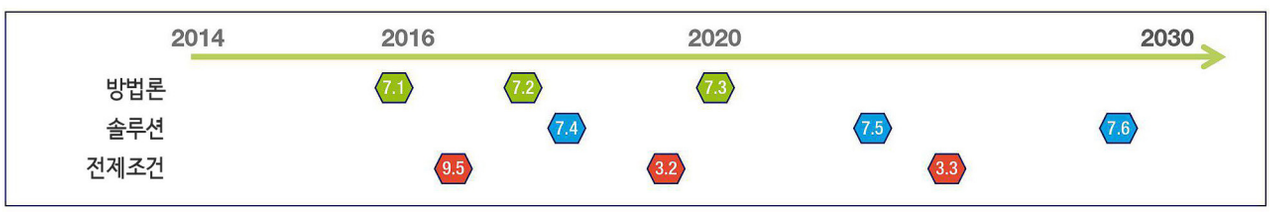


그림 8: 지능 – 유연성 – 가변성 연구를 위한 핵심 사안들과 주요 일정

5.5 주제영역 : 노동의 새로운 사회적 기반시설

제3작업부는 그 역량과 경험에 비추어 볼 때 연구개발의 필요성에 대해 단지 기술적 관점에서만 그 언급이 가능하다. 따라서 이 장의 내용에 대하여 학술 자문단으로부터 도움을 받았다.

5.5.1 보조체계의 멀티 모드

5.5.1.1 연구와 혁신 내용

이 주제는 원칙적으로 인간–기계–인터페이스에 대한 인간 중심적 해석을 다루는 것이다. 인더스트리 4.0의 영역 안에서 인간–기술–상호작용이 달라진다. 기계들이 인간에 맞춰 적응하지, 그 반대가 아니다. 멀티 모드, 이용 편의적인 이용자 인터페이스를 갖춘 스마트 산업 보조시스템은 일하는 사람들의 작업 과정을 지원하고 디지털 학습기술을 일자리에 직접 접목시킨다.

상호작용 설정 때 고려해야 할 관점들은 다음과 같다.

- 인풋/아웃풋의 명확한 확인 가능성
- (이롭지 못한 조건 하에서도) 인식 가능 여부
- 확인 가능성, 착오에 대한 안전성
- 업무 적합성
- 자기 기술(記述) 능력
- 제어 가능성
- 기대 충족성

5.5.1.2 연구와 혁신에서 추구한 결과

공장에서 지능형 보조 시스템들의 지원을 받는 공동 작업의 새로운 형식들이 생겨나야 한다. 증강 현실(augmented reality), 이중현실(dual reality), 동기화된 복수 세계 실시간 관련한 방법과 기술들 (즉 실제 현실의 공장들과 함께 감각운동성이고 의미론적인 공장모델)로 하여금 오류탐색과 같이 고도로 복잡한 요소들에 대한 공동의 원격

제어가 가능해진다. 그렇게 함으로써 일하는 사람들의 공동작업 모습은 근본적으로 변화된다. 이를테면 조절된 소셜 네트워크와 소셜 미디어를 통한 협력과 공동작업은 기업 및 교육 수준의 한계를 초월하여 가능해진다. 쉽게 받아들일 수 있는 상호작용 체계들은 일하는 사람 전체의 이질성을 감안한다. 왜냐하면 이 시스템들은 개개인이 원하는 대로 할 수 있도록 그리고 특별한 목표 그룹들을 위해 개발되었기 때문이다.

기대되는 성과들은 다음과 같다.

- 기계적 생산 과정 시뮬레이션의 지원을 위한 가상 인간 모델의 통합
- 안정된 시스템 운영 조건인 근로자들의 경험지식 활용과 유지를 위한 전제조건들
- 근로자들을 위한 시스템 현황 평가를 통한 투명성 확보 및 유지
- 근로자 모든 층을 대상으로 하는 자격 및 능력 관리
  - 디지털 학습 기술의 지원
  - 디지털 학습기술의 지속적인 개발

5.5.1.3 핵심 사안들과 주요 일정들

방법론
8.1 작업 단계들에 대한 유의미한 멀티 모드 지원을 위한 산업적 적용 사례들의 정의 8.3 상호작용 평가를 위한 일반적 방법론
솔루션
8.2 제품 생애주기의 모든 단계에서 업무 관련 상호작용 설정을 위한 실무에 실제 도움이 되는 가이드라인 8.4 인간–기계–인터페이스 설정 지침들의 정교화
전제조건들
8.a 산업 적용 분야에서 증강현실 내지는 듀얼 리얼리티 안의 응용프로그램을 위한 실용적인 단말기 8.b PLM 시스템의 네트워크화와 AR/DR(증강/디지털 현실) 적용을 위한 엔지니어링 개념들의 계획 8.c 고용관계의 유연화를 위한 준비 8.d 전체 근로자의 이질성을 감안한 상호작용 체계 설정을 위한 준비 8.e 근로자 그룹 전부를 위한 자격증 취득 가능성의 확보

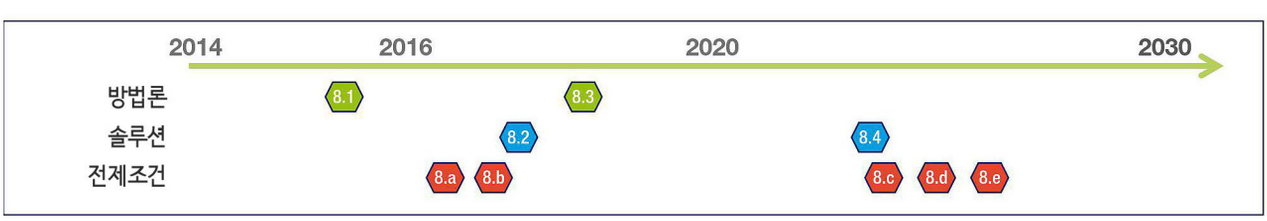


그림 9: 멀티모드 보조시스템 연구를 위한 핵심 사안과 주요 일정

5.5.2 기술의 수용과 작업 형태

5.5.2.1 연구와 혁신의 내용

인더스트리 4.0은 생산에 종사하는 근로자들에게 받아들여져야만 한다. 이에 대한 전제조건은 동료들 간의 유연성을 가능케 하고 그들의 창의성과 학습 능력을 지원할 수 있는 근로조건을 갖추는 것이다. "멀티 모드 보조 시스템"이 이를 위한 기술적 전제조건을 제공한다. 이 주제영역의 핵심에 속하는 것으로는 교육을 통한 자질개발, 작업조직 및 인더스트리 4.0 시스템의 범위 안에 있는 작업수단 조성 등이다.

고려해야 할 사항으로는 다음과 같은 것들이 있다.

- 기술과 조직 및 근로 인력이 서로 체계적으로 조율되어야만 하는 사회·기술 체계로서의 인더스트리 4.0에 대한 철저한 이해
- 일하는 사람들의 수용성, 능력, 편안함 및 건강을 지원하는 작업구성
- 도입 과정에 근로자들과 노조 대표자 연합의 참여

5.5.2.2 연구와 혁신에서 추구한 결과들

근로자들이 맡는 업무의 스펙트럼이 확장되어야 하고, 그들의 자질과 활동 영역도 향상되어야 하며 지식에 대한 접근도 확실하게 개선되어야 한다. 이는 생산 작업의 새로운 형태의 공동 형태가 가능하고 시스템의 특징에 맞추는 게 필요하다는데에 그 출발점을 두고 있다. 이에 따라 인더스트리 4.0은 생산 활동의 매력을 높이고 머지않아 현실이 될 전문 인력의 부족에 대응할 기회를 제공한다. 궁극적으로 작업구성에서 상황에 부응하는 조치들을 통해 노화되어 가는 근로자들에게 필요한 요구사항들이 늘어나는 것에 대응하기 위한 양질의 전제조건들을 마련하는 것이다.

기대되는 결과들은 다음과 같다.

- 일하는 사람들의 수용성, 능력, 편안함 및 건강을 지원하는 활동 및 업무 구조를 위한 개념
- 하나의 일자리에서 계획하고, 조직하고, 실행하고, 조종하는 활동들의 통합을 위한 제안들
- 요구조건이 별로 없는 일상적 업무와 요구조건이 까다로운, 문제해결 업무들 사이의 적절한 관계를 위한 모델
- 작업조직화를 지원하는 학습 촉진 작업수단
- 인더스트리 4.0의 실현프로세스에 해당 근로자들은 물론이고 노사 협의회의 노동자 측 대표까지 참여하는 모델

5.5.2.3 핵심 사안들과 주요 일정들

방법론
–
솔루션
9.1 적절한 활동구조 및 업무구조 개념 9.2 계획 활동, 조직활동, 실행활동, 조종 활동들의 통합을 위한 제안 9.3 요구조건이 별로 없는 일상적 업무와 요구조건이 까다로운, 문제해결 업무들 사이의 적절한 관계를 위한 모델 9;4 작업조직화를 지원하는 학습 촉진 작업수단 9.5 인더스트리 4.0 실행에 해당 근로자들은 물론이고 노사 협의회의 노동자 측 대표까지 참여하는 모델
전제조건
–

그림 10: 기술 수용 및 업무 구성을 위한 핵심 사안들과 주요 일정

5.6 주제영역 : 인더스트리 4.0을 위한 크로스오버 기술(분야를 아우르는 기술)

이 장에 소개되는 크로스오버 기술 목록은 완성된 것이 아니고 확장될 수 있다. 더 많은 기술들을 추가하여 확장시킬 때 중요한 것은 해당 크로스오버 기술이 인더스트리 4.0을 위하여 어떠한 의미를 갖고 있는가를 명확히 하여야 한다는 것이다.

5.6.1 인더스트리 4.0 시나리오를 위한 네트워크 통신(network communication)

5.6.1.1 연구와 혁신의 내용

이 주제 영역에는 사이버-물리-시스템에 포함된 고정된 요소들과 유동적 요소들 사이의 네트워크통신이 자리한다. 이 요소들은 생산현장에 위치하는 서비스 시스템과 생산성 시스템들이며, 맞물려 있는 공급 사슬을 통해 생애주기의 단계들을 넘어서는 데이터 교환이 이루어지는 기업들의 배경-시스템에 위치한다.
고려해야 할 사항들은 다음과 같다.

- 사무실과 생산 현장에서 요구되는 사정에 적합한 무선 통신의 사용
- 다양한 유무선 통신체계들과 소유 관계가 다양한 체계들의 공존
- 다양한 무선 통신체계들 사이의 상호 정보 교환 가능
- 시스템 환경설정(configuration)의 변화에서 미리 예측하는 영향분석
- 사용 가능한 주파수대에서 전 세계 차원의 제품들의 투입
- 대역폭, 결정론(Deterministic), 실시간 등의 요구 매니지먼트
- 공동사용 가능한 엔지니어링-사슬에서 문제없이 확장과 축소 가능(scalable)하고 편재한 이용
- 보안과 안전(Security und Safety)

5.6.1.2 연구와 혁신에서 추구한 결과들

인더스트리 4.0의 생산 시나리오에 도입하기 위한 요구사항들을 충족시키기 위해서는 산업계를 아우르는 사용이 가능한 네트워크화와 접속솔루션이 개발되고 평가되어야 한다.

특히 전달역량, 탄력성, 보안과 안전 및 신뢰성, 경제성, 국제적 통용성 등에 대한 요구사항들이 이 주제영역의 목표들이다.

기대되는 성과들은 다음과 같다.

- 솔루션의 표준화를 통하여 인더스트리 4.0의 비용의 효율성과 수용을 확보하는 바, 그 표준화는 상호운용, 등급분류, 비용에 대한 민감(cost sensitivity) (예컨대 소량의 가격 높은 센서들에 대한 것 포함)과 요구의 수용 등의 목표를 고려하는 것이다. 표준에 적합하다는 자격을 취득하는 것은 통상의 개발과정에서 이용 가능한 제도에 의해 가능하고, (기술적으로나 지역적인 이유로도 실시될 수 없고) 비용을 증대시키는 인정증서를 취득할 필요는 없다. 여기에는 이를테면 CE "제조자의 제품 표준 적합성 자기 선언"(self declaration of conformity) 같은 공개 절차를 따를 수 있다.
- 현재와 미래의 가능성들에 대한 평가
  - 인더스트리 4.0-맥락에서 공공 네트워크
  - WLAN-기술과 인더스트리 4.0-맥락의 블루투스(Bluetooth) 같은 가능한 대안들
  - 인더스트리 4.0 맥락에서 근접장-기술(Near-field technology)
- 다음 요구들에 대한 확인
  - 무선 솔루션, 공공 인터넷망의 네트워크 기술, 소유권 문제 솔루션 및 가능한 대안들의 확인 등
  - 건물, 프로세스 기술 혹은 사회기반 시설(에너지, 물, 운수)과 같은 애플리케이션 분야

5.6.1.3 핵심 사안들과 주요 일정들

방법론
10.1 공공 통신망의 재디자인, 공-사 파트너십에서 새로운 통신기술 + 주파수 계획 유도 10.3 SDN-베이스에 네트워크 리소스들의 가상현실화(virtualization)를 위한 표준화 10.5 통신표준, 근거리장과 적응성 안테나 시스템(adaptive antenna system)의 혁신적 개발
솔루션
10.2 공공 통신망에 100Gbit/s 5G 네트워크 인프라구조 10.4 생산적인 용도에 SDN 투입 10.6 인더스트리 4.0 적용에 신 통신표준, 근거리장기술, 적응성 안테나 체계 등의 사용
전제조건들
10.a 5세대(5G) 네트워크 인프라 및 신 통신표준과 근거리장 기술의 디자인과 표준화 10.b SDN-베이스의 네트워크-가상현실화를 위한 표준하드웨어 사용 가능성 10.c 유연한 통신네트워크를 위한 새로운 안테나 기술의 산업화 10.d 간섭의 검출(interference detection), 간섭의 억제 및 회피를 포함한 공존 프로세스의 표준화

그림 11: 인더스트리 4.0-시나리오를 위한 네트워크 통신 연구에 대한 핵심 사안들과 주요 일정

5.6.2 마이크로 전자공학(microelectronics)

5.6.2.1 연구와 혁신 내용

마이크로 전자공학은 인더스트리 4.0에 있어서 생산 프로세스와 물류 프로세스를 스마트하게 제어하고 감시하며 확인할 수 있는 CPS-하드웨어를 제공해주는 기반이다. 인더스트리 4.0 시나리오 요소들을 단계적으로 실현하기 위해서는 마이크로 전자공학에서 광범위의 툴-키트를 마련한다. 이러한 의미에서 마이크로 전자공학은 "무어(Moore)의 법칙"은 물론이고 "무어의 법칙 이상"(More than Moore)의 기술을 위한 것이다. 이 기술에는 중요한 의미가 부여되는데, 시스템 통합(이를테면 웨이퍼레벨, 자체진단능력, 에너지 효율성 등을 기반으로 한 3D-통합) 기술이 여기서 핵심 역할을 하기 때문이다.

매우 중요한 연구 주제들은 다음과 같다.

- 센서와 작동장치를 포함한 마이크로-전자-기계 체계(MEMS)
- 특수 프로세스, 특수 실시간 마이크로 콘트롤러, 고성능 최소 동력 소비의 하이테크-저장장치 및 멀티-코어-아키텍처 등을 포함하는 칩에 내장한 시스템
- 효율적으로 작업하는 작동체계를 위한 전력전자(power electronics)
- 무선통신(저출력, 저지연 low power, low latencty)
- 가능한 최대 수확의 에너지수확(Energy Harvesting)
- 시스템 통합
- 내장 IT-보안 아키텍처
- 강건성(robustness)과 내노화성(aging resistance)

5.6.2.2 연구와 혁신에서 추구한 결과

마이크로 전자공학은 유연성, 생산성 향상, 비용절감 등 인더스트리 4.0의 목표들을 실현하는 핵심 기술 중 하나다. 여기에 전제되는 것이 최적화된 특수 전자 하드웨어와 스마트 소프트웨어의 공동작용이다. 인더스트리 4.0 시나리오의 실현은 적절한 마이크로전자공학 키트와 시스템의 사용 가능성에 달려 있다. 이에 따라 마이크로 전자공학의 새로운 요소들을 개발하고 기존 요소들을 인더스트리 4.0의 환경에 적응시키기 위한 지속적인 연구와 개발의 필요성이 있다.

5.6.2.3 핵심 사안들과 주요 일정들

방법론
11.1 시스템 통합
11.2 강건성(robustness)과 내노화성(aging resistance)
11.3 가능한한 최대의 수율을 실현하는 에너지 수확(Energy Harvesting)
11.4 칩에 내장한 시스템, 실시간 기능 특수 마이크로 콘트롤러 및 하이테크-저장장치
솔루션
11.5 센서와 작동장치를 포함한 마이크로-전자-기계 체계(MEMS)
11.6 내장 IT-보안
11.7 효율적으로 작동하는 작동체계를 위한 전력전자(power electronics)
11.8 무선통신(저출력, 저지연 low power, low latencty)
전제조건들
5.1 상호 조율된 제1차 방법세트; 상호 조율된 제1차 툴키트
10.5 신 통신표준, 근거리장기술, 적응성 안테나 체계의 혁신적이고 지속적 개발

그림 12: 마이크로 전자공학 연구를 위한 핵심 사안들과 주요 일정

5.6.3 안전과 보안

5.6.3.1 연구와 혁신 내용

보안[정보보안(information security)]이라는 것은 인더스트리 4.0의 시설과 시스템 내 정보들의 사용성, 완전성, 신뢰 등을 안전하게 지키기 위한 것이다. 보안에서 중요한 것은 시설 내지 그 기능에 영향을 미치는 위험을 막아내는 일이다. 특히 공공연한 공격과 의도하지 않은 공격을 다 포괄한다. 안전하게 지켜야 할 대상은 모든 기능에 관한 정보인데, 운영기능뿐만 아니라 감시기능과 [안전(safety)과 같은] 보호기능도 포함한다.

시스템의 안전[기능적 안전성(functional safety)]에서 중요한 것은 적절한 조치들을 통해 기계나 시설의 기능에 의하여 사람이나 환경에 위험이 초래되지 않도록 하는 일이다. 안전은 기업의 안전한 운영을 위한 보호 기능의 일부다.

제품, 요소 그리고 인더스트리 4.0-시설을 위해 고려해야 할 보호 목적들은 다음과 같다.

- 사용성과 완전성
- 기업운영의 안전성
- 노우-하우(Know-how)의 보호
- 데이터 보호

인더스트리 4.0에서 아이디의 안전한 확인은 특별히 중요한 의미를 갖는다.

고려해야 할 중요한 사항들은 다음과 같다.

- 안전조치의 비용/효용 산정을 포함한 잠재 위협과 위험들에 대한 평가 절차
- 외부관계와 내부관계의 접점(인터페이스) 보호
- 시설 내 통신체계 보호
- 보안-허점 기업운영의 안전에 대한 위험들에 미치는 영향
- 개인정보 보호와 같은 것에 대한 법적 가이드라인과의 상호작용
- Security-by-Design
- 보안솔루션의 장기 사용 가능성
- 공격 탐지와 분석

또한 여기서 고려해야 할 경계 조건들로는 다음과 같은 것들이 있다.

- 해당 수평적 및 수직적 방향의 가치창출네트워크에 안전성 검토
- 구체적인 사용사례들(Use Case)에 대한 정리, 실용성이 확인된, 적용이 가능한 결과들에 즉각적인 전달
- "요소인 인간"에 대한 고려: 투명성, 사용성, 이용자 수용성, 개인정보 보호

5.6.3.2 연구와 혁신에서 추구한 결과들

오늘날 이미 다양한 표준들이나 기술들이 존재하지만, 산업 현장에서 아직까지 이용된 경우는 매우 드물다. 그 이유도 다양한데, 근본적인 면을 보자면, 자동화 솔루션의 중심 목적이 안전-기능이 아니기 때문이다. 공급자로서는 안전-관련 프로세스가 개발과 제작의 비용을 높이기 때문에 현재 이미 존재하는 지식들을 요구하지 않는 경우가 많다. 운영자 측으로 보면 보안-개념이 이용하는 근로자의 수용성과 비용과 관련하여 장애가 될 때가 많다.

관련자 모두로부터 높은 수용성을 얻기 위해서는 이용자가 사용하기 편리하고, 개발자는 툴을 통해 부담을 덜고 효율적인 보안-평가 방법들을 제공하는 그런 솔루션을 실현해야 한다.

기대되는 결과들은 다음과 같다.

- 이용이 편리하고 이용자 친화적인 보안-방법
- 산업 도메인들을 위해 확장과 축소가 마음대로 가능한 보안-사회설비
- 개개 요소의 보안 특성과 인더스트리 4.0 장치에 대한 그 요소들의 조합과 관련하여 적용이 간단한 방법과 평가 절차. 여기서 고려해야 할 점은 "Plug & Operate" (연결 즉시 가동) 시스템과 자율적이고 동적인 배치다.

- 안전성에 비추어 남아있는 위험에 대한 영향을 고려한 시설의 안전 기능에 대한 역동적 조사와 평가를 위한 방법들
- 보안의 표준화 준비
- 예컨대 CERT[컴퓨터 침해사고대응반 (Computer Emergency Response Team)]의 방법에 따른 보안공백이 생길 경우에 대한 적절한 조치·목록 작성

5.6.3.3 핵심 사안들과 주요 일정들

"보안과 안전"이란 주제에 대한 장기적인 연구 계획을 위한 방법론, 솔루션 및 그에 꼭 필요한 전제조건들에 대한 핵심사안과 주요 일정은 아직 나오지 않았다.

5.6.4 데이터 분석

5.6.4.1 연구와 혁신 내용

데이터 분석의 핵심 동기는 한편으로는 그와 함께 제공되는 (새로운) 지식의 생성 가능성이다. 다른 한편으로는 "실행 가능한(actionable)" 데이터 분석이 의사결정 지원과 자율적인 결정에 보탬이 된다(어떤 정보가 누구에게 그리고 언제 사용할 수 있게 하는가). 그렇게 되면 기업이 자체 제품의 품질과 생산과정의 효율성을 향상시키고 가능한 오류발생을 일찍 파악하는 데 도움이 된다. 이것은 특히 새로운 사업모델의 기반 구축에도 기여하는 바가 있다. 여기에서 적용되는 것은 예측 분석 방법이다. 이 방법들은 통계학, 기계 학습과 데이터 마이닝 등 여러 가지 기초 기술들을 아우른다. 현재의 측정치와 역사적 측정치는 물론 소셜네트워크(SN)에서 나오는 "비구조화된" 데이터들 같은 경우도 분석하여 거기에서 지금까지 알려지지 않은 맥락들을 밝혀낸다(descriptive analytics). 혹은 미래의 시스템 행태나 효과들에 대한 평가들도 도출해 낼 수 있다(predictive analytics). 새로 얻은 지식들은 궁극적으로 여러 가지 활동 대안들에 대한 평가를 가능케 하고, 그와 함께 시스템, 프로세스, 전략(prescriptive analytics) 등에 대한 지속적인 최적화도 가능하다. 데이터 분석을 바탕으로 한 활동지침이나 직접 조치들을 도출하는 일이 실질적인 도전이 된다.

"데이터 분석"이란 주제에 담긴 사항들은 다음과 같다.

- 데이터 조작(Data Manipulation)
- 상태 감시(State Detection)
- 예후 평가(Prognostic Assessment)
- 보고 생성(Advisory Generation)

5.6.4.2 연구와 혁신에서 추구한 결과들

데이터 분석을 실시하기 위해서는 준거목록 같은 것을 개발해야 한다. 이 목록은 다음 원칙들의 실현을 가능하게 한다.

- 구체적(물리적)인 소스(유래)에 대한 지식이 없는 상태에서의 데이터에 대한 액세스(캡슐화와 가상현실화)
- Plug & Use 원칙을 사용하여 새로운 데이터 소스를 표준화된 인터페이스에 연결 [(의미론적 기술(記述) (semantic description))
- 업종들을 아우르는 가치창출 네트워크 안에서의 데이터 이용
- 새로운 적용사례들의 도출을 허용하는 폭이 넓고 지속적 확장이 가능한 프로세스 기반의 구축
- 법적 안전(누가 어떤 데이터에 대하여 어떤 권리를 가지며 그 결과로 나오는 지식들)

이를 위해 소프트웨어 아키텍처와 그에 상응하는 인터페이스에 데이터 퓨전의 의미에서의 여러 데이터 흐름들의 활용을 메타 층위에서 가능케 하는 원칙들이 개발되어야 한다(개별 사용 사례들을 일일이 개발할 필요는 없다).

- 미래의 상태에 대한 예측이 가능한 상태 기술 모델들이 개발되어야 한다.
- 꾸준히 증가하는 데이터 분량을 효과적이고 효율적으로 분석할 수 있는 절차와 알고리즘이 개발되어야 한다.

5.6.4.3 핵심 사안들과 주요 일정들

방법론
13.2 생산 현장에서 데이터 분석의 활용을 위한 사용지침 13.4 생산 프로세스의 온라인 적응과 최적화를 위한 분석 기술들
솔루션
13.1 데이터 분석을 위한 기술과 적용 사례들 13.3 분산 데이터 분석(Fog-Computing)을 위한 알고리즘, 클라우드-컴퓨팅-기업을 이용한 융합 13.5 복잡한 제작 과정들에 대한 동적 제어, 경제 프로세스와의 수직적 통합
전제조건들
13.a 데이터에 대한 소유관계와 이용관계에 대한 법 제도적 정비 13.b 기술적, 예측적, 지시적 분석을 위한 이론 토대들

그림 13 : "데이터 분석" 주제에 대한 연구를 위한 핵심 사안들과 주요 일정

5.6.5 인더스트리 4.0을 위한 syntax(컴퓨터언어 문법)과 semantic(의미론)

5.6.5.1 연구와 혁신 내용

인더스트리 4.0의 각종 시나리오가 실현되기 위하여는, 참여한 대상들(이를테면 기계, 기계부품, 제품, 제품설명 또는 디지털 공장이란 의미에서의 자원 등)이 활동하는 주체들(이를테면 사람들, 소프트웨어-도구, 소프트웨어-에이전트, 가이드 시스템, 소프트웨어-서비스)에 의해 해석, 즉 확인되고 이해될 수 있어야 한다는 것을 전제로 한다. 그러기 위해 대상들의 그때그때 중요한 성격들이 하나의 모델 안에서 드러나는 특징의 형식으로 설명되고 또 역할과 관련하여 대상들의 과제가 설명되어야 한다. 그 토대는 전산모델이다. 이 모델들이 컴퓨터 안에서 처리될 수 있으려면 생산 환경에서 (데이터)모델, 모델체계, 설명모델, 계획모델 및 요소모델 등이 필요하다.

컴퓨터언어의 문법(syntax)이란 문서와 데이터 설명을 위해 통용될 수 있는 상징들(이를테면 알파벳, 숫자, 특수기호, 그래픽 심벌 등)과 이러한 기호들이 정교하게 서로 심벌의 사슬로 맞물리는 방식을 나타낸다.

의미론(언어)은 심벌들과 모델들 사이의 관계를 만들어낸다. 이를 통해 데이터가 정보로 되는 것이다. 이와 같은 관계는 이를테면 어떤 데이터에서 특정 기호사슬이 어느 모델의 특정한 특징을 기술하며, 이에 따라 어떤 속성이 이 특징을 더 자세하게 기술하고 또 어떤 특성(두드러진 점)이 그 속성을 가져도 좋은지에 대한 합의 같은 것을 나타낸다. 여기에는 특징들과 속성들 사이의 상호의존관계도 함께 기술되어야 한다.

5.6.5.2 연구와 혁신에서 추구한 결과

목표는, 인더스트리 4.0-시나리오를 위해 공동의 의미론으로서 형식적이고 컴퓨터 처리가능한 기술(記述)을 개발하고, 그것을 통하여 적용 차원과 이용 차원에서 도메인 특징적인 "언어"를 특성화하고,,이 언어로 하여금 모든 대상과 주체들 그리고 그 연결들(즉 프로세스, 통신네트워크와 가치창출 네트워크)을 통합하여 이용할 수 있도록 하는 것이다. 여기서 중요한 것은 정보의 흐름이 가치창출의 흐름 안과 흐름들 사이에서 언제 어디서나 접근할 수 있도록 보장하는 것과 언급된 기존의 표준들 위에 놓아서 이 표준들을 계속 발전시키고 표준에서 알려진 공백을 메워 나가는 일이다.

- 의미론과 문법은 제작자들을 망라하여 데이터 저장, 데이터 전달, 데이터 처리 등에서 상호 정보 교환 가능성을 열어준다.
- 표준화된 의미론적 기술은 자체 최적화 행태와 가치창출 흐름의 자동화를 위한 토대가 된다.
- 이로써 전체 생애주기에서 모델들 사이의 연결이 가능해진다(제품, 프로세스 및 자원들에 대한 기술이 엔지니어링 안에서 의미론으로서 존재하기 때문)
- 문법과 의미론의 도움으로 포괄적인 도구 내지는 도구-기능들을 만들어낼 수 있다.
- 의미론과 문법으로 인더스트리 4.0-요소들의 Plug& Produce 기능이 가능해지고, 그럼으로써 유연성과 적응성도 가능하다.

여기서 제기되는 과제는 한편으로는 인더스트리 4.0을 위한 구문론과 의미론의 구체화 작업에서 조속한 결과를 얻는 것이고, 동시에 (산업 족적 Industry Footprints의 의미에서) 가급적 커다란 적용분야에 도달하는 것이다.

5.7 주제들의 상호의존성과 관련성

각기 상이한 연구 주제들은 홀로 독립되어 있는 것이 아니라, 연구결과들간에 있어서 상호 종속성을 보인다. 그렇기 때문에 어느 연구 분야에서 나온 새로운 결과들이 다른 분야의 연구에 영향을 미친다. 제3작업팀에서는 근래 학술 자문단과 공동으로 주제들의 상호 영향과 중요성을 분석하였다. 여기서 가우제마이어(Gausemeier) 교수의 시나리오 분석 방법이 적용되었다. 이 분석의 결과는 올해 중에 발표될 예정이지만, 이미 현재 시점에서도 다음 주제들의 연구결과가 다른 연구 결과들에 커다란 영향을 미치리란 사실은 이미 확인될 수 있다.

- "유연성, 지능, 변화에의 대응능력"
- "센서 네트워크"
- "가치창출 네트워크의 프레임워크"
- "보안과 안전"

5.6.5.3 핵심 사안들과 주요 일정들

방법론
14.8 인더스트리 4.0에서 문법과 의미론을 다루는 관점의 사용지침서
솔루션
14.1 문법과 의미론 분야 표준화/규격 통일화에 대한 제1차 분석 14.2 문법과 의미론 분야에서 중요한 개념들에 대한 제1차 분석과 평가 14.3 문법과 의미론에 대한 인더스트리 4.0의 요구목록 14.4 적용 사례들과 가치창출흐름 베이스에서 연구주제들 정하기(naming) 14.5 표준화의 틈새들과 해당 표준화 수요를 표준화-로드맵에 담기 14.6 선정된 상호 정보 교환 가능성-설명 모델의 실현 14.7 기존 통신표준에 대한 통합개념, 소프트웨어-툴에 대한 개념 확장
전제조건
14.a 적용 사례들과 가치창출 흐름에서 도출된 데어터와 정보 모델에 대한 요구사항들

그림 14 : 인더스트리 4.0을 위한 문법과 의미론 연구에 대한 핵심 사안들과 주요 일정

참조 아키텍처, 표준화, 규격화

6. 참조 아키텍처, 표준화, 규격화

이 장에서는 여러 기관들의[2] 협력에 의하여 얻어진 인더스트리 4.0의 기반이 되는 참조 아키텍처와 거기서 도출되는 표준화 및 규격화의 불가피성을 정리하고 있다.

「플랫폼 인더스트리 4.0」에는 수많은 산하 위원회들의 활동들을 조율하는 역할과 일관된 노선을 지켜 유지하는 역할이 주어져 있다. 이에 따라 플랫폼은 여러 조직들과 단체들을 조율하며 그 사명을 다하고 있다. 아래에서 폭넓게 제시되는 검토 결과들은 독일 산업 경쟁력의 유지를 위한 중요한 발걸음이 된다.

6.1 머리말

인더스트리 4.0의 참조 아키텍처에 대한 토대가 되는 발상의 하나는 여러 가지 관점들을 공통의 모델 하나에 모은다는 것이다. 공장 내의 수직적 통합은 자동화 기계들이나 서비스 같은 생산수단들을 네트워크화하는 것을 의미한다. 인더스트리 4.0에는 새로운 관점에서 제품 내지는 부품의 도입이 추가되었다. 거기에 해당하는 모델은 이를 반영해야만 한다. 그렇지만 인더스트리 4.0은 훨씬 더 멀리까지 미친다. 가치창출 흐름 전체에 걸쳐 시종일관하는 엔지니어링이란 하나의 생산수단이나 부품과 관련하여 발생하는 기술적, 행정적 그리고 상업적 데이터들을 가치창출 흐름 전반에 걸쳐 한결같이 유지하고 언제든 네트워크를 통해 액세스 할 수 있다는 것을 의미한다. 인더스트리 4.0에서 제3의 관점은 개별 공장의 범위를 벗어나 가치창출 네트워크의 동적 형성을 가능케 하는 가치창출 네트워크 위의 수평적 통합이다. 이 관점들을 하나의 모델 안에서 설명하는 과제는 해결될 수 있었다.

2) VDI와 VDE의 측정 및 자동화기술협회(GMS)에서 함께 일하는 전문가들은 이 접근방법들을 작성하는 데에 탁월한 파트너십을 보여주었다. 여기서 특히 7.21 "인더스트리 4.0"과 7.20 "사이버 물리 시스템"의 양 전문가 위원회를 거명하고 싶다.
이와 나란히 ZVEI에서는 "거울(mirror)위원회"라는 SG2가 설립되어, 이 역시 공동검토에 기여하였다. 나아가 SG2내의 해당 대표자들을 통해 DKE(독일 전자공학 위원회)도 합류하여 표준화도 공동검토의 대상이 되었다.

결국 천분의 1초 단위로 스캐닝하는 제어회로들, 공통된 가치창출 네트워크 안에서 이루어지는 여러 공장들 상호간의 역동적 협조를 부가적인 상업적 문제들과 함께 하나의 모델 안에서 설명할 수 있어야 한다. 여기서 중요한 것은 다양한 애플리케이션 도메인들의 시각에서 관점들을 이해하는 것, 근본적인 것을 파악하고 하나의 공통된 모델에 통합하는 것 등이다.

참조 아키텍처 모델 RAMI4.0에 대한 실질적인 작업들이 시작되기 전에 기존의 원리들과 방법들 전체에 대한 개관이 그래서 꼭 필요하였다. 기존에 존재하며 이용 가능한 프로토콜이며 방법론들이 다수 있지만, 위에서 설명한, 인더스트리 4.0에 대한 통합적 시각에는 그 부분적인 측면만이 포함될 수 있다. 개별적으로 더 자세히 따져본 프로토콜은 다음과 같다.

통신 층위(layer) 실현을 위한 프로토콜

- OPC UA: Basis IEC 62541

정보 층위(layer) 실현을 위한 프로토콜

- IEC Common Data Dictionary (IEC 61360Series/ ISO13584-42)
- Merkmale, Klassifikation und Werkzeuge nach eCl@ss
- Electronic Device Description (EDD)
- Field Device Tool (FDT)

기능 및 정보 층위 실현을 위한 프로토콜

- 통합기술로서 Field Device Integration (FDI)

시종일관하는 엔지니어링을 위한 프로토콜

- AutomationML
- ProSTEP iViP
- eCl@ss (징표)

첫 단계에서 중요했던 것은 이 프로토콜들이 다음에 이어질 장들에서 소개되는 참조 아키텍처 모델에 맞는지 철저하게 검증하는 일이었다. 그 결과는 원칙적으로 긍정적이었는데, 다만 고찰된 개념들과 방법들에게는 더 상세한 다방면의 고찰이 필요하였다.

6.2 참조 아키텍처 모델 인더스트리 4.0(RAMI4.0)

인더스트리 4.0에 관한 토론에는 아주 다양한 이해관계자들이 모여든다. 각기 상이한 규격을 가진 프로세스로부터 공장 자동화에 이르기까지의 업계, 정보통신 기술과 자동화 기술 등을 가진 전문가, BITKOM, VAMA, ZVEI 및 VDI과 같은 산업단체, IEC와 ISO 같은 규격화 단체 및 그들의 (독일)국내 위원회인 DKE와 DIN 등이 그것이다.

인더스트리 4.0을 위하여 어떠한 표준이나 사용 사례, 규격 등이 필요한지에 대한 인식을 공유하기 위하여 통일된 아키텍처 모델을 레퍼런스(참조)로 개발하고 이것을 바탕으로 상호간의 관계나 세부사항이 논의될 수 있도록 할 필요성이 생겼다.

그 결과 발생한 것이 "참조 아키텍쳐 모델 인더스트리 4.0"(RAMI4.0)이다.

여기에는 인더스트리 4.0의 근본적인 측면들이 담겨져 있다. 여기에서는 IEC 62264에서 나온 계층단계에 대하여 최하부 단계에 제품 및 부품("Product")을 추가하고, 최상부 단계에는 개별 공장들을 넘어서는 "접속된 세상(Connected World)"을 추가하였다. 수평축은 시설 내지 제품들의 생애주기를 나타내고 있는데, 여기서 또한 유형과 실증(Type & Instance)이 구별되어 있다. 최종적으로 6개 층(Layer) 위에 인더스트리 4.0의 대표적인 구성 요소들을 구조화하여 나타내고 있다.

따라서 참조아키텍처의 특징은 생애주기와 가치창조흐름을 조합한 계층구조에 의하여 인더스트리 4.0의 요소를 정의하고 있는 점이다. 그럼으로써 인더스트리 4.0의 환경을 기술(記述)할 때 유연성을 최대한 확보할 수 있다. 이 프로토콜은 또 기능성의 의미 있는 캡슐화(역주: 통신에 잠시 장애가 있어도 핵심 기능을 유지하는 능력)도 가능케 한다.

이로써 참조아키텍처를 수단으로 유연성 정도가 높은 개념들을 기술하고 실현할 수 있는 전제조건들이 마련되었다. 그러면서 이 모델로 오늘날의 세계에서 인더스트리 4.0의 세계로 단계적인 이동이 가능해지며, 특별한 핸디캡과 요구조건들이 있는 적용분야에 대한 정의도 가능해진다.

참조아키텍처 모델 RAMI4.0은 DIN SPEC 91345로서 규격 통일(표준화)에 포함되었다.

6.2.1 요구조건과 목표

목 표

인더스트리 4.0은 "사물 인터넷과 서비스 인터넷"을 특수화 한 것이다. 그 구상에는 대략 15개 분야 업종들이 고려될 수 있다. 참조아키텍처 모델을 통해 그것들의 과제와 업무 흐름을 정리·분석하는 것이 가능하다. 어떤 사항이던 파악이 가능해야 (예컨대 표준화나 규격화와 관련한) 적확한 논의가 가능할 것이다. 또한 기존의 표준이나 규격들 중에 문제가 되는 것들로 어느 것들이 있는지 확인할 수 있어야 확장이나 수정의 필요가 있거나 또는 규격 및 표준이 흠결된 것을 알 수 있을 것이다. 모델 고찰에서 동일하거나 비슷한 사항에 대한 표준이 여러 개 존재한다면 참조 아키텍처 모델에서는 우선적인 표준 하나에 대해 논의할 수 있다.

목표는 가능한 적은 수의 표준으로 해결하는 것이다.

표준의 준수

선택된 규격이나 표준은 그 안에 기술(記述)된 관념과 방법들이 인더스트리 4.0 환경에서의 적용에 어느 정도나 적합한지를 중심으로 검증된다. 초기의 인더스트리 4.0에 대한 적용에 있어서는 규격이나 표준의 일부만으로 충분하다. 이로써 제조자들을 아우르는, 인더스트리

4.0에 없어서는 안 될 솔루션의 실현과 도입을 가속화하고 아울러 소규모 기업들에게도 인더스트리 4.0의 실현을 더 빨리 완수할 수 있는 기회가 열릴 것이다.

사용 사례(Use Case)

참조아키텍처 모델에서는, 인더스트리 4.0의 사용 사례를 찾을 수 있는 가능성을 제시함으로써, 예컨대 해당 사용 사례에 없어서는 안 될 규격이나 표준을 확인할 수 있도록 한다.

위치 설정과 관계들

여러 가지 주제들이 참조아키텍처 모델의 부분 공간들 subspaces로서 설명될 수 있다. 인더스트리 4.0의 근본적인 먹거리는 이를테면 저 부분 공간들 사이의 관계들을 전자 차원으로 파악하여 처리할 수 있게 하는 것이다.

상위 규정들의 정의

참조아키텍처 모델로 인더스트리 4.0의 상위 층위에서의 실현을 위한 규정들을 도출해낼 수 있다.

목표들의 개관

- 참조로서 일목요연하고 간단한 아키텍처 모델 설정
- 기존의 규격 및 표준을 찾아 확인하기
- 규격 및 표준의 흠결을 찾아 보정하기
- 중복된 표준 찾아 확인하고 우선적인 솔루션 정하기
- 적용 규격이나 표준의 수를 최소화하기
- 인더스트리 4.0의 조속한 부분적 실현을 위해 어떤 규격이나 표준의 부분집합을 특정하기("I4.0-Ready")
- 사용 사례 내용 찾아 확인하기
- 관계들의 확인
- 상위 규칙들의 개념 정의

6.2.2 참조아키텍처 모델에 대한 간략한 설명

인더스트리 4.0 공간을 가장 잘 표현할 수 있는 것이 3차원 모델이다. 이 모델은 그 근본을, 유럽 Smart Grid Coordination Group(SG-CG)이 정의하고 전 세계적으로 인정되고 있는 스마트 그리드 아키텍처 모델(SGAM[3])에 두고 있다. 이 모델은 인더스트리 4.0의 요구조건들에 맞게 수정, 확장되었다.

수직 축에서 데이터 복사, 기능 설명, 커뮤니케이션 활동, 하드웨어/자산 내지 사업프로세스 등과 같은 여러 시각들의 설명을 위한 층위(Layer)들이 이용되고 있다. 이것은 복잡한 프로젝트들을 조망 가능한 부분내용들로 클러스터화한 상황의 IT의 사고방식에 부응한다.

또 하나 중요한 기준이 제품 생애주기인데, 그 안에는 가치창출 흐름이 내포되어 있다. 이런 사항들은 수평 축에 설명된다. 그럼으로써 참조아키텍처 모델에서 생애주기 전체에 걸친 데이터 액세스의 편재성과 같은 종속적 특성들도 잘 설명될 수 있다.

세 번째 중요한 기준은 공장/시설 내의 기능들과 책임소재들의 위치설정으로 제3의 축에서 설명된다. 여기서 중요한 것은 기능적인 위계(class)이지 종래의 고전적인 자동화 피라미드에서의 기기의 분류라든가 위계 층위는 아니다.

3) CEN/CENELEC/ETSI SG-CG, Overview of SG-CG Methodologies, Version 3.0, AnnexSGAM User Manual, 2014

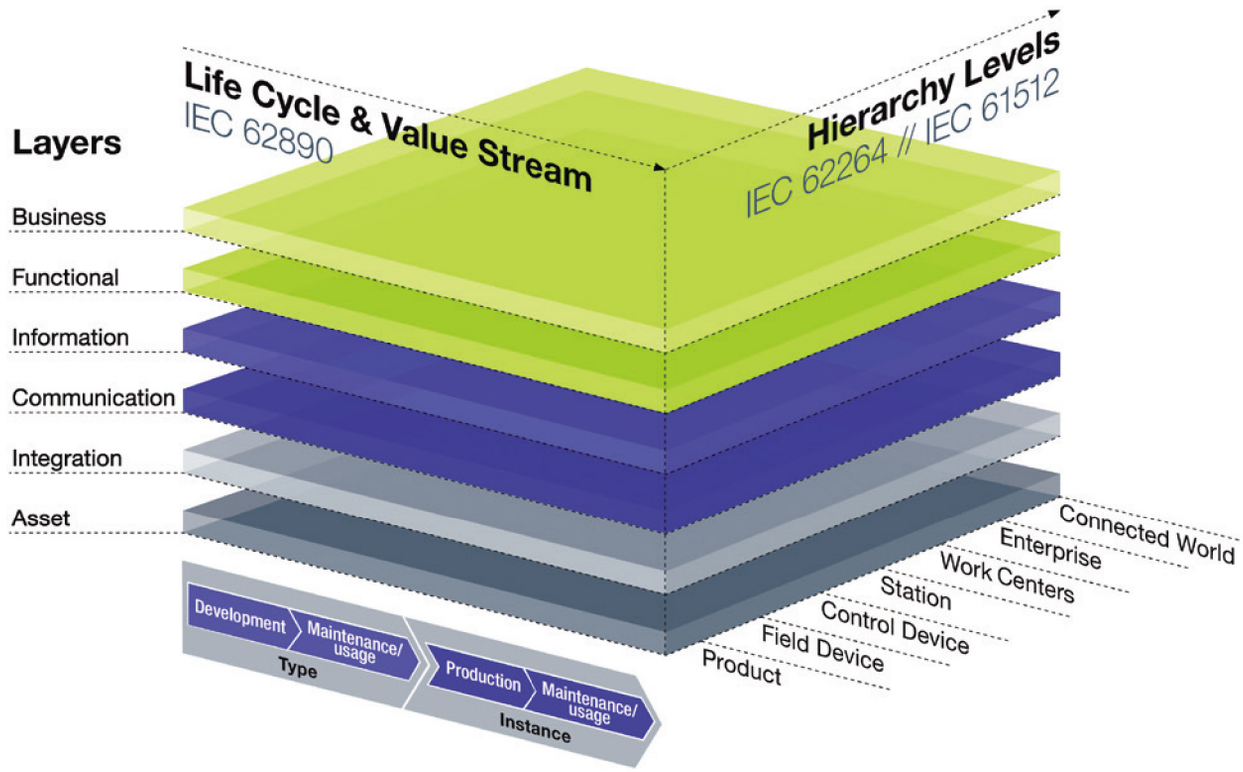


그림 15: 참조 아키텍처 모델 – 인더스트리 4.0(RAMI4.0)

6.2.3 참조아키텍처 모델의 층위(layers)

스마트 그리드 아키텍쳐 모델 (SGAM)은 기술되어야 하는 상황을 설명함에 있어 좋은 방법을 제시한다. SGAM은 발전으로부터 송전과 배전을 거쳐 소비자에 이르는 전력 공급망을 다룬다. 인더스트리 4.0에서는 제품개발 시나리오와 생산 시나리오가 핵심 위치를 차지한다. 말하자면 개발과정, 생산라인, 제조 기계들, 필드 장치(field devices)와 제품 자체까지 어떻게 만들어지고 또 그 기능이 어떤지 설명되어야 한다.

기계든 제품이든 모든 요소들에 대한 관심은 단지 전산기술과 통신기술적 기능들에만 국한하지 않는다. 어떤 기계 전체와 같은 어느 시스템의 시뮬레이션을 위해서는 그에 속하는 케이블, 선형드라이브 또는 그 기계적 구조까지도 함께 보아야 한다. 이들은 능동적 소통을 하지 못하는 현실세계의 부분들이다. 이들에 대한 정보는 가상 현실적 재현으로 존재해야만 한다. 이를 위해 이들 정보는 예컨대 2D-Code를 통해 수동적으로 데이터뱅크와 연결된다.

기계, 요소들, 공장 등을 더 잘 설명할 수 있기 위하여 SGAM의 요소(component) 층위(layer)를 자산(asset) 층위로 대체하여 하위 층위로 설정하고, 그 위에 통합(integration) 층위를 새로 추가한다. 그렇게 함으로써 가상현실의 재현을 위한 자산의 디지털 변환이 가능해진다. 통신(communicationr) 층위는 프로토콜과 아울러 데이터와 파일의 전달을 다룬다. 정보(information) 층위에는 중요한 데이터들을 담고 있고, 기능(functional) 층위에서는 꼭 필요한 (형식적 記述이 가능한) 기능들 모두를 다루며, 비즈니스(business) 층위에서는 중요한 사업 프로세스들이 다루어진다.

참고: *각 층위 내에서는 응집력(cohesion)이 높고, 층위와 층위 사이에는 연결이 느슨하다. event의 교환은 오직 이웃해 있는 두 개의 층위와 하나의 층위 내부에서만 일어날 수 있도록 한다.*

여러 개의 시스템들이 모여 그보다 더 큰 전체체계를 구성한다. 이때 개별 시스템들과 전체 시스템은 참조 아키텍처 모델에 따라야만 한다. 층위의 내용들은 서로 호환

성이 있어야 한다.
이제부터 개별 층위들과 서로 간의 관계에 대해 설명하기로 하겠다.

6.2.3.1 사업 층위(Business Layer)

- 가치창출 흐름에서 기능들의 완전성 확보
- 사업 모델 설정과 거기서 비롯하는 전체 프로세스 설정
- 법과 규제 관련 기본 여건들
- 시스템이 따라야 할 규정들의 모델링
- 기능 층위의 서비스들 조율
- 여러 사업 프로세스들 사이의 연결요소
- 전체 프로세스 진행을 위한 사건들 수용

비즈니스 레이어는 예컨대 ERP와 같은 구체적인 시스템과는 상관이 없다. 프로세스의 맥락에서 작동하는 ERP 기능은 전형적으로 (후술하는) 기능 층위에서 다시 나타난다.

6.2.3.2 기능 층위(Functional Layer)

- 기능들에 대한 형식적(일정 양식에 따른) 기술
- 여러 기능들의 수평적 통합을 위한 플랫폼
- 사업 프로세스를 지원하는 서비스들을 위한 운영환경 및 모델링 환경
- 적용과 전문적 기능을 위한 운영환경

기능 층위 내에서는 규정/의사결정논리가 생성된다. 이들의 실행은 하위 층위들(정보 내지는 통합 층위)에서의 적용사례의 영향도 받는다.

원격조정과 수평적 통합은 오직 기능 층위에서만 일어난다. 그렇게 함으로써 프로세스 내의 정보들과 상태들의 완전성 및 기술 층위의 통합이 확보된다. 유지보수(maintenance)를 목적으로 할 때에는 자산 층위에 임시 액세스와 층위들의 통합도 허용된다.

그와 같은 액세스의 경우 특히 하위 층위에만 관련된 정보와 프로세스에 액세스하기 위해 이용된다. 이에 대한 예로는 센서/작동기 병들이나 아니면 진단데이터의 판독을 들 수 있다. 유지보수를 위한 일시적인 원격 액세스는 영속적인 기능통합이나 수평 통합에는 중요하지 않다.

6.2.3.3 정보 층위(Information Layer)

- 사건의 (前) 처리를 위한 운영환경
- 사건 관련 규정의 이행
- 규정들에 대한 형식적 기술
- 맥락: 사건 전처리preprocessing

여기서 하나의 또는 여러 사건으로부터 규정들을 통해 하나 또는 여러 개의 사건들이 다시 생성되는데, 그 경우 다시 생성된 사건들은 기능 층위에서 처리된다.

- 모델을 대표(표현)하는 데이터의 유지
- 데이터 완전성 확보
- 여러 데이터들의 지속적 통합
- 새로운, 가치가 높은 데이터(데이터, 정보, 지식) 획득
- 서비스 인터페이스를 통한 구조화된 데이터 준비
- 기능 층위에서 이용가능한 데이터들에 따른 사건의 수령과 변환

6.2.3.4 통신층위(Communication Layer)

- 정보 층위의 방향으로 통일된 하나의 데이터 포맷을 사용함으로써 통신의 통일화
- 통합 층위 제어를 위한 서비스 준비

6.2.3.5 통합 층위(Integration Layer)

- 컴퓨터 운영이 가능한, 자산 정보(물리/하드웨어/문서/소프트웨어 등) 준비
- 컴퓨터 기반의 기술 프로세스 제어
- 자산으로부터 사건들 생성
- RFID Reader, Sensoren, HMI 등과 같이 IT와 맞물린 요소들 포함

사람과의 상호작용도 마찬가지로, 예컨대 사람-기계 인터페이스를 이용하여 이 층위에서 이루어진다(HMI).

참조 : 현실에서 일어나는 중요한 사건은 각기 가상세계, 즉 통합 층위에 있는 사건을 암시한다. 현실이 달라지면 그 사건은 적절한 메커니즘으로 통합 층위로 보고된다. 중요한 사건들은 통신 층위를 거쳐 정보 층위의 사건들을 불러일으킬 수 있다.

6.2.3.6 자산 층위(Asset Layer)

- 선형축, 판금 부품, 문서, 배선도, 아이디어, 아키브 등이 현실을 보여준다.
- 사람도 마찬가지로 층위의 구성요소며 통합 층위를 통해 가상세계와 연결된다.
- 예컨대 QR-코드를 통해 자산을 통합 층위와 수동적으로 연결한다.

6.2.4 생애주기와 가치창출 흐름(Life Cycle & Value Stream)

생애주기(Life Cycle):

인더스트리 4.0은 제품, 기계, 공장 등의 전체 생애주기를 통해 커다란 개선의 잠재력을 제공한다. 여러 관계들과 연결들을 시각화하고 표준화하기 위해서 참조아키텍처 모델의 제2의 축은 생애주기와 거기 맞물린 가치창출 흐름을 나타낸다.

생애주기 고찰을 위해서 IEC 62890의 초안이 훌륭한 방향을 제시한다. 여기서 유형과 사례(Type & Instance)의 원칙적 구분이 고찰을 위한 핵심 부분이 된다.

유형(Type):

유형이란 언제나 맨 처음의 아이디어로서, 즉 "개발(Development)" 단계에서 제품의 생성과 함께 생겨난다. 이것은 주문, 개발, 테스트에서 제1차 견본과 프로토타이프 제작까지를 말한다. 이 단계에서 제품, 기계 등의 유형이 생겨난다. 모든 테스트와 비준이 끝나고 나면 이 유형은 대량생산으로 넘겨진다.

사례(Instance):

일반적인 유형을 바탕으로 생산 공정에서 제품이 생산된다. 이에 따라 제작된 제품 하나하나는 이 유형의 사례가 되고, 일정한 일련번호를 받는다. 이 사례들은 판매로 넘어가 고객에게 인도된다. 고객에게 이 제품들은 우선은 단지 유형일 뿐이다. 그러다가 구체적인 시설에 설치되면 이제 비로소 사례가 된다. 유형에서 사례로 바뀌는 것은 여러 번에 걸쳐 되풀이될 수 있다.

판매단계에서 되돌아와 개량이 이루어지면 어떤 제품 생산자에게서는 유형 기반의 변화로 이어진다. 새로 생겨난 유형으로 다시 새로운 사례들이 생산될 수 있는 것이다. 그럼으로써 유형은 개별 사례들 하나하나와 마찬가지로 이용과 관리에 맡겨진다.

보기:

새로운 유압밸브(hydraulic valve)의 개발은 새로운 유형을 나타낸다. 밸브가 개발되고, 첫 샘플이 만들어지고 테스트된 다음 끝으로 첫 프로토타입-시리즈가 생산 단계로 넘어가고 이어서 타당성 검사를 통해 확인 절차가 이루어진다. 성공적으로 검사가 끝나고 나면 이 유압밸브는 판매 단계로 넘어간다(자재번호 material number 및/또는 제품설명(이름)이 판매 카탈로그에 오른다.). 이로써 양산 단계도 시작된다.

이제 양산과정에서 제조된 유압밸브 하나하나는 이를테면 고유의 식별번호(일련번호)를 부여 받고 일단 개발된 유압밸브에 대한 사례가 된다.

판매되어 현장에서 쓰이는 유압밸드(사례)에 기술적 구조나 설계상의 작은 수정이나 밸브 펌웨어에 있는 소프트웨어 수정이 이루어는 피드백이 이루어질 수 있다. 이런 변화는 유형 차원에서 이루어지는 변화다. 다시 말해 유형 베이스로 돌아가 다시 인도됨으로써 생산과정에서 변화된 유형의 새로운 사례들이 생겨난다.

가치창출 흐름:

가치창출 흐름의 디지털화와의 결합으로 인더스트리 4.0에 의한 고도의 개선 잠재력이 제공된다. 여기서 결정적인 의미를 갖는 것이 여러 기능을 아우르는 전체의 연결이다.

물류 데이터들은 설치할 때 쓰일 수 있고, 공장내 물류는 수주량에 따라 자체로 조직화된다. 구매는 실시간으로 재고를 확인하고 특정 시점에 판매처가 어디에 있는지 확인한다. 고객은 주문한 제품이 어느 정도까지 제작되었는지를 알 수 있다. 구매, 주문계약, 설치, 물류, 유지보수, 고객, 공급자 등을 연결함으로써 개선의 잠재력이 커진다. 그렇기 때문에 생애주기는 거기에 내포된 가치창출 프로세스와 함께 살펴야만 한다. 공장을 하나하나 따로 보지 않고, 모든 공장들과 엔지니어링부터 공급자를 거쳐 고객에 이르는 모든 파트너들을 연결하여 보아야 한다.

가치창출흐름과 관련하여서는 VDI/VDE GMA FA7.21 "가치창출 흐름"[1]도 참고가 된다.

6.2.5 계층 단계(Hierarchy Levels)

참조아키텍처 모델의 셋째 축은 인더스트리 4.0 내 어느 상황의 기능적 위치를 설명한다. 여기서 중요한 것은 이행이 아니라 오로지 기능 할당일 뿐이다.

어느 공장 내의 배열을 위해 참조아키텍처 모델은 이 축에 대해 IEC 62264와 IEC 61512(그림 참조) 표준에 따른다. 가능한 많은 프로세스 산업 분야들과 공장 자동화까지 아우르며 통일된 시각으로 보기 위해서는 거기에 기입된 옵션들로부터 "Enterprise", "Work Center", "Station"과 "Control Device" 등의 개념들이 쓰인다.

인더스트리 4.0에 결정적인 것은 제어장치(Control Device) 외에도 기계나 시설 내의 고찰도 있다. 그렇기 때문에 제어장치 아래에 "필드 장치"(field device)가 추가되었다. 이것은 지능형 센서와 같은 필드 장치의 기능층위를 나타낸다.

그 밖에 인더스트리 4.0 내 제품 생산을 위한 시설 외에 생산될 제품 자체도 중요하게 보아야 한다. 이에 따라 하위 층위로 "제품" 층위가 추가되었다. 그렇게 함으로써 참조아키텍처 모델 내에서 서로 종속되어 있는 생산될 제품과 생산시설을 균질하게 볼 수 있다.

계층 단계 최상부에도 마찬가지로 추가되는 항목이 있다. 앞서 언급한 IEC의 표준 둘 다 공장 내의 층위들만을 나타낸다. 그러나 인더스트리 4.0은 한 단계 더 나아가서 공장연합, 외부 엔지니어링 사무실, 공급자, 고객 등과의 협업까지 설명한다. 그렇기 때문에 기업 층위를 넘어서 추가적으로 "Connected World"에 대한 고찰도 삽입되었다.

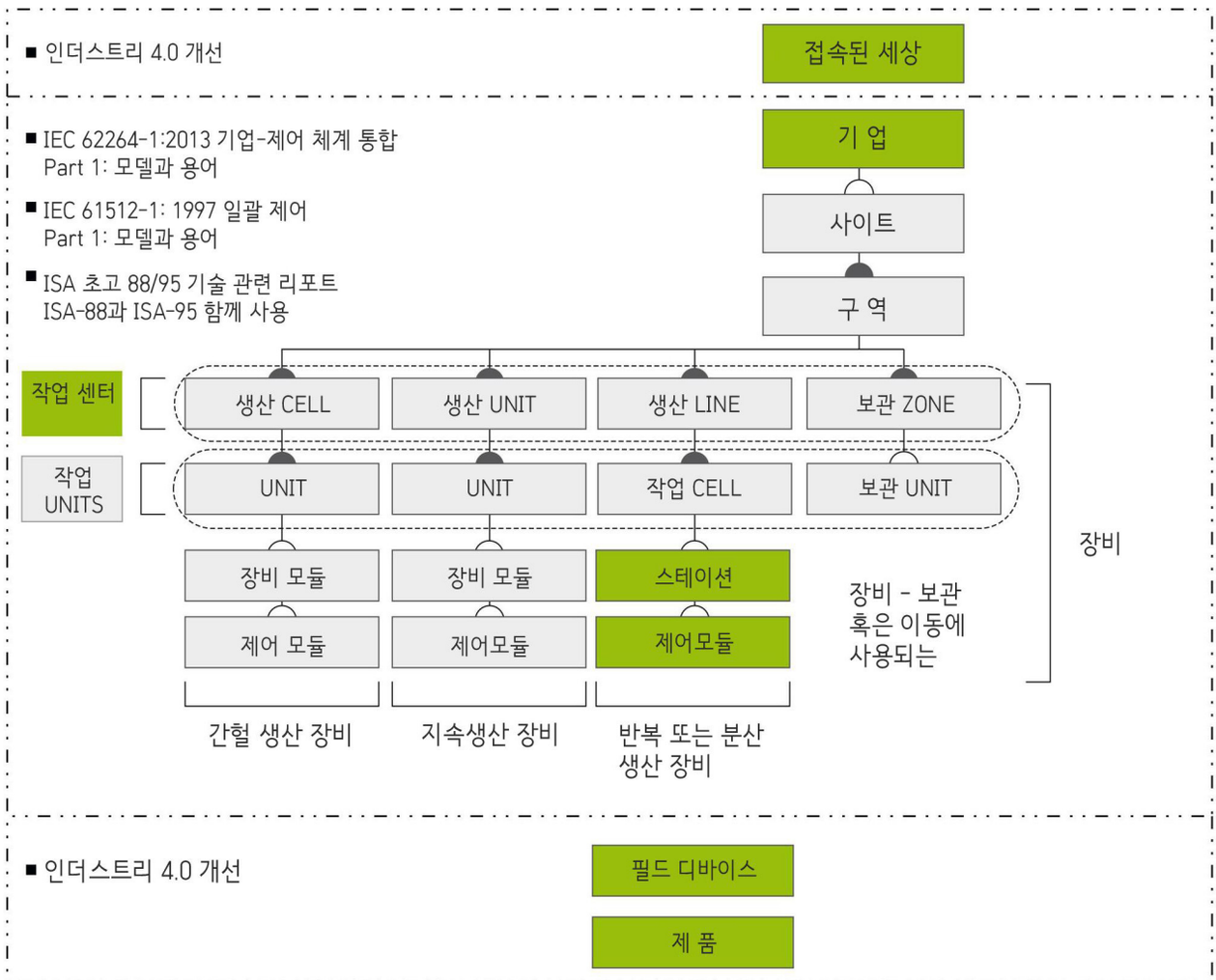


그림 16: 참조아키텍처 모델 RAMI 4.0 위계 층위들의 유도[4]

6.3 인더스트리 4.0-요소들을 위한 참조모델

아래에서 설명될 인더스트리 4.0-요소들이라는 참조모델 버전 1.0은 추후 시간 간격을 두고 발표될 여러 차례에 걸쳐 다듬어진 버전들 중 첫째 버전이다. 따라서 그 다음 단계에서는 좀 더 자세한 정의(定義)를 다룬 장이 이어지고 UML(Unified Modeling Language)을 이용한 공식화가 예정되어 있다.

이 장에서는 인더스트리 4.0과 관련하여 다른 출처로부터 나온 문장이나 인용을 명확하게 밝히고자 한다(예컨대 VDI/VDE GMA 7.21). 최종적으로는 사용된 개념들이 GMA 7.21과 통일시키도록 한다. 또한 사례에 대하여는 그것이 사례임을 명기하고, 그 사례 중에 명기되지 않은 사항이 배제되지 않도록 한다.

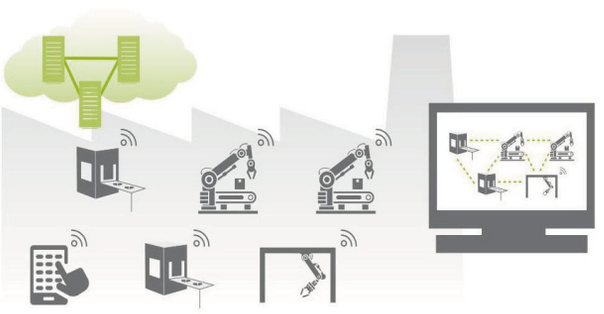
6.3.1 인더스트리 4.0에 관한 논의 정립하기

인더스트리 4.0은 대략 참고문헌 [3]으로부터 전재한 아래 그림의 네 개의 측면들의 상호작용으로 설명될 수 있다.

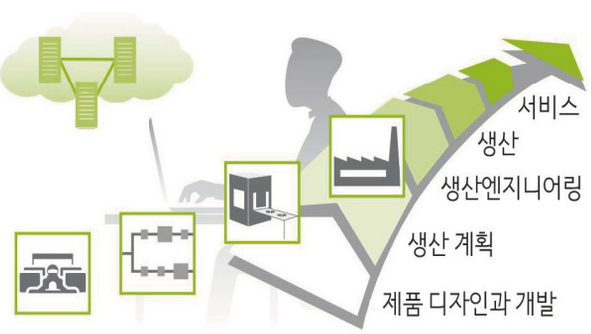
4) 출처: IEC 61512, IEC 62264, ISA Draft 88/95 Technical Report, Plattform Industrie 4.0

가치창출 네트워크를 횡단하는 수평적 통합

수직적 통합과 네트워크화된 생산시스템



가치창출 흐름 전체에 걸친 엔지니어링의 디지털 일관성



가치창출의 지휘자로서의 사람

그림 17. 인더스트리 4.0의 네 가지 주요 측면[5]

아래 그림들에 따르면 네 개의 측면들은 다음과 같다.

- 인더스트리 4.0–측면(1)
  가치창출 네트워크를 횡단하는 수평적 통합
- 인더스트리 4.0–측면(2)
  공장/제작 내부 같은 곳에서의 수직적 통합
- 인더스트리 4.0–측면(3)
  생애주기 관리, 엔지니어링의 시종일관성
- 인더스트리 4.0–측면(4)
  가치창출 네트워크에서의 지휘자로서의 사람[6]

이 텍스트에서 설명된 인더스트리 4.0–구성요소들이 어떤 데이터와 기능으로 기술(記述)되고 준비될 수 있는지, 위에 거론한 인더스트리 4.0–측면들을 지원하고 가능하게 하는 것들은 어떤 것들인지 그 영역범위는 유연하다. 이 텍스트에서 설명된 개념들은 현재 시점에서 무엇보다 측면(2)에 도움이 되며 측면(3)에서 제기된 요구조건들을 고려한다.

6.3.2 다른 작업팀에서 나온 관련 데이터들

VDI/VDE GMA 7.21: 대상들, 독립체들(entity), 요소들

VDI/VDE GMA 7.21에서 나온 개념정의들에 대해서는 앞서 제시했던 장들을 참조하라.

유형과 사례들

인더스트리 4.0에 있어서 유형과 사례의 구분과 관련한 기술(技術)의 현 수준에 대해 간략하게 살펴본다.

5) 참고문헌 [3]을 참고하여 작성. 우측 하단 사진의 출처: Festo
6) 바우어른한슬(Bauernhansl) 교수에 따른 것.

생애주기

프라우엔호프 IPA, 콘스탄티네소우 교수, 바우어른한슬 교수에 따르면 어느 공장의 운영을 위한 다음 여러 차원의 생애주기가 인더스트리 4.0에 중요하다.

- **생산** : 하나의 공장에서는 여러 개의 제품들이 생산된다. 제품 하나하나에는 저마다 생애주기가 있다.
- **주문** : 제작에 대한 주문마다 각각의 생애주기가 있으며, 그 특수성들을 공장운영 내의 주문이행 과정 동안 반영할 수 있어야 한다.
- **공장** : 공장이란 것에도 생애주기가 있다. 재정을 투입하여 계획을 세우고 지은 다음에는 재활용된다.
  공장은 여러 제조사들의 생산시스템과 기계를 통합한다.
- **기계** : 기계는 발주되고, 제조되어 운영에 들어가 가동, 유지보수, 개조되고 재활용된다.

기계 제작사는 기계제작을 위하여 개별 부품들을 구매하는데, 이하의 서술에서 이 부품들을 대상으로 호칭한다. 납품업자(통상 부품제조사) 역시 이 공급부품들에 대해서도 생애주기를 실현시킨다.

- **구성요소** : 계획, 개발, 신속 프로토타이프 제작(Rapid Prototyping), 생산시설 구축(construction), 생산, 이용과 서비스까지를 말한다.

그림 18에서 이 모든 것이 분명하게 제시된다.

생애주기들의 연결

유형들과 사례들을 구별해야할 이유는 여러 거래선이 있는데 그들 각자의 계획 프로세스와 생애주기가 상호작용하기 때문이다. 하나의 계획을 세우는 동안 여러 가설과 대안들을 따져보게 된다. 계획은 잠재적인 대상들로부터 출발하는데, 이를 가리켜 "유형"(Type)이라 한다.

그림 18: 인더스트리 4.0 구성요소와 관련한 생애주기들 7)

7) 출처 : 마틴 한젤, 토마스 바우에른한슨

- **납품업자**는 이를 "부품유형"이라 부른다. 제작 완료되고 이어서 고객(기계 제조사)에 인도됨으로써 비로소 사례가 "생성"된다. 이 사례를 제조사가 공급부품으로 사용하게 된다.
- **기계 제조사**는 고객들과 협의하여 "기계유형"을 계획한다. 어떤 특별한 기계를 제작하고 실현시키는 일에서 사례가 창출되고, 이 사례를 공장 운영자가 계속해 사용해 간다.
- **공장 운영자**는 제품의 개발에 있어 처음에는 프로토타입을 개발한다. 계약이 성립하고 제작과정에 들어서야 비로소 구체적인 제품-사례가 제조되어 인도된다.

여기서 주목할 것은, 어느 유형을 설계하고 계획하는 동안 많은 정보들과 데이터들이 생성되며, 이들 정보와 데이터가 가치창출 네트워크 하부에 있는 상대방 거래선에 의해 이용될 수 있다는 점이다. 특정한 사례의 생산 과정에서도 새로운 정보들이 추가된다(예컨대 tracking data와 품질 데이터 등). 따라서 인더스트리 4.0-구성요소를 위한 참조모델에서는 유형과 사례들을 등가로 똑같이 다룬다.

인더스트리 4.0 참조아키텍처 모델(RAMI 4.0)

"인더스트리 4.0 참조아키텍처 모델(RAMI 4.0)"의 개념정의에 대해서는 앞의 장들을 참조하라. 여기에 소개되는 "인더스트리 4.0-구성요소들"은 RAMI 4.0의 층위들에 배열된다. 생애주기와 가치창출 흐름(Value-Strams)은 물론 여러 위계 층위들에서도 위치가 다를 수 있다. 여기서 분명하게 위치를 결정하기 위해서는 구체적인 유형의 의미에서 대상의 특성들이 드러나게 하는 것이 필요하다.

6.3.3 "인더스트리 4.0-구성요소"

6.3.3.1 이 장에서는 인더스트리 4.0-구성요소에 대해 처음으로 일반적으로 승인된 개념정의를 도출한다. "Office floor"와 "Shop floor" 사이의 인더스트리 4.0-구성요소 구분

책임소재의 경계 설정을 위해 기업에서는 통상 "Office Floor"와 "Shop Floor"를 구분한다. 그러나 현대 기업에서는 이 두 영역이 갈수록 서로 맞물리는 분야가 많다. 자동화 기술을 중심으로 생각한다면 "Office Floor"의 중요성이 감소하는 반면, 고려할 필요가 있는 "Shop Floor"에 대한 요구가 점점 더 늘고 있다. 다른 방향에

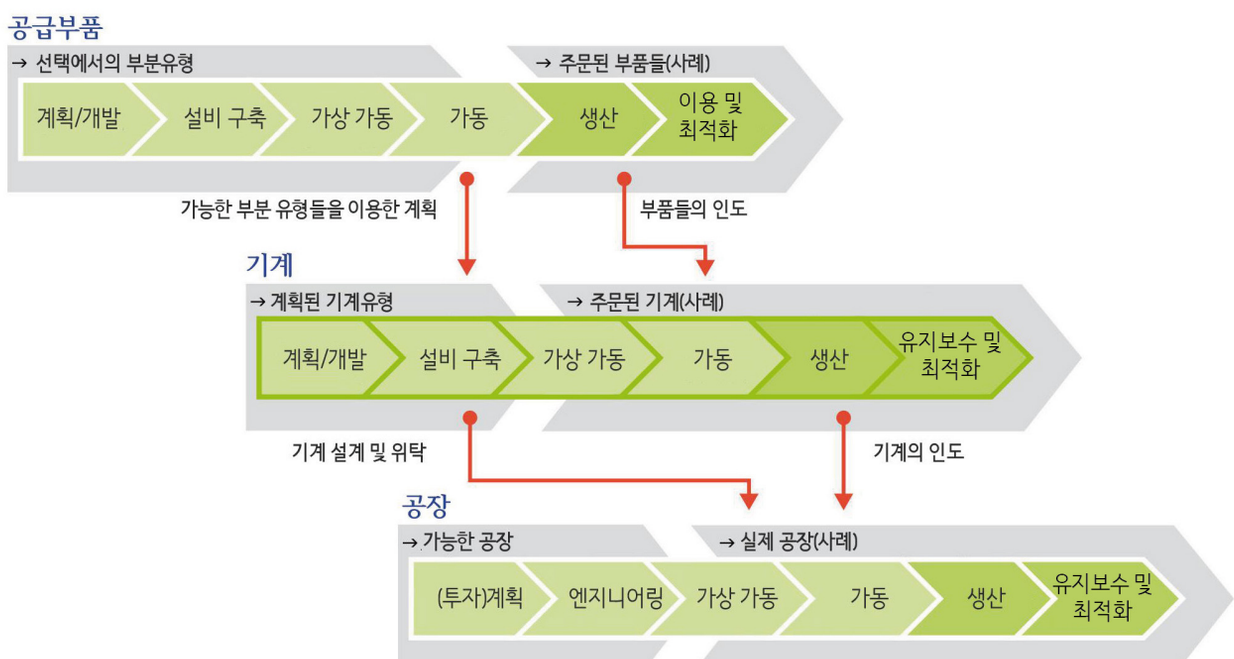


그림 19: 생애주기에서의 유형과 사례

서도 마찬가지다. 다음 그림에서 보는 바와 같이, 임의의 터미널과의 연결성 및 공통의 의미론 모델이라는 요구 때문에 구성요소들은 층위와 무관하게 일정한 공통의 특징을 갖고 있지 않으면 안 된다. 이 내용에 대해 인더스트리 4.0-구성요소의 형식으로 상술하기로 한다.

그림 20: "Office Floor"와 "Shop Floor"의 구분

인더스트리 4.0-구성요소는 하나의 생산시스템, 개별 기계, 중간단계(station) 또는 어느 기계 안의 한 모듈로 나타낼 수 있다. 이로써 인더스트리 4.0-구성요소는 저마다 아무리 다르다 할지라도 "Office Floor"와 "Shop Floor"의 양극 사이에서 공장의 생애주기에 따라 그리고 PLM(Product Lifecycle Management)이나 ERP (Enterprise Ressource Planning) 또는 공장용 제어시스템(Industrial Control and Logistic Systems)처럼 핵심적이고 중요한 공장시스템들과 연결되어 움직인다.

요구사항:

인더스트리 4.0-구성요소 네트워크는 임의의 터미널들(인더스트리 4.0-구성요소) 사이의 연결이 가능해지도록 구축되어야 한다. 인더스트리 4.0-구성요소와 그 내용은 하나의 공통 의미론 모델을 따라야 한다.

요구사항:

인더스트리 4.0-구성요소의 개념은 "Office Floor" 또는 "Shop Floor"처럼 서로 다른 핵심 요구사항들에 부응할 수 있도록 개별화되어야만 한다.

6.3.3.2 대상에서 인더스트리 4.0-구성요소로

이하에서는 인더스트리 4.0-구성요소에 대한 정의를 도출하기 위해 GMA에서 확정한 표준들 하나하나를 서로 연결시켜 보기로 한다.

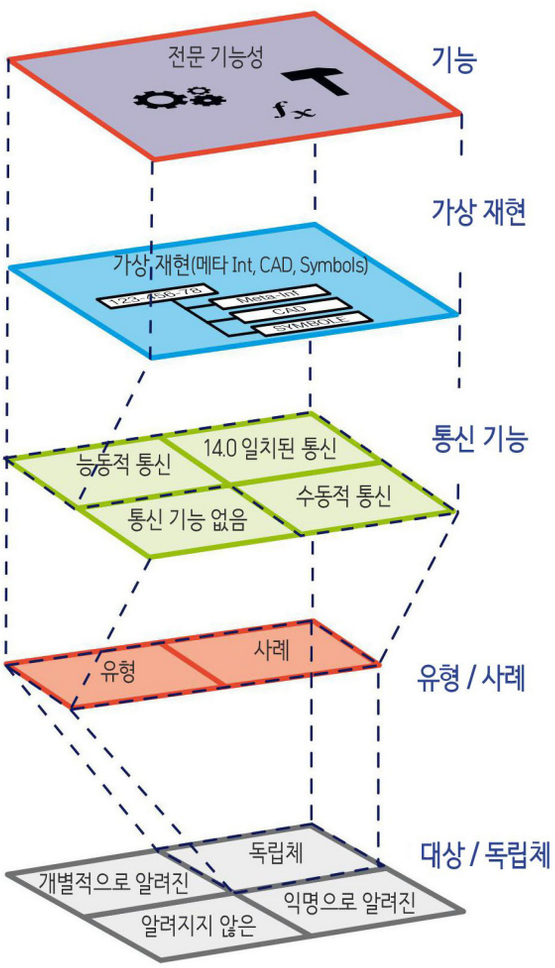


그림 21: GMA 7.21에 따른 인더스트리 4.0 – 구성요소 계층구조

대상의 분류

GMA는 대상의 분류로 다음 네 가지를 지정 :

- 알려지지 않은
- 익명으로 알려진
- 개별적으로 알려진
- 독립체

데이터와 기능들을 하나의 대상에 맞물리게 할 수 있으려면 우선 독립체로서의 대상이 있어야 한다. 종래의 의미에서 물리적이거나 비물리적으로 출하되는 소프트웨어도 마찬가지로 하나의 대상이다. 아이디어, 아키브, 개념 등도 이런 의미에서 대상들이다.

참조 1:

인더스트리 4.0-구성요소의 목적이 데이터와 기능들을 하나의 정보체계에 제공하는 것이기 때문에 개별적으로 알려진 대상들에 대해 GMA의 의미에서 그 자체로 독립체로의 전이가 이루어진다.

참조 2:

아래에서 대상/독립체로 표시하는 경우 언제나 대상에 대해 언급하는 것이다.

유형/사례(Type/Instance)

대상들은 유형으로 또는 사례로 알려질 수 있다. 예컨대 계획단계에서 대상은 유형으로 알려진다. 계획된 어느 대상의 주문정보들이 알려졌다면, 이 대상은 개별적으로 알려진 유형으로 파악될 수 있다. 예컨대 현실에 실제로 존재하는 기계의 대상들은 모두 사례로 파악할 수 있다. 셀 수 있다는 의미에서 어느 유형이 여러 차례에 걸쳐 실체화(instantiation)됨으로써 생겨나는(Chargen) 외형상의 사례들은 현재 특별히 따로 고려하지 않는다. 여기서 실체화가 구체적으로 수행되어야 하고 유형으로 돌이켜 참조(reference)할 수 있게 해야 한다.

통신 가능성

인더스트리 4.0-구성요소의 특징들을 제공할 수 있으려면 적어도 정보체계가 대상과의 연결을 유지해야 한다. 따라서 최소한 대상에 대한 수동적 통신가능성이 전제되어야 한다. 다시 말하면 대상이 반드시 GMA FA 7.21에 상응하는 인더스트리 4.0에 상응하는 통신 가능성을 보여야 할 필요는 없다. 그럼으로써 기존의 대상들도 인더스트리 4.0-구성요소로 "확장"될 수 있는 것이다. 이 경우 상위의 IT-시스템이 SOA아키텍처와 대행원칙(deputisation principle)의 의미에서 인더스트리 4.0에 상응하는 통신 기능의 일부를 넘겨받는다.

이를테면 식별 가능한 연결단자나 (I&M-데이터를 통해 식별 가능한) ProfiNet-기기도 인더스트리 4.0 구성요소가 될 수 있다.

가상의 이미지

가상의 이미지에는 대상에 관한 데이터가 보관되어 있다. 이 데이터들은 인더스트리 4.0-구성요소 자체 "위/안"에 머물거나 아니면 인더스트리 4.0과 일치되는 외부세계의 통신을 통해 사용될 수 있다. 아니면 (상위의) IT-체계에 보관되고, 이 체계가 인더스트리 4.0과 상응하는 외부세계의 통신을 통해 사용할 수 있도록 하기도 한다.

참조 아키텍처 모델 RAMI 4.0 안에는 가상의 재현이 정보 층위에서 얼어난다. 그렇게 함으로써 인더스트리 4.0과 상응하는 통신의 중요성이 높아진다.

요구사항:

인더스트리 4.0에 대응하는 통신은 인더스트리 4.0-구성요소의 가상 이미지 데이터를 대상 자체 안이거나 아니면 (상위) IT-체계 안에 유지될 수 있도록 수행되어야 한다.

가상 재현에서 더 중요한 부분은 가상 재현의 개별 데이터 내용 목록으로 볼 수 있는 "Manifest"[8]이다. 그럼으로써 이른바 메타-정보를 갖게 된다. 그 밖에도 인더스트리 4.0-구성요소에 대하여 의무를 부여하는 지시들을 갖는데, 특히 상응하는 확인(identification) 가능성을 통해 대상과의 연결 지시가 중요하다.

가상 재현에서 가능한 또 다른 데이터들이라면 CAD-데이터, 접속도, 사용설명서 등과 같이 생애주기 개별 단계를 포괄하는 데이터들이다.

전문 기능성

인더스트리 4.0-구성요소에는 데이터들 외에 전문적 기능성도 있다. 이 기능성은 이를테면 다음과 같은 것들을 포괄한다.

- 대상과의 연결에서 "local planing"을 위한 소프트웨어. 예컨대, 용접계획, 연결단자 식별 표시를 위한 소프트웨어 등
- 프로젝트 계획수립을 위한 소프트웨어, 구성, 조작, 유지보수
- 대상에 대한 잉여가치
- 사업논리 실행에 중요한 그밖에 다른 전문 기능들

전문적 기능성은 참조 아키텍처 모델 RAMI 4.0 안의 기능 층위에서 실행된다.

6.3.3.3 대상을 인더스트리 4.0-구성요소로 만드는 "관리-셸(shell)"

위의 장에서 기술한 것처럼 여러 종류의 통신 가능성들을 지닌 여러 대상들이 인더스트리 4.0-구성요소로 이행될 수 있다. 이 장에서는 이 여러 가지 이행 형식들을 사례들을 통해 더 자세히 살피고자 한다. 인더스트리 4.0-구성요소라는 개념에 비추어 볼 때 이 이행 형식들이 지니는 가치는 동일하다.

그림 22에서 보듯이 종류가 어떻든 간에 어느 대상이 처음부터 인더스트리 4.0-구성요소가 되는 것은 아니다. 독립체와 적어도 수동적인 통신이 가능해야 하는 그 대상이 "관리-셸"로 둘러싸일 때 비로소 인더스트리 4.0-구성요소로 표시될 수 있다.

위의 장에서 설명된 의미에서 관리-셸은 대상의 가상 이미지와 전문적 기능성을 포괄한다.

8) "JAR-데이터" 때문에 선택. Manifest [11] 참조.

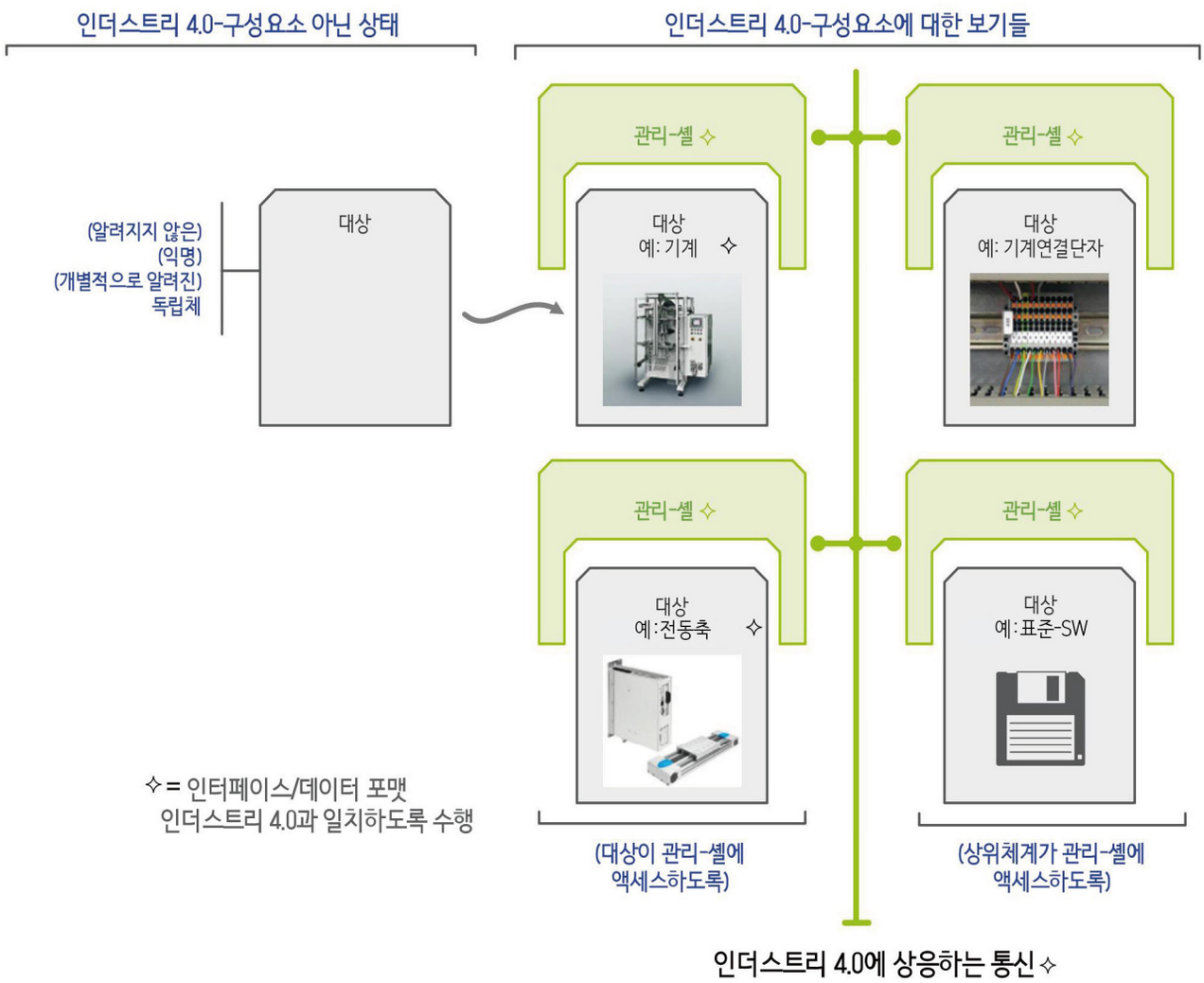


그림 22: 인더스트리 4.0 구성요소가 되는 대상

가능한 대상에 대하여 위의 그림은 네 가지 예를 제시하고 있다.

1. 기계 전체의 경우에는 무엇보다 제어장치를 갖고 있기 때문에 인더스트리 4.0-구성요소로 넘겨질 수 있다. 인더스트리 4.0구성요소의 이러한 이행은 그 다음에 이를테면 기계제조사가 넘겨받는다.
2. 어느 납품업자에게 전략적으로 중요한 모듈[9]도 역시 독자적인 인더스트리 4.0-구성요소로 파악함으로써 이를테면 자산-매니지먼트 시스템과 유지보수 시스템의 독자적 구성요소로 파악할 수 있다. 인더스트리 4.0-구성요소의 이행은 그 다음 이를테면 구성요소 제조사에서 넘겨받는다.
3. 개별적으로 구축된 기계의 모듈들을 인더스트리 4.0-구성요소로 파악하는 것도 마찬가지로 가능하다. 예컨대 연결단자의 경우도 개별 신호들을 받아서 기계들의 생애주기를 넘어서 실시간으로 유지하는 것이 중요하다. 이 인더스트리 4.0-구성요소의 이행은 그 다음에 이를테면 전기 설계자와 전기 기술자가 넘겨받는다.
4. 나아가 제공되는 소프트웨어가 생산시스템의 중요한 자산이 되어 인더스트리 4.0-구성요소로 될 가능성이 있다. 이와 같은 표준-소프트웨어는 이를테면 독자적인 계획의 도구 혹은 엔지니어링의 도구일

9) 구성요소라는 개념을 피하기 위해

수 있다. 이 도구는 오늘날 또는 미래에 제작 기업에 중요하다. 납품업자가 자기 제품의 확장된 기능을 제공하는 도서관을 순수한 소프트웨어로 판매하려는 것도 생각해볼 수 있다. 인더스트리 4.0-구성요소의 이런 이행은 그 다음에는 이를테면 소프트웨어 제공자가 넘겨받을 수 있다. 개별 IEC61131-제어들에 분할시키는 일은 그 다음에는 여러 가지 인더스트리 4.0-체계들이 수행할지도 모른다.

그림 22는 논리적 시각에서 "관리-셸"이 대상에 속한다는 사실을 보여준다. 분할의 시각에서 보면 대상과 관리-셸은 전적으로 연결되지 않은 상태로 존재할 수 있다. 그렇게 함으로써 수동적 통신이 가능한 대상들의 경우 상위 IT-체계에 있는 관리-셸이 관리[10]할 수 있다. 대상과 인더스트리 4.0에 상응하는 상위 IT-체계의 통신의 수동적 통신 가능성의 도움으로 대상과 관리-셸 사이의 연결이 보장된다. 대상이 능동적이지만 인더스트리 4.0에 상응하는 통신이 가능하지 않을 경우라도 마찬가지다. 인더스트리 4.0에 상응하는 통신능력이 있을 때에야 비로소 대상 "안"에 있는 관리-셸이 관리될 수 있다(이를테면 기계 제어에 저장되어 네트워크 인터페이스를 통해 내보낸다.). 인더스트리 4.0-구성요소의 개념이 갖는 의미에서 대안들은 모두 동가로 인정될 수 있다.

대상 하나가 여러 목적으로 여러 개의 관리-셸을 가질 수 있다.

요구사항:

상위 IT-체계가 관리-셸을 어떤 식으로 인더스트리 4.0에 상응하게 사용하게 할 수 있는지(SOA-원칙, 대행-원리) 적합한 참조모델을 통해 기술되어야만 한다.

10) hosted

요구사항:

관리-셸이 생산자(이를테면 요소-생산자, 전자-계획자)에 의해 어떻게 상위 IT-체계로 "이송"될 수 있는지(이를테면 Email에 첨부되어) 기술되어야 한다.

6.3.3.4 그 밖의 개념의 경계설정

아래 그림은 개념들을 한 번 더 서로 구분지어 경계를 설정한다.

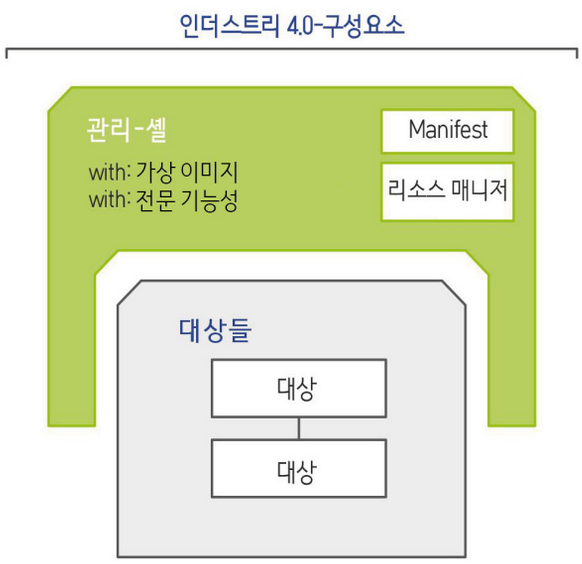


그림 23: 인더스트리 4.0-구성요소

인더스트리 4.0-구성요소란 논리적 시각에서 하나 또는 그 이상의 대상들과 하나의 관리-셸을 포괄한다. 관리-셸은 가상 이미지의 데이터와 전문 기능성의 기능들을 포함한다. Manifest는 가상 이미지파트로서 인더스트리 4.0-구성요소에 관리-기술 관련 필수 지시들을 상세히 기술한다. GMA FA 7.21에서 정의한 "리소스-매니저"도 마찬가지로 관리-셸 파트이다. 그럼으로써 IT-기술 서비스는 관리-셸의 데이터와 기능들에 액세스할 수 있고, 이들을 외부 세계에 쓸 수 있도록 제공한다.

관리-셸과 그 대상들은 대상의 "내장 체계(embedded system)" 안에 호스팅(hosted)될 수 있다(능동적 인더스트리 4.0에 상응하는 통신 가능). 또는 하나 또는 그 이상의 상위 IT-체계에 배치될 가능성도 있다(배치 view).

요구사항:

상위 체계들의 종류에 따라 관리대상들은 하나 이상의 상위 IT-체계 안에 분산될 수 있어야 한다.

사이버-물리 체계

인더스트리 4.0-구성요소들은 사이버-물리-체계의 특수화를 나타낸다.

6.3.3.5 분할-시각에서 본 인더스트리 4.0-구성요소들

위의 장에서는 논리적 시각에서 개개의 인더스트리 4.0-구성요소들에 대하여 대상 하나하나에 각 하나의 "관리-셸"이 속한다는 것을 설명하였다. 아울러 상황에 따라 분할-시각에서 관리-셸이 상위 체계에 저장될 수 있다는 사실도 강조하였다.

저장소에 디스플레이된 인더스트리 4.0-구성요소

더 나은 이해를 위해 "디지털-공장"의 저장소에 상응하는 (즉 설명된 개념들과 일치하는) 그림으로 나타낼 수 있다.

대상을 통해 보여주는(display) 인더스트리 4.0-구성요소

인더스트리 4.0-구성요소들의 대상들 중 하나가 인더스트리 4.0에 상응하는 통신이 가능하다면([2]에 따른 CP34 또는 CP 44), 인더스트리 4.0-구성요소를 그 대상을 통해 보여 줄 수 있다.

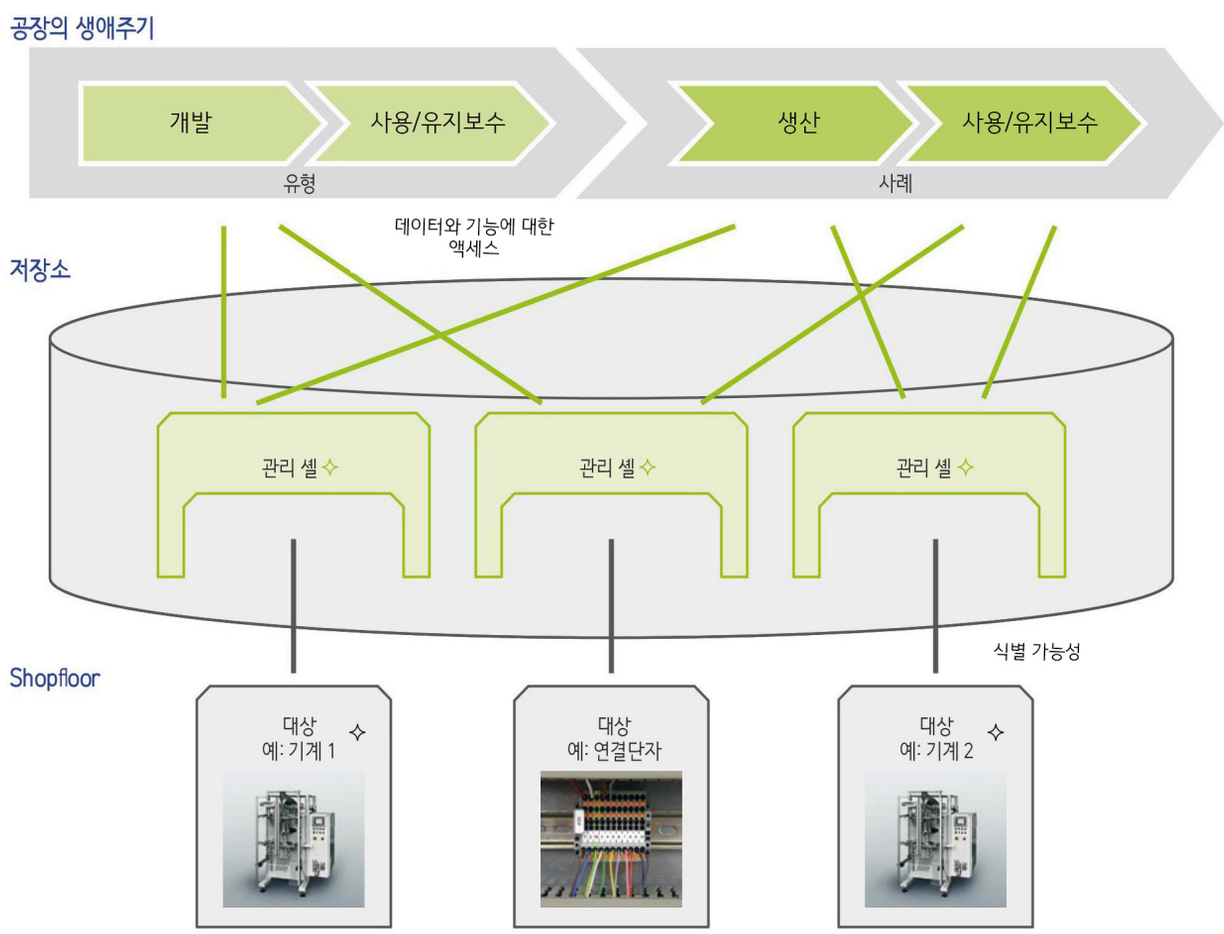


그림 24: 저장소

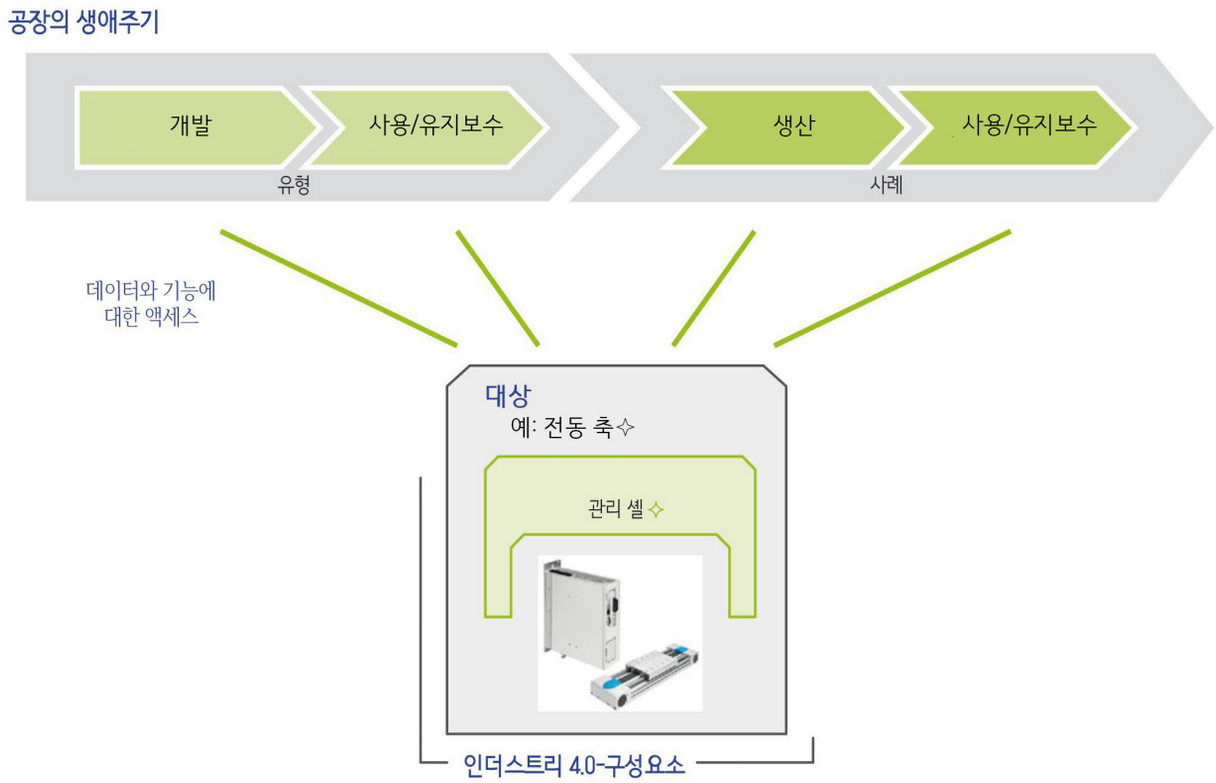


그림 25: 공장의 생애주기

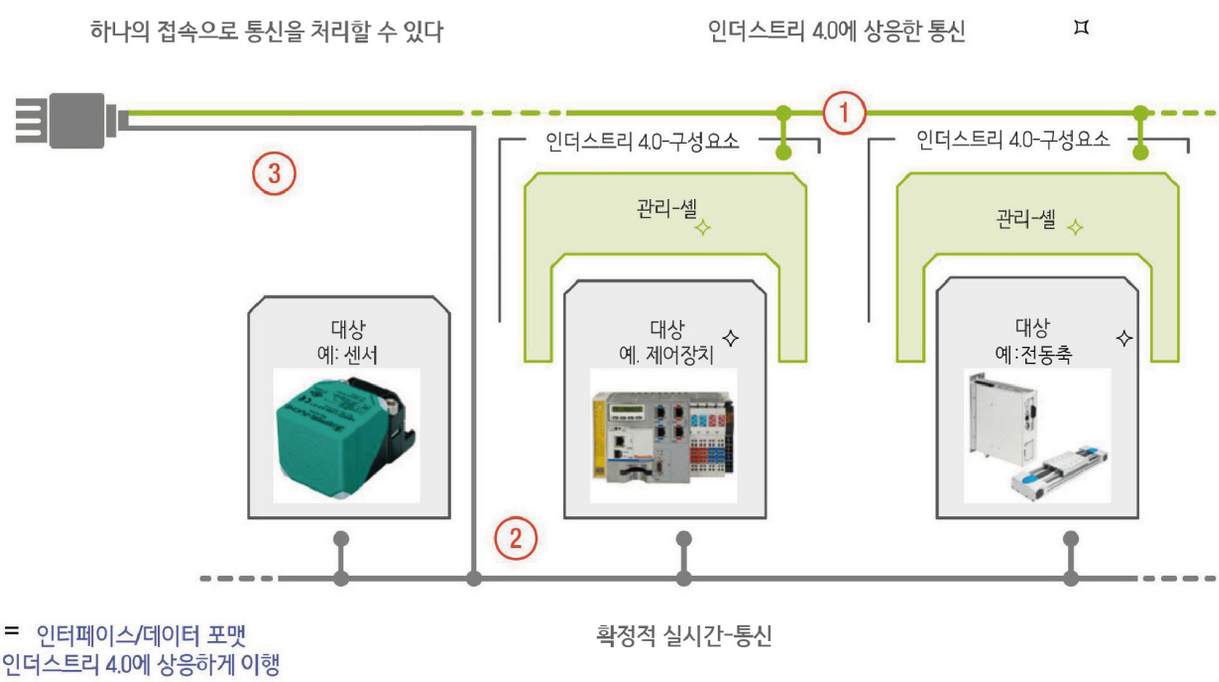


그림 26: 인더스트리 4.0—구성요소의 캡슐화(통신에 잠시 장애가 있어도 핵심 기능을 유지하는 능력) 가능성 및 네트워크화

캡슐화가 가능한 인더스트리 4.0-구성요소

인더스트리 4.0-구성요소는 인더스트리 4.0-공장 내부의 가능한 모든 상호접촉에 대응하는 것이 명확하게 의도되어 있거나 그렇게 구축될 수 있어야 한다(그림 26). 그러나 이 네트워크화가 핵심 기능의 제한을 초래해서는 안 된다(그림 26). "외부" 네트워크에 장애가 생기더라도 이 핵심 영역을 장애 없이 유지할 수 있는 역량을 SG2(ZVEI 그림자 위원회 참조 아키텍처)와 SG4(ZVEI 그림자 위원회 보안)에서 "캡슐화 능력)"이라 명명하였다.

요구사항:

인더스트리 4.0-구성요소는 특히 관리셸과 거기에 포함되어 있는 기능 및 그것을 위한 프로토콜 등에 대하여 "캡슐화 능력"을 갖고 있지 않으면 안된다.

현재의 개념은 관리-셸이 독립적인 데이터대상/기능대상으로 실행되는 것을 통해 이 요구사항을 실현한다. 거기에 있는 데이터와 기능들에 대한 액세스는 "관심의 분리"(SoC = Separation of Concerns)[11] 원칙에 따라 설정되어야 한다. 그렇게 함으로써 기술 상태에 따라 제작에 문제가 되는 과정의 영향을 차단할 수 있다.

이 원칙을 적용함으로써 인더스트리 4.0에 상응한 통신이 오늘날의 수준에 따라 제작 과정에 사용된 인터넷-베이스의 필드버스(field bus)를 완전히 대체할 필요가 없다(이주 시나리오).

그러나 인더스트리 4.0에 상응하는 통신과 가능한 결정론적 또는 실시간-통신이 상호 조율되어 이를테면 가능한 한 동일한 (물리적) 인터페이스와 인프라 구조를 사용해야 한다. 이 두 가지 통신-채널 사이에 장애가 없도록 보장되어야만 한다.

이 추론은 이 텍스트에서 설명된 참조모델의 경우 인더스트리 4.0에 상응하는 통신이 결정론적 또는 실시간-통신 전체의 속성 전체를 실현할 필요가 없이 기존 기술에 맡길 수 있다는 것을 의미한다.

11) http://en.wikipedia.org/wiki/Separation_of_concerns

요구사항:

인더스트리 4.0-구성요소가 갖춰야 할 요구사항은 대상의 셸로 이어지거나 그 셸을 떠나는, 인더스트리 4.0에 상응하지 않은 통신관계들을 파악하여 편재하는 엔지니어링에 개방하는 것이다.

오늘날 일상화된 실시간-인터넷-프로토콜로 동일한 통신-인프라구조(접속, 플러그, 중계소) 두 가지 모두 실현하는 것이 가능해 보인다(그림 26). 그러나 "관심의 분리" 원칙에 따르면 두 가지 통신 양식은 논리적으로 계속해서 분리된다.

인더스트리 4.0-구성요소는 여러 대상들을 내포할 수 있다.

이 장에서는 하나의 사례를 통해 인더스트리 4.0 구성요소가 하나의 대상뿐만 아니라 여러 대상들도 담을 수 있다는 것을 보여준다.

인더스트리 4.0에 대응하는 통신*

그림 27: 여러 개의 대상으로 구성된 인더스트리 4.0 구성요소

그림 27에서 제시된 대상들은 합쳐서 전동축 시스템의 본보기를 만든다. 어느 제조사에서 나온 해석-소프트웨어가 있는데, 엔지니어링-단계에서 개별 부분체계들이 하나의 체계로 조합되도록 한다. 그 밖에 환경설정-소프트웨어가 있는데, 이를 이용해 체계가 전체로서 운영될 수 있다. 블록 위치 설정, 소모된 데이터, 표시 및 컨디션 모니터링이 개별 시스템 구성요소들을 연결시킨다(이를테면 최적의 처리거리 관련).

이에 따라 인더스트리 4.0 시각에서 이 개별 대상들을 하나의 체계로 관리하고 하나의 인더스트리 4.0-구성요소로 디스플레이하는 것이 의미 있다. 개별 인더스트리 4.0-구성요소로 나누면 하나 또는 그 이상의 상위 인더스트리 4.0체계를 통한 여러 가지 의미 맥락의 디스플레이가 요구되기 때문에 불필요하게 복잡해진다.

6.3.3.8 인더스트리 4.0-구성요소는 논리적으로 세팅 가능

인더스트리 4.0은 인더스트리 4.0 측면(2) "수직적 통합" 영역 내에서 계약에 맞는 환경의 재설정과 (기업)자산 생산체계의 모듈화[12]를 요구한다. 그래서 이 개념은 인더스트리 4.0-구성요소 하나가 다른 요소들을 논리적으로 포괄하고, 통일체로 행동하고 상위체계를 위해 논리적으로 추상화될 수 있도록 미리 계획한다.

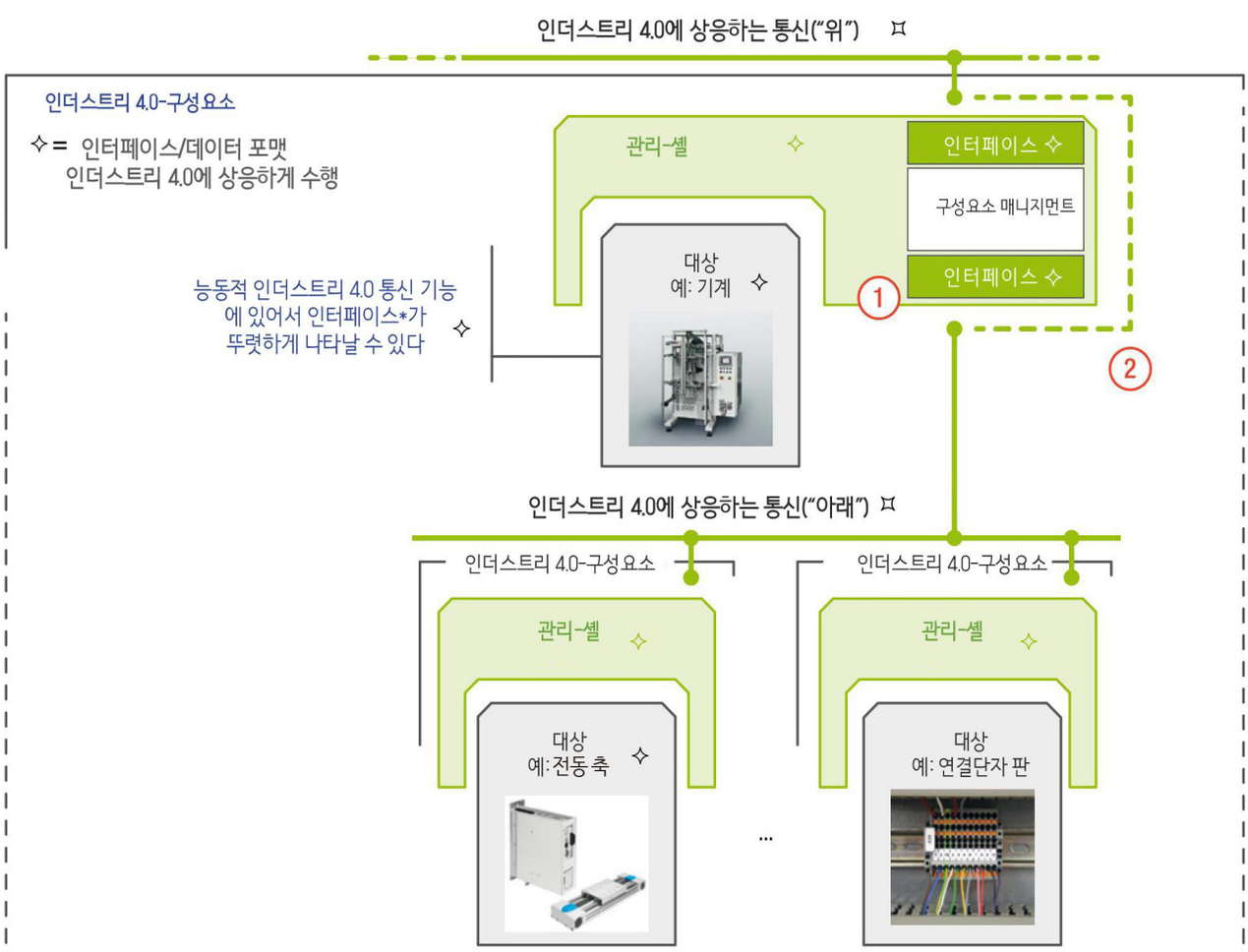


그림 28: 인더스트리 4.0 구성요소의 세팅 가능성

12) [3] 참조: "나아가 모듈화 개념과 재사용 개념은 이를 위한 생산체계와 적절한 통합 시설-기능설명들과 조합하여 네트워크화와 환경재설정을 위한 전제조건으로 개발될 수 있다."

나아가 인더스트리 4.0–측면(3) “엔지니어링에서의 편재성”은 어느 생산체계의 가급적 많은 대상에게 전달되는 데이터와 엔지니어링–계획이 온라인으로 이용 가능할 것을 요구한다. 이 관리–셸은 인더스트리 4.0–구성요소의 대상들에게 분명하게 배열될 수 있는 데이터들이 그런 식으로 분산되어 사용 가능하게끔 고안되었다. 그렇게 분할된 데이터들은 분할된 엔지니어링과 신속한 환경재설정에 득이 된다.

따라서 인더스트리 4.0–구성요소를 위한 이 개념은 인더스트리 4.0–구성요소(이를테면 한 기계 전체)에 다른 인더스트리 4.0–구성요소들이 논리적으로 배열되어 (임시로) 세팅이 되도록 고안하였다.

기술적으로 보면 이 과정은 상위 대상(예컨대 기계 등)이 인더스트리 4.0–구성요소 두 개에 작용하여 상위 인더스트리 4.0–구성요소와 하위 인더스트리 4.0–구성요소 사이의 논리적이고 물리적으로 명확한 구분이 되도록 할 수 있다(그림 28). 또 하나의 가능성이 인더스트리 4.0에 상응하는 통신 “위”와 “아래”가 물리적으로 하나를 이루되, 논리적으로는 서로 분리되도록 하는 데에 있다(그림 28).

요구사항:

인더스트리 4.0–구성요소 하나(예컨대 기계 전체 등)에 또 다른 인더스트리 4.0–구성요소들이 논리적으로 배열되어 (임시) 세팅이 형성되도록 할 수 있어야 한다.

요구사항:

모든 인더스트리 4.0–구성요소들이 (임시로) 논리적으로 배열되어 있더라도 상위 체계들은 인더스트리 4.0–구성요소 모두에 목적과 관련하여 제한 가능하게 액세스할 수 있어야 한다.

6.3.3.9 상태모델

인더스트리 4.0–구성요소의 상태는 인더스트리 4.0에 대응하는 통신의 다른 참여자들에 의해 언제든 이용할 수 있다. 이는 개념 정의된 상태 모델에 따라 일어난다.

인더스트리 4.0–구성요소들은 계층구조로 조직될 수 있기 때문에 하위 상태들에 대한 적절한 디스플레이를 통해 어느 상태로 정의될 수 있어야 한다(어느 부분이 가동 상태가 아니라면 그것이 기계에 무슨 의미가 되는가?).

부가적으로 상태모델은 가상 이미지와 전문 기능성의 상태들에 대한 세세한 관찰을 허용하는 비교적 많은 상태 변수들로 보완되어야 한다. 그렇게 함으로써 어느 시점 ‘t’에 있어서 예컨대 통계적으로 정확한 데이터 분석의 목적으로 어느 인더스트리 4.0–구성요소의 상태에 대한 한결같은 관찰이 가능해진다.

6.3.3.10 인더스트리 4.0–구성요소의 일반 특징

GMA 7.21 [2]에서는 구성요소의 개념을 인더스트리 4.0의 맥락에서 다음과 같이 정의하였다.

구성요소란 개념은 일반적이다. 이 개념은 물리세계나 정보세계의 한 대상을 나타내는데, 이 대상은 그 시스템 환경에서 특정 역할을 하거나 그런 역할을 위해 마련된 것이다. 구성요소란, 예컨대 하나의 파이프, SPS–기능구성요소, 램프, 밸브, 지능형 구동장치(drive unit) 등일 수 있다. 중요한 것은 하나의 체계 안에서 맡게 되거나 이미 맡고 있는 역할의 단위요 관계(기능)로 보는 것이다. 우리가 인더스트리 4.0–구성요소라 부르는 것은 특수한 종류의 요소들이다. 인더스트리 4.0–구성요소들은 위에 설명된 분류의 특징들과 관련하여 특정 요구조건들을 충족시키는 것을 통해 드러난다. 인더스트리 4.0–시스템 안에도 이런 요구들을 충족시키지 못하고, 따라서 인더스트리 4.0–구성요소가 아닌 요소들이 많다.

여기에 제시된 개념은 수동적이거나 능동적이되 인더스트리 4.0에 상응하는 통신이 가능하지 않은 대상들도 허용한다. 따라서 이 보고서에서 말하는 인더스트리 4.0–구성요소들에는 다음 사항들이 중요하다.

- 인더스트리 4.0-구성요소는 CP-분류(classification)와 관련하여 CP24, CP34거나 아니면 CP44-구성요소다.
- 관리-셸이 있으며, 셸은 인더스트리 4.0네트워크 안에서 서비스체계의 완전한 참여자가 되도록 통신이 이루어질 수 있다.

다음 장에서는 GMA-정의[2]를 바탕으로 이 개념에 대한 상세한 설명이 제시된다. [2]와 완전히 일치하는 가운데 인더스트리 4.0-네트워크 내의 서비스체계 참여자로서 인더스트리 4.0-구성요소에 대해 다음과 같은 특징들이 요구된다(요구사항).

식별 가능성

인더스트리 4.0-구성요소는 네트워크 안에서 분명하게 식별될 수 있어야 하며 그 물리적 대상들도 명확한 ID를 통해 식별된다. CP34-요소나 CP-44 요소라면 통신주소(예컨대 IP-Address)를 통해 액세스 가능하다.

인더스트리 4.0에 상응하는 통신

인더스트리 4.0-구성요소는 적어도 SOA 원리(공통의 인더스트리 4.0에 상응하는 의미론을 포함하여)에 따라 서로 통신이 이루어진다.

인더스트리 4.0에 상응한 서비스와 상태

인더스트리 4.0-구성요소는 그 역동적인 행태를 포함한 가상 묘사를 제공한다. 이 묘사는 가상 재현과 마니페스토 Manifest로 다다를 수 있다.

인더스트리 4.0에 상응한 의미론 semantic

인더스트리 4.0-구성요소는 인더스트리 4.0-체계를 위해 표준화된 인더스트리 4.0에 상응한 의미론을 지원한다.

보안과 안전

인더스트리 4.0-구성요소는 그 기능과 데이터를 위해 과제에 상응하는 충분한 보안을 제공한다(Security). 추가적으로 사용에서 기능상의 안전, 기계의 안전 조치들도 필수불가결하다(Safty).

서비스 품질

인더스트리 4.0-구성요소는 그 과제에 필요한 서비스 품질(QoS)로서의 특성을 지닌다. 자동화기술에서의 사용과 관련하여서는 실시간 가능성, 자동안전장치(failure safty), 시계 동기화(clock synchronization) 등의 특징이다. 이 특징들은 프로필에 맞추어 이루어질 수 있다.

상 태

인더스트리 4.0-구성요소는 언제든 자기 상태를 제공한다.

세팅 가능성

인더스트리 4.0-구성요소는 저마다 다른 인더스트리 4.0-구성요소들로 이루어질 수 있다.

이 문서의 맥락에서 인더스트리 4.0-구성요소들은 생산체계, 기계, 스테이션 등을 나타내며 개념상 기계의 중요 부분 내지 모듈이다.

특징 (1)에 대해: 식별 가능성

"인더스트리 4.0" 방식의 목표는 모든 중요한 데이터를 실시간으로 액세스할 수 있게 하는 것이다. 인더스트리 4.0-구성요소들은 오늘날 확장된 인프라구조에 대하여 중요한 부분이 된다. 이는 생산체계 생애주기 전체에 걸쳐 적용된다. 따라서 인더스트리 4.0-구성요소들은 모든 인더스트리 4.0-가치창출 사슬[1]과 그 모든 가치창출 프로세스에서도 편재하고 통일된 정보교환을 위해 핵심 역할을 한다.

능동적인 인더스트리 4.0-구성요소는 인더스트리 4.0에 상응하는 통신 자체를 처리할 수 있다. 수동적 인더스트리 4.0-구성요소에 대해서는 없어서는 안 될 인프라구조가 이를 처리한다.

산업적 요구에 부합한 통신을 위해 필요불가피성이 있다. 생산체계들이 갈수록 연결되어 작업하고 그러면서 비교적 먼 거리도 극복해야만 하기 때문에 원거리 트래픽기술을 통해 로컬 네트워크들을 연결한다.

요구사항:

인더스트리 4.0–구성요소들을 네트워크로 연결할 때 원거리 트래픽기술은 로컬 네트워크들이 대체로 제한 없이 원거리트래픽연결을 통해 서로 통신할 수 있도록 해야 한다.

이는 해당하는 네트워크 연결들의 사용 가능성과 보안(security)은 물론이고 시간 관련한 적절성에도 해당한다. 스트리밍 streaming–기술이나 다른 메커니즘들이 적절한 솔루션의 바탕이 될 수 있다고는 하더라도 이에 대해서는 아직 더 근본적인 연구들이 필요하다.

한 차원 높게 보면 네트워크 연결들은 통신이 장기적으로 신뢰도가 높고 안정적으로 보장될 수 있도록 해야 한다. 여기서는 기존의 프로토콜이 인더스트리 4.0–사용에서도 유용한지 검증되어야 한다. 인더스트리 4.0–구성요소의 어드레싱(addressing)과 (사용)대상들의 어드레싱은 구별되어야 한다. 이 구별은 전 세계 차원에 생산자들을 아울러 1:1 대응의 ID를 이용하여 충족시킬 수 있다. IDs 문제에 대해서는 [4]와 [5] 및 다른 표준들을 참고하라.

참고사항:

인더스트리 4.0–구성요소의 어드레싱 addressing과 (사용)대상들의 어드레싱은 구분되어야 한다.

특징(2)에 대하여: 인더스트리 4.0에 상응하는 통신

인더스트리 4.0–구성요소의 자체정보는 서비스를 갖춘 서비스 지향적 아키텍처(SOA)를 바탕으로 서비스–모델에 상응하게 실현된다(리소스–매니저). 인더스트리 4.0–구성요소의 해당 프로필이 이 서비스가 기술적으로 어떻게 실현될 수 있을지 규정할 수 있다(예컨대 OPC–UA–기반 서비스를 통해).

특징 (3)에 대하여: 인더스트리 4.0에 상응한 이용과 상태

Shop floor와 Office floor내에 여러 가지 사용이 이루어져야만 하기 때문에 인더스트리 4.0–구성요소들이 여러 가지 사용차원을 여러 가지 프로토콜로 이용할 수 있는 옵션이 있어야만 한다.

요구사항:

따라서 프로토콜과 사용기능은 옵션에 따라 차후 로딩 될 수 있어야 한다.

특징 (4)에 대해: 가상 모사

인더스트리 4.0–구성요소의 중요한 역동적 행태를 포함한 특징들의 기술description에 대한 정보는 인더스트리 4.0–데이터 포맷에 있는 현실의 실제 구성요소의 가상의 모사로부터 생성될 수 있다. 이 모사를 가상의 재현이라 한다. 가상 재현의 일부가 Manifest인데, 명확한 의미론으로 입증되어야 한다. 여기서 중요한 역할을 하는 것이 특징들의 설명(specification)이다.

매니페스트의 부분에는 이를테면 다음과 같은 것들이 있다.

- 현실의 실제 구성요소의 특징적 징표
- 특징들 상호 간의 관계에 대한 정보
- 생산 및 생산프로세스에 중요한 인더스트리 4.0–구성요소들 사이의 관계
- 기계의 중요 기능들과 그 프로세스에 대한 형식적 기술(formal description)

가상의 이미지에는 이를테면 다음과 같은 것들이 있다.

- 상업적 데이터
- 내력과 관련한 데이터 – 예컨대 서비스 내력
- 기타 등등

특별한 Manifest와 일반 관리 대상들의 구분은, Manifest가 인더스트리 4.0–측면들에 부응하게 인더스트리 4.0에 상응하는 네트워크 실현을 위해 명확한 의미론에 따라 공개적으로 알려져야만 하는 정보를 포함하는 식으로 이루어진다. 관리 대상들 역시 저 정보를 지닐 수 있는데, 이들의 경우 어떤 형식으로 공개할지는 제조사에서 직접 결정할 수 있다.

특징 (5)에 대하여: 인더스트리 4.0에 상응하는 의미론

둘 또는 그 이상의 인더스트리 4.0-구성요소들 사이의 정보교환에는 일의적인 의미론이 요구된다. 이는 4장에서 설명된 인더스트리 4.0의 특징들을 통해 정해져야 한다. [4]에 따른 특징들의 분류가 다음 분야들에 도움이 될 듯하다.

- 기계구조(mechanics)
- 기능성
- 지역성
- 생산성
- 사업적 기본 조건들

특징들에 대한 설명은 [4], [5], [6] 참조.

특징 (6)에 대하여 : 보안과 안전

인더스트리 4.0-구성요소들은 저마다 보안-기능의 확보를 위한 최소한의 인프라구조가 필요하다. 보안이 확보되는 것은 오직 해당 생산프로세스가 보안-관찰에 직접 연결되었을 때뿐이기 때문에, 인더스트리 4.0-구성요소의 보안-인프라구조가 없어서는 안 될 것이지만, 전반적으로 출분한 기능을 사용하지 않는다. 통신의 보안, 기계의 안전(safety)이 확보되어야만 한다면, 이는 개별 인더스트리 4.0-구성요소들의 특성에 영향을 미치게 된다. 여기에 추가적인 특징들이 파악되고, 평가되어 상위 체계로 전달되어야 한다.

요구사항:

최소 인프라구조는 "Security-by-Design"(SbD) 원칙에 부합되어야만 한다.

특징 (7)에 대하여 : 서비스 품질

특정 환경에서 어느 인더스트리 4.0-구성요소를 사용하게 되면서 그 요구조건들이 정해진다. 따라서 해당 환경에서 요구되는 특징들(QoS)은 기계 또는 시설을 위한 요소들을 선정할 때부터 고려해야만 한다. 특별히 자동화 환경을 위해서는 다음과 같은 특징들이 고려되어야 한다.

- 예컨대 D1ms의 실시간 처리 능력이 있는 Deterministic 과 같은 생산적 통신을 위한 실시간 인터벌
- 주변 인터넷인프라구조와 관련한 최고의 자동안전장치(견고성)
- 시계 동기화
- 컴퓨터 시스템이나 프로그램의 상호 정보 교환 가능성
- 통일된 규칙 바탕의 진단과 엔지니어링
- 적절한 연결 구축

특징 (8)에 대하여 : 상태

인더스트리 4.0-구성요소들 저마다 특정 과제를 지닌 결합체의 부분을 나타내고 또 이 과제들은 프로세스에서 조정, 처리되기 때문에 매 시점마다 인더스트리 4.0-구성요소 저마다의 상태는 인더스트리 4.0에 상응하는 통신네트워크의 다른 참여자들에 의해 이용 가능해야만 한다. 이 정보들ㄹ은 다른 인더스트리 4.0-구성요소들의 지역적 관리와 프로세스의 조절을 위한 글로벌차원의 관리에 도움이 된다.

특징 (9)에 대하여 : 세팅 가능성

인더스트리 4.0-구성요소들은 인더스트리 4.0-구성요소 어느 하나와 합쳐질 수 있다. 따라서 예컨대 기계 하나가 인더스트리 4.0-구성요소가 될 수 있다. 이 구성요소 자체는 여러 개의 독자적인 인더스트리 4.0-구성요소들에서 나오는 구성요소들로 이루어질 수 있는데, 이를테면 모듈식 기계다. 개별 기계 모듈들 역시 다시 개별 인더스트리 4.0-구성요소로 나뉠 수 있다.

6.4 표준화와 규격화

6.4.1 배 경

독일 표준화 전략에 의하면 표준화[(영어로는 "법적인 표준(de jure standard)"])란 일반적 또는 반복적인 사용을 위한 활동들에 대한 규정, 지침, 특징들이 공인된 조직에 의해 완전한 합의 하에 마련된 것을 의미한다. 표준화란 독일 표준화 전략에서 사양(Specification)들을

작성해가는 과정을 말한다. 이를 위한 문서형식으로는 여러 가지가 있는데, 예컨대 VDE-사용규정이나 DIN-사양(DIN SPEC), PAS(Publicly Available Specifications), 기술 사양(TS), ITA(Industry Technical Agreement) 또는 TR (Technical Report) 등이 그것이다.

지난 해 DKE에서 1차 버전으로 발표하여 현재 수정작업 중에 있는 "DKE-로드맵 인더스트리 4.0"이 여기서 매우 도움이 된다. 이 문서의 목적은 전략적, 기술적 지향의 로드맵 구상을 지원하는 것인데, 이 지원은 산학합동연구 및 그에 상응하는 BMWi & BMBF-지원조치의 가이드라인을 특별히 고려하면서 인더스트리 4.0을 위한 표준과 사양들에 대한 요구사항들을 나타낸다. 그러면서 꼭 필요한 활동분야를 제시하고 그에 상응하는 지침들을 제시한다. 게다가 이 지원으로 이 분야의 표준과 사양들에 대한 개관이 제공된다.

표준화 로드맵은 플랫폼에서 한편으로는 재고조사(inventory)에 도움이 되고, 다른 한편으로는 자동화기술, 정보화기술, 통신기술, 생산기술 등 다양한 기술 섹터 참여한 행위자들 사이의 통신 수단 역할도 한다.

6.4.2 혁신의 원동력으로서의 표준화와 규격화

규격 및 표준은 기술적 창조 작업을 위한 안정적인 토대를 마련하고, 사용 사례에서 상호 정보 교환 가능성을 보장하며, 통일된 안전규정을 통해 환경과 시설 및 소비자를 보호한다. 표준은 제품 개발의 미래를 보장할 토대고, 통일된 개념과 규정들을 통해 모든 참여자들 사이의 소통(통신)을 지원한다.

표준화야말로 인더스트리 4.0이라는 미래의 프로젝트 성공에 핵심적 의미를 지닌다. 인더스트리 4.0에서는 도메인 경계나, 계층의 구분 또는 생애주기의 단계들을 넘어서는 시스템들의 통합이 요구된다. 이는 오직 합의를 바탕으로 한 사양과 표준의 토대 위에서만 가능하다. 그에 따라 플랫폼-인더스트리-4.0에서는 전반에 걸친 혁신의 창출을 위해 필요 불가결한 다음의 전제조건들을 마련하기 위해 연구, 산업, 표준화 사이의 긴밀한 협력이 이루어진다. 방법론적 기반 마련과 기능성, 안정성, 투장안전성, 실용성, 시장타당성(그림 29 참조). 산업 현장에 신속한 전환을 위해서는 합의에 기반한, 연구를 동반하는 표준화 과정을 통한 조속한 개념 안정화가 불가피하다.

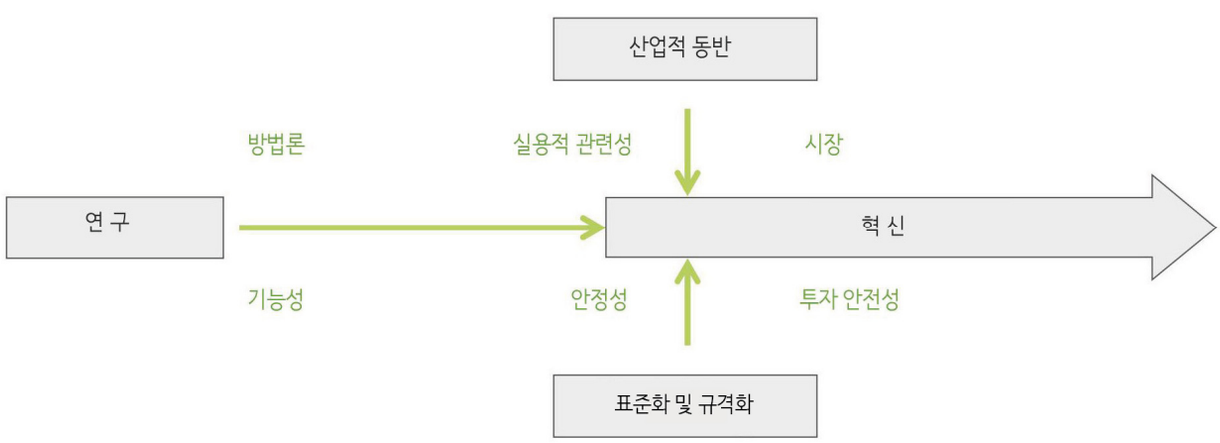


그림 29: 표준화를 통한 혁신([10]의 차용)

6.4.3 표준화 위원회와 규격화 위원회의 협업

지구 전역에서 활동하는 수출 지향적인 독일 산업을 위해 글로벌 차원에서 유효한 표준체계에 담긴 기술적 요구조건들을 확정하는 것은 특별히 중요한 의미가 있다. 목표는 통일된 기술 기능과 적용 가능성에 근본적으로 중요한 모든 결정들을 단계적으로 국제 표준으로 정하는 일이다. 여기서 중요한 목표-표준기관들은 무엇보다 IEC와 ISO다.

전산학 기술에 대해 중심 역할을 하는 것으로는 무엇보다 전 세계적으로 받아들여진 IETF와 W3C-컨소시엄의 표준들이다. 인더스트리 4.0을 위한 표준화의 목표는 한편으로는 적용 차원에서의 상호 통신 가능성의 개선이고, 다른 한편으로는 네트워크 품질의 개선이다.

합의에 기반한 표준안을 세우는 일은 여러 가지 경로를 통해 이루어진다. 그림 30에서는 전형적인 절차를 도식적으로 보여준다. 출발점은 특정 표준의 필요성을 확정하는 일이다. 표준의 필요성은 실제 적용 현장으로부터의 피드백을 통해, 새로운 기술의 성립을 통해, 연구 결과나 아니면 규제 목적에서 생겨난다.

국제 표준(ISO3, IEC4)에 이르는 길을 보면 다음 3가지 전형적인 루트를 구분할 수 있다.

- 해당 표준화 위원회 내에서 직접 확정. 이 경우 표준 확정 작업은 해당 국제 및 국가 그림자 위원회에서 이루어진다. 한 가지 예가 IEC/SC 65B/WG 7과 독일의 DKE/AK 962.0.3 "SPS언어" 안에서 IEC 51131-3 "프로그래머블 로직 컨트롤러(영어: programmable logic controller, PLC)의 개발이다.
- 컨소시엄의 사양을 직접 넘겨받기. 이 경우 컨소시엄 안에서 사양(specification 기술설명)이 작성되고, 그 다음 대체로 변경 없이 표준으로 받아들여진다. 이에 대한 예로는 이를테면 Batch-Control-사양 ISA S 88(ISA)이 IEC 62541로 받아들여진 경우나 PROLIST-사양이 IEC 61987로 받아들여진 경우가 있다.
- 합의에 기반한 국가 위원회에서 개발하고 이어서 해당 표준 위원회에서 더 발전시키기. 이 경우 전문가협회에서 기본이 되는 확정안이 마련되고 지침 또는 국가의 사양으로 공개되고 나서 두 번째 단계에서 해당 표준화 위원회에서 국제 표준으로 계속 발전시킨다.

대안이 되는 방식들이 그림 5.4.2에 제시되었다. 전자기술 표준안 영역에서 국가 차원의 표준은 오늘날 90%가 IEC의 국제 표준에 바탕을 둔다. IEC 표준들은 작성 과정에 유럽(CENELEC5)과 국제 차원에서 병행하여 조율되고, 이어서 국가 차원에서 DIN-표준으로 넘겨받는다(드레스덴-협약). ISO와 CEN의 경우 비교할 만한 처리 방식이 비엔나 협약이다.

지난 10년 동안 나타나듯이 해당 표준화 위원회를 통한 표준안과 표준 내용의 개발과 작성 작업마저도 점점 더 한계에 봉착하였다. 게다가 많은 경우에 명예직으로 함께 일하는 위원회 위원들의 시간마저도 충분하지 못하다. 이런 이유에서 컨소시엄과 전문가협회를 통해 광범위한 표준 준비작업을 하는 길이 여러 분야에서 대안으로 자리 잡았다. 인더스트리 4.0 플랫폼도 내용적으로 중요한 부분결과들과 관련하여 이 길을 걷게 된다.

표준화를 맡고 있는 위원회들은 그러면서 검증, 수정, 반주, 조언, 통합 등의 과제를 넘겨받는다. 이 위원회들에서는 이해 당사자 그룹이 내용과 계획된 접근방식을 통해 정보를 얻고 표준화 과정이 합의에 기반하여 성공을 거두도록 보장한다. 이런 과제들과 관리 기술적이고 편집기술적 일과업무들 외에도 표준화 위원회는 기존 표준환경에 대한 분석과 전략적으로 중요한 분야 표준화계획의 선도와 조율의 역할도 맡는데, 이쪽 역할이 갈수록 늘고 있다. 이 지점에서 표준화 위원회는 프랫폼 프로젝트 인더스트리 4.0에서의 작업 시작부터 아주 도움이 컸다. 이제 결과에 대한 평가라는 임박한 문제에서도 이들은 없어서는 안 될 존재다.

표준화 작업에서 컨소시엄과 전문가협회의 목표설정을 비교하면 원칙적인 차이 하나를 확인할 수 있다. 컨소시엄에서는 표준안을 확정하면서 완벽한 솔루션을 기술하려고 노력하는데, 전문가 협회에서는 솔루션의 개별 측면들에 대한 가이드라인이나 표준화를 만드는 걸 목표로 한다. 인더스트리 4.0의 주변환경에서는 두 가지 방향이 모두 필요하다. 국가 차원의 환경에서는 일련의 중요한 전문가 협회가 있다. 많은 경우 이들은 구성 범위가 워

낙 광범위하고 또 내적 합의를 바탕으로 조직이 꾸며지기 때문에 그들이 발표하는 것은 해당 전문가 공동체의 공통된 의견으로 이해될 수 있고, 그럼으로써 그 이후의 표준화 과정을 위해서뿐만 아니라 산업 현장에서 즉각 이용하는 데에도 특히 더 안전하고 안정적인 바탕을 보여준다. 이 플랫폼에도 이 점이 유용하였다. 다음과 같은 전제조건들이 충족될 경우 합의를 바탕으로 한 처리 방식이라고 이야기될 수 있다.

- 표준안의 완성은 위원회에서 이루어지는데, 이 위원회 안에서 전문가들이 각자 함께 일할 수 있다. 어느 조직의 회원 자격은 전제조건이 아니다. 회원 수가 제한되어야만 할 경우 투명하고 비차별적 절차에 따라 선발이 이루어진다.
- 이 위원회의 성과들은 조기에 초안(Draft for comment)으로 공개된다. 이 초안들은 조직 내의 회원 자격과 상관없이 누구나 꺼내 보고 평할 수 있다.
- 표준안으로 공개하기 전에 이의제기 절차가 있다. 여기서 누구든 이의제기를 할 수 있다. 위원회에서는 열린 토론에서 이의에 대해 고려하며 결정을 짓는다.

체결된 표준안은 공개되고 관심이 있는 사람이면 누구나 조직의 회원 자격과 무관하게 얻을 수 있다.

합의를 바탕으로 한 표준화로 먼저 국가 차원의 토대에서 조속히 기업 내의 개발 프로세스를 위한 견고한 표준화가 마련될 수 있다. 그 다음 이 표준안들은 국제적 표준화를 위한 훌륭한 출발점이 된다. 그런 점에서 특히 플랫폼-인더스트리-4.0 내부의 참조모델의 형식으로 인더스트리 4.0에 대한 개념의 개발과 그 개념을 국제적 표준으로 넘기는 것은 논리적이다.

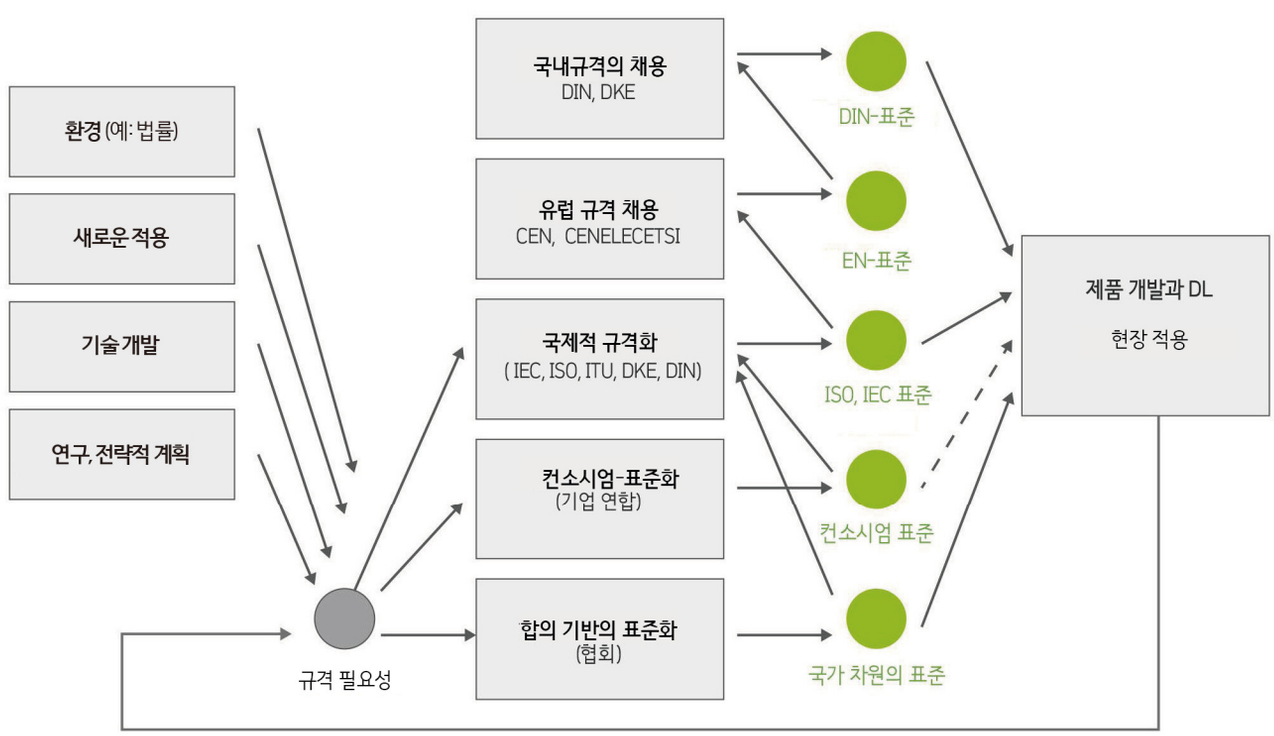


그림 30: 표준화 필요성에서 표준으로 ([10]에 상응)

문서 번호	제목	위원회
ISO/IEC 62264	Enterprise–control system integration	IEC TC65
IEC TR62794	Industrial–process measurement, control and automation – Reference model for representation of production facilities (Digital Factory)	IEC TC65
IEC 62832	Industrial–process measurement, control and automation – Reference model for representation of production facilities (Digital Factory)	IEC TC65
IEC 62541	OPC Unified Architecture	IEC TC65
IEC 61360–1 IEC 61360–2	Standard data element types with associated classification scheme for electric items	IEC SC3D
ISO 13584–42	Industrial automation systems and integration – Parts library – Part 42: Description methodology: Methodology for structuring parts families	ISO TC184
IEC 61987	Industrial–process measurement and control – Data structures and elements in process equipment catalogues	IEC TC65
IEC 62683	Low–voltage switchgear and controlgear – Product data and properties for information exchange	IEC TC17B
IEC 61804–1 IEC 61804–3	Function blocks (FB) for process control – General requirements Function blocks (FB) for process control – Part 3: Electronic Device Description Language(EDDL)	IEC TC65 IEC TC65
IEC 62453	Field device tool (FDT) interface specification	IEC TC65
IEC 62769	Devices and integration in enterprise systems; Field Device Integration	IEC TC65
IEC 62714	Automation ML	IEC TC65
ISO/IEC 2700x	Information technology – Security techniques – Information security management systems – Requirements	ISO/IEC JTC1
ISO 15926	Industrial automation systems and integration – Integration of life–cycle data for process plants including oil and gas production facilities	ISO TC184
ISO 8000	Data Quality	ISO TC184
IEC 62439	Industrial communication networks – High availability automation networks	IEC TC65
IEC 62443	Industrial communication networks – Network and system security	IEC TC65
ISO 15926	Industrial automation systems and integration – Integration of life–cycle data for process plants including oil and gas production facilities	ISO TC184
IEC 61158	Industrial communication networks – Fieldbus specifications	IEC TC65
IEC 61784	Industrial communication networks – Profiles	IEC TC65
IEC 62591 IEC 62601 EN 300328	Industrial communication networks – Wireless communication network and communication profiles – WirelessHART™ Industrial communication networks – Fieldbus specifications – WIA–PA communication network and communication profile Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) – Breitband–Übertragungssysteme – Datenübertragungsgeräte, die im 2,4–GHz–ISM–Band arbeiten und Breitband–Modulationstechniken verwenden	IEC TC 65 IEC TC65 ETSI

문서 번호	제목	위원회
IEC 62591 IEC 62601	Industrial communication networks – Wireless communication network and communication profiles – WirelessHART™ Industrial communication networks – Fieldbus specifications – WIA–PA communication network and communication profile	IEC TC 65 IEC TC65
IEC 61984	Connectors – Safety requirements and tests	IEC TC65
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety–related systems	IEC TC65
IEC 61511	Functional safety – Safety instrumented systems for the process industry sector	IEC TC65
IEC 62061	Safety of machinery – Functional safety of safety–related electrical, electronic and programmable electronic control systems / This document and its separate amendments continue to be valid together with the consolidated version	IEC TC44
VDMA 24582	Fieldbus neutral reference architecture for Condition Monitoring in production automation	VDMA
ecl@ss V9.0	Database with product classes and product properties	ecl@ss
IEC CDD	IEC Common Data Dictionary	IEC SC3D
PROFIBUS International Profile 3.02	Profile for Process Control devices	Profibus Internationa
Sercos	Function Specific Profiles	Sercos International
Recommendation 5th Edition 2008	XML	W3C
Recommendation 5th edition 2014	HTML5	W3C
VDI 5600	제조매니지먼트 시스템	VDI
…	…	…

표 1: 인더스트리 4.0에 중요한 등급으로 인정된 표준들의 공개 목록

6.4.4 결 론

합의에 바탕을 둔 표준안 개발은 해당 위원회에서 전 세계 차원에서 장기간에 걸쳐 지속적으로 지원하고 있다. 독일에서는 특히 DKE과 DIN이, 유럽에서는 ETSI, CENELEC, CEN이, 그리고 국제 차원에서는 IEC와 ISO가 있다. 이 지침들로 마련된 표준화 위원회 외에도 특히 합의에 바탕을 둔 표준화 위원회가 플랫폼–인더스트리–4.0 내에서 조직된 산업계 기업 연합들과 연합하여 표준안 작성과 표준안 제안 등의 작성을 통해 표준화를 추진한다. 국가 차원에서 여기에는 예컨대 VDI/GMA가 있다. 여러 위원회들에게 보장된 협업은 플랫폼–인더스트리–4.0의 성과들을 평소의 방식으로 이행하는 것을 지원한다.

그럼에도 불구하고 인더스트리 4.0과 함께 새로운 주제 영역들과 특히 시스템–지향적 접근방식이 초점이 된다. 층위와 도메인을 아우르는 개념들이 개발되고 그런 다음 표준이 된다. 이제까지의 연구 결과로서 확정지을 수 있는 것이라면 인더스트리 4.0이 기존하는 표준들로부터 일련의 개념들 위에 구축될 수 있다는 사실이다. 물론 그중 몇 가지는 수정–보완되고 또 확장되거나 새로운 표준들이 만들어져야 한다는 것은 분명하다. 기존하는 표준의 환경은 인더스트리 3.0의 회유경로(migration path)를 지속적으로 지원한다. 잠재적으로 중요한 표준들의 공개 목록이 표에서 제시되었다. 이 목록은 특히 근본적인 자동화 표준들로 예컨대 ICT–표준만큼 단계적으로 확장되고 DKE와 DIN의 “인더스트리 4.0” 표준화–로드맵의 개정판 형식으로 공표될 것이다.

6.5 주제영역들의 로드맵

참조아키텍처 모델 인더스트리 4.0(RAMI 4.0)과 인더스트리 4.0-구성요소들의 작성과 토론과 함께 이제 앞으로 지속될 작업을 위한 첫 번째 바탕이 마련되었다. 곧 이어질 중요한 주제들이 아래에서 설명된다. 그 가운데 중요한 목표의 하나가 한편으로는 사용 층위에서 상호 통신 가능성의 개선이고, 다른 한편으로 인더스트리 4.0에서 제기되는 요구조거들에 따른 네트워크 품질의 개선이다.

식별 가능성

식별 가능성은 모든 것들이 알아서 제 스스로의 존재를 찾을 수 있기 위해 없어서는 안 될 전제조건이다. 첫 토론들에서 이미 드러났듯이, 상품 운송에서의 식별, 장소의 식별, 네트워크 내에서의 식별 가능성이 필요하다. 이와 관련하여 여러 가지 표준들이 존재하지만, 부분적으로는 새로운 기술적 가능성들과 함께 여러 가지 보완들에 대해서도 토론될 것이다.

의미론

RAMI 4.0에서 중요한 층위 하나가 정보 층위다. 여기서는 무엇보다 데이터들이 보관되어 있다. 생산자들을 아우르는 데이터의 교류를 위해서는 데이터를 위한 문법을 포함한 통일된 의미론이 필요하다. 이에 대한 첫 고민들이 존재하는데, 표준을 포함한 전체 구성을 위한 개념을 세우는 게 중요하다는 것이다. 포괄적인 특징들의 정의를 위한 토대로서 “인더스트리 4.0”에서는 예컨대 eCl@ss의 사양서가 마련되어 있다.

서비스 품질(QoS) / 인더스트리 4.0-구성요소의 서비스 품질

이로써 인더스트리 4.0-구성요소의 중요한 특징들이 정해졌다. 이 특징들은 채택 내지 이용이 가능하다. 구성요소들 사이에는 서비스 품질 관련한 통일 협약이 가능해야 한다. 자동화 기술에서의 적용과 관련하여서는 실시간 처리 능력, 자동안전장치(신뢰도), 시계 동기화 등과 같은 특징들이 필요하다. 저와 같은 특징들은 프로필에 기술될 수 있다.

인더스트리 4.0-통신

자동화기술과 전산기술에는 통신네트워크와 프로토콜들이 이미 많다. 여기에다 텔레커뮤니케이션(원격 통신/전자통신)기술과 전산기술 분야에서 새로운 방식들이 더해진다. 그 모든 방식들이 인더스트리 4.0-통신에 대한 요구조건들에 부합하게 그 적용 가능성을 검증하고 경우에 따라 수정되어야만 한다. 여기서 RAMI 4.0에서 통신 층위의 구조화 가능성이 제시된다. 이 통신을 이용하여 적절한 표준의 식별 절차가 잘 설명될 수 있다. 표준화를 위해 예컨대 적절한 후보들을 모두 층위에 기재하는 것이다. 교차와 중첩되는 것들에 대하여 토론하고 우선하는 프로토콜을 정의한다. 경우에 따라 구멍이 있다면 메운다.

표준 기능:

커다란 과제중의 하나가 제조사들을 아우르는 (RAMI 4.0의 기능 층위에 디스플레이된) 표준 기능들을 형성하는 것이다.

단순한 정보교환과 제조사들 사이의 상호 통신 가능성을 위해서는 통일된 기본기능들을 정하는 것이 필수적이다. 따라서 간단하면서도 정보교환에 중요한 기능들이 공개적으로 상술되어야만 한다. 그럼으로써 사용자에게 기계/시설/공장에서 인터페이스 적응 비용을 확연하게 낮추어줄 수 있다. 이에 대한 본보기로는 컨디션 모니터링 확정과 관련한 VDMA의 기준표(Standard Sheet)가 있다. 여기서는 제조사들을 아우르는 표준기능들이 정해졌을 뿐만 아니라 제조사들 저마다 자기만의 기능들을 끼워 넣을 수(캡슐화) 있는 모델도 하나로 통일되었다. 그 과정에서 데이터 교환과 컨디션 모니터링 기능의 연결도 쉽게 유지된다.

네트워크화된 시스템의 안전성

7. 네트워크화된 시스템의 안전성

7.1 머리말

보안은 인더스트리 4.0-가치창출 네트워크를 "가능하게 하는 존재"(Enabler)이다. 인더스트리 4.0 개발과정에서 결정적으로 중요한 것은 선형(線形)의 가치창출 사슬이 가치창출 네트워크로 변화한 사실이다. 가치창출 파트너 모두를 이와같이 완벽하게 네트워크로 연결함으로써 지금껏 알려진 바 없는 정도로 많은 관계자들이 깊이 그리고 부분적으로는 즉석에서 기업 프로세스와 제작 프로세스에까지 연결할 수 있게 되었다. 효율성을 추구하고 생산성 측면의 이익을 확보하기 위해 파트너들은 민감한 생산 데이터와 프로세스 데이터들을 상호 교환할 수 있다. 이는 오직 파트너들 사이의 신뢰를 바탕으로 할 때만 가능한 일이다. 핵심 노-하우(즉, 각 기업의 핵심-자산)를 적어도 일부라도 함께 나누어야 하기 때문이다. 신뢰는 정보와 데이터들이 안전하고 정확하게 실제로 정당한 접근 자격이 있는 파트너들 사이에서 입증될 수 있도록 교환될 수 있을 때에 형성된다. 이를 보장하는 것이 바로 인더스트리 4.0에서 안전의 과제다. 오피스 시스템과 생산 시스템에서 확실하게 보장된 보안 없이는 인더스트리 4.0을 실현할 수 없다. 민감한 커뮤니케이션 프로세스를 위한 신뢰가 형성될 수 없기 때문이다.

보안에 대한 부가적인 도전이라면 인더스트리 4.0의 구현 과정들이 보안상 안전할 뿐만 아니라 이용 친화적이고 이용자 편의적으로 이루어져 고객의 수용성까지 확보하는 일이다. 고객들이 원하는 것은 결국 플러그 & 오퍼레이트(Plug & Operate) 방식이다. 게다가 개별 고객들과 인더스트리 4.0의 조율 과정에서 고객이 바라는 것들이 생산프로세스에 직접 영향을 미치는 경우가 증가하고 있다(예컨대 자동차생산과정의 로트 사이즈 1 참조). 필수불가결한 B2B와 B2C 사이의 긴밀한 커뮤니케이션이 보안상 안전하고 정확하며 법적으로 안전하게 보장되어 진행될 수 없다면, 추구하는 사업모델들의 실현 가능성은 희박하다. 보안-조치들이야말로 이 요구사항을 충족시킬 수 있는 바탕이 된다.

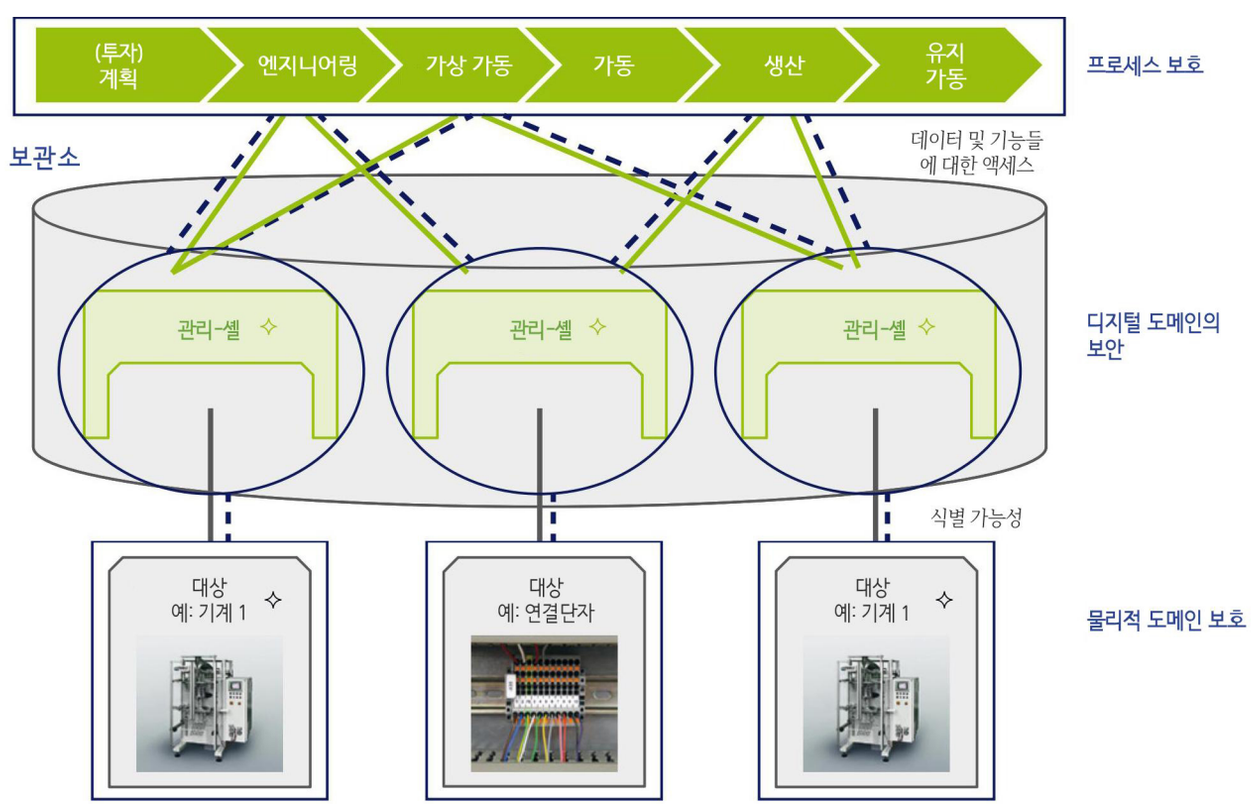


그림 31: 보안 요구들

인더스트리 4.0–개발의 현재 차원에 비추어보면 다음과 같은 원칙이 중요하다.

물리적 도메인과 디지털 도메인, 해당 프로세스들과 이들 영역들 사이의 커뮤니케이션 등을 총 망라하는 보안이 인더스트리 4.0의 성공을 위한 전제조건이다. 개별적인 보안 적용은 비켜가기 쉽고 따라서 효과가 없을 것이기 때문이다.

안전은 누구에게나 중요하다

기업들은 기업 내외부의 다차원성을 관리해야 하는 과제에 직면해 있다. 인더스트리 4.0에는 정적(靜的)인 선형 조직도(Organigram)와 같은 기업내 조직의 "사일로식 사고방식"(silo mentality)은 더 이상 있을 수가 없다. 생각할 수 있는 것은 예컨대 생산프로세스들이 ERP–수준의 통합적 구성 요소들이 된다(참조: 생산네트워크들이 갈수록 더 기업 네트워크의 통합 성분이 된다.). 장기적으로 이런 발전양상은 오피스–IT와 생산–IT의 융합으로 이어지고, 그럼으로써 정적–선형적 기업조직의 필수불가결한 과제가 된다. 그에 따라 횡단면을 가로지르는 주제로서 전 분야로 이어지며 통합되어야 할 과제들이 더 많아진다. 기업 내 편재하고 끊임없이 이어지는 위험 및 안전에 대한 관리는 인더스트리 4.0과 함께 없어서는 안 될 것이다. 다차원성이 생겨나는 것은 이 매니지먼트 과제가 더 이상 "내적", "외적"으로 구분될 수 없기 때문이다. 위험 및 안전 매니지먼트는 인더스트리 4.0에서 변화를 거쳐야 하고, 외부 관계자를 통해 전통적으로 내적 프로세스에 직접적 영향을 미치는 경향이 강해지는 걸 받아들여야 한다. 고전적으로 "울타리 쳐진" 그리고 이를 통해 규정할 수 있는 기업영역은 해체 된다. 가치창출 네트워크 안에서 기업의 내부와 외부의 넘나듦이 물 흐르듯 하며 언제나 유동적이다.

이러한 상황하에서 기업은 더 이상 자신의 안전을 혼자서 해결할 수 없다. 생각할 수 있는 예방수단들을 모두 동원한다 하더라도 안전한 것으로 인정될 수 없다. 고객과 공급자가 긴밀하게 맞물림으로써 해당 접점들이 공격 가능성으로 이용될 수 있는 곳이라면 고객과 공급자의 보안–매니지먼트는 자체 보안수준에도 영향을 미친다. 전체 가치창출네트워크의 안전에 대한 취약한 부분이 미치게 될 영향은 오늘날보다도 앞으로 더 강해지게 된다. 이에 따라 인더스트리 4.0에 있어 보안은 누구에게나 중요하다는 사실을 원칙으로 인정해야 한다. 보안은 해당 기업의 규모가 얼마나 큰가와 상관없이 그 어느 관계자가 더 많은 역할을 해야 하는 게 아니라 공동의 책임이다.

보안은 움직이는 표적

인더스트리 4.0에서 보안에 대한 다차원적 검토의 필요성은 오늘날 이미 적용되는 기술 원칙을 바탕으로 더 많아질 인터페이스들 때문에 중요성이 더 커지게 된다. 보안은 "움직이는 표적"으로 이해되어야 한다. "어디를 겨냥해야 하는가?"와 "어떤 수단을 쓸 수 있는가?"와 같은 핵심 물음들은 언제나 새로 재평가되어야만 한다. 보안전략은 저마다 그에 맞서 그 전략에 영향을 미치는 대응전략의 탄생을 초래하기 때문이다. 게다가 기술의 발달이 공격방법과 가능성들을 끊임없이 변화시킨다. 기술과 사람을 통한 조치들마다 그에 해당하는 비용을 들여 기술과 사람을 통한 조치들로 맞설 수 있다. 따라서 보안에는 언제나 변화가 가능하고 동적인 위협상황이 상존하여 끊임없는 대응변화가 요구된다. "설치하고 잊어버린다!"는 의미의 효과적인 보안의 구현이란 있을 수 없다. 무엇보다 보안과 기업안전(= 기계에 대한 사람의 보호)의 기본적인 차이다. 안전–수칙들은 확고한 그리고 부분적으로는 법적으로 규정된 규정들과 전술적 평가가 가능한 가정에 바탕을 두고 있다.

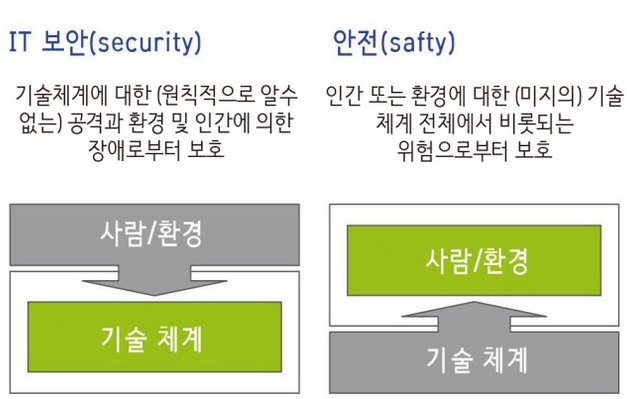


그림 32: IT 보안 대 안전

인더스트리 4.0–가치창출 네트워크에서 보안–분야의 높은 역동성 때문에 효율적이고 적응 능력이 있는 보안–리소스의 투입이 요구된다. 이에 대한 기반은 기업 내의 고유한 가치들과 그 가치들의 보호 필요성에 대한 지식이다. 경제성의 이유만으로도 보안–조치들이 변화 가능해야 할 뿐만 아니라 적절하기도 해야 한다. 모든 자산이 다 예컨대 "고도로 안전하게" 보호되어야만 하는 것은 아니다. 요구되는 조치들은 오직 지속적인 위험매니지먼트를 통한 기업 운영으로만 실현할 수 있다. 해결해야 할 것은 다음과 같다. 무엇을 어느 정도 비용과 보호의 필요성으로 지켜야 하는가? 평가결과는 이후의 모든 조치들에 대한 방향을 제공해주며 어느 정도 간격을 두고 정기적으로 평가되어야 한다.

인더스트리 4.0에 대한 100%–보안이란 존재할 리 없다

"무빙 타겟"의 역동성과 기술의 발전으로 보안은 다음 두 가지로 이해되어야 한다. 첫째, 보안이란 기술과 사람 및 프로세스가 통합된 것이다. 둘째, 보안은 현장에서 특별한 개별 사건이다. 보안은 완성된 제품으로 구매할 수 없다. 보안조치의 필수적인 특징들은 기업의 사정에 맞게 결정되는 부분이 크다. 따라서 보안이란 주제에서 원칙적으로 인정하고 넘어가야 하는 것은 보편적으로 적용되는 솔루션이란 존재할 수 없다는 사실이다.

7.2 가정, 가설, 전제조건

인더스트리 4.0의 아키텍처, 모델, 시설들 하나하나가 확립되지 않았다 하더라도 개별 산업구성요소들 간에 자동화되고 기업들을 아우르는 커뮤니케이션이 점점 증가하리라는 기술적 경향만큼은 신뢰성 있게 가정할 수 있다. 특히 보안의 시각에서 볼 때 이런 경향에 따라 함께 초래되는 여러 가지 결과들이 있다. "완결된 공장"이란 단위로 확정할 가능성이 흐려진다. 책임의 영역에서 내부와 외부를 명확하게 경계짓기도 갈수록 어려워진다. 이는 물리적 의미에서뿐만 아니라 디지털/정보기술적 의미에서도 마찬가지다. 인더스트리 4.0–가치창출네트워크에서는 공급자와 생산자 사이에 아주 긴밀한 커뮤니케이션 프로세스가 성립하는데, 경우에 따라 여기에서 실시간 조건으로 생산에 중요한 결정들이 내려지기도 한다. 따라서 어느 공급자가 생산자의 생산 프로세스에 직접적인 영향을 미칠 수도 있다. 이에 따라 프로세스 장애는 쌍방향으로 영향을 미칠 수 있다. 내부 프로세스의 통제 가능성과 제어가능성은 감소하고 상호 의존성은 높아진다. 자체 기업 영역에 구체적인 영향을 미치는 결정적인 영향의 범위는 자체 처리역량 범위를 벗어난다.

이제 공장의 경계는 공장의 울타리를 벗어난다. 이제까지는 물리적 도메인(울타리 + 수위/경비서비스)은 물론 정보기술적 도메인(인트라넷과 인터넷의 구분, DMZ 도입)에 대해서도 출입구를 통제할 수 있다. 그러나 인더스트리 4.0과 더불어 고전적인 영역 개념은 동적이고 경우에 따라 즉석에서 정의할 수 있는 방향으로 바뀔 수밖에 없다.

보안–가설

이러한 발전 양상들은 7.1장에서 설명한 핵심 내용들과 함께 다섯 가지 보안–가설로 정리할 수 있다. 이 가설들은 미래의 인더스트리 4.0을 위한 아키텍처와 모델들의 개념화 과정에서 처음부터 함께 생각해야 한다.

1. 가치창출 네트워크 자체가 공격 벡터가 된다.

   기업 자체로서는 커뮤니케이션 차원과 제조 차원에서 엄청난 수단을 동원하여 시스템을 보호할 수 있을지도 모른다. 이 모든 것은 공급자와 고객들의 시스템 역시 마찬가지 신뢰수준의 보안이 지켜지지 않는다면 곧 휴지조각이 되어 버리고 말 수 있다. 인더스트리 4.0–환경에서는 공격과 장애가 외부 파트너의 시스템들을 통해서도 일어날 수 있다는 사실을 감안해야만 한다. 자체 통제되는 영역이라는 순 "내적 시각"으로는 충분하지 못하다. 특히 예컨대 공급파트너가 바뀌는 경우 시작단계부터 예방, 보안–설정(set up), 적절한 방식에 따른 시험검증은 사업 합의 내지 관계설정의 필수요소이어야 한다. 이를 위해 보안 대책들에 대한 상호 (신뢰할 수 있는) 합의가 필요하다.

2. 안전기능의 취약성이 증가한다.

산업생산 전 분야에 걸쳐 네트워크 연결이 가속화됨에 따라 상호 왕래 과정에서 조작과 방해공작의 잠재적 가능성이 수적으로나 파급효과의 깊이로나 증가한다. 기계나 시설의 자체 기능제어에까지 자격과 권한이 없는 공격이 이루어질 수 있는 가능성이 증가한다. 극단적으로 생각하면 조작이 불가능한 영역이란 존재하지 않는다.

인더스트리 4.0에 의하여 기계나 시설들의 가장 내밀한 기능제어 부분까지 디지털화가 증가한다. 여기에는 경우에 따라 안전기능[예컨대 긴급차단, 접속보호, 자전벽(electric screen), 화상보호(burn protection) 등]을 포괄하기도 하는데, 이들의 경우도 마찬가지로 공격받을 수 있다. 지금까지 안전기능은 별개였고, 최고 이용가능성과 신뢰성을 보장하기 위해 부분적으로는 과잉으로 설치되기도 하였다. 인더스트리 4.0-환경에서 네트워크화는 이제 안전장치들과 다른 장치들 사이의 기술적인 성격이 더 큰 인터페이스와 "접점"이 많아지는 결과를 낳았다. 시스템들에 대한 접근 가능성은 이런 방식으로 이론적으로는 더 커졌다. 말하자면 보안사고(예컨대 외부의 해커공격)를 통해 안전사고가 초래될 수도 있다는 의미다(금속 압연에서 끼임이나 협착에 대한 보호체계를 작동시키는 차광막 제어장치의 조작 같은 것이 그 예다). 지금까지 안전 체계와 나머지 체계들을 일부러 분리시키거나 캡슐화(모듈화)하였지만, 이는 지양되어야 한다. 지금까지 안전 규정은 유연성 증가로 점점 더 지키기 어려워진다.

로봇 지원(robot-assisted) 제조 공정처럼 사람들이 기계와 긴밀하게 함께 일해야 하는 분야에서 이 상관관계가 갖는 폭발력은 강하다. 그 결과 지금까지 서로 분리시켜 보았던 (안전에만 표준이 정해진) 영역들은 갈수록 더 상호의존적으로 이해되어야 하고, 안전개념도 그런 방향으로 수정되어야 한다.

3. 탐지 및 대응능력이 기본이다

여러 보안사건들을 평가해본 결과 분명하게 드러나는 것은 보호조치들마다 그에 상응하는 비용을 투입하면 피해갈 수 있을지도 모른다는 사실이다. 그러나 "100% 보안이란 존재하지 않는다." 이 말은 (보안)제품이면 제품, 조치면 조치 그 어느 것도 궁극의 안전을 보장할 수는 없다는 뜻이다. 어느 공격을 인식하는 데 걸리는 평균시간은 오늘날 수백일로, 해당 기업들로부터 인지되지 못하는 공격의 수도 점점 느는 추세다.

여러 가지 기술적 조치와 조직적 대책을 강구하더라도 시간적 여유와 조사능력 및 보안지식이 많은 공격자의 공격(이른바 ATP 공격)에 대응하는데에는 한계가 있다. 그런 식의 목표를 정하여 장기간에 걸쳐 이루어지는 공격은 현재의 안전조치들로서는 발견할 수 없는 것이다.

국가의 지원을 받는 조직들이 그러하지만, 프로세스나 사람들 및 기술 등의 신뢰관계에 바탕을 둔 공격의 가능성들은 훨씬 더 광범위한 것으로 나타났다. 그와 같은 공격을 막는 일은 그 전문성에 비추어볼 때 경제적 비용을 감당할 수 없다.

일상적인 공격들과 사이버-범죄의 스펙트럼에서도 그 역량 수준이 점차 높아진다. 조만간 사건이 일어날 것이다. 이 모든 걸 차단하는 방화벽이란 존재할 리가 없다. 다시 말하자면 그런 사건들을 식별하고 거기에 대응하여 가능한 자체적으로 해결할 수 있으려면 필요한 곳에 전문역량이 존재해야만 한다는 말이다. 예방이나 대응 조치들의 협력으로서의 보안조치(탐지능력이 내포된 것)의 견고성(robustness)은 도입부에서 언급한 바 있는 가정 하에서 인더스트리 4.0의 보안에 결정적이다. 예측해 보건대 향후 전문적인 공격들은 실시간은 물론 신속하게도 확인할 수 없을 것이다. 외부를 통해 보안이 뚫린 사실이나 새로운 공격가능성에 대해 나중에 가서야 전해 듣고 알게 되는 경향은 무엇보다 중간 규모의 기업들에서 심화될 것이다. 그러나 꼭 필요한 탐지역량과 대응

역량을 강화한다면 APT 공격들을 공격 중이나 공격이 끝나 후 확인하거나 적어도 추후에 그 규모나 효력의 깊이를 적절히 평가하여 대응조치들을 개선할 수는 있을 것이다. 그럼으로써 기업들은 민감도를 높여도 되는 것이 무엇인지 알 수 있을 뿐만 아니라 더 효율적이고 그에 따라 비용도 더 절감할 수 있도록 대응할 태세를 갖추게 된다.

4. Office 영역에서 알려진 탐지역량들은 생산영역을 위해 개발되어 장착되어야 한다.

   아직까지 보안의 초점은 Office-커뮤니케이션체계에 있다. 이는 이제까지 통용되는 공격 벡터며 취약점이 오피스-체계와 관련되었다는 사정 때문이다(예컨대 운영체계, 브라우저, 인터넷 기반의 커뮤니케이션, 디스켓 같은 데이터 저장매체 등). 그 결과 통상의 보호조치는 정확하게 이 영역에 초점이 맞추어졌다(예컨대 바이러스 스캐너, E메일 암호화, 하드 디스크 암호화, 데이터 트래픽, 데이터 액세스 등). 생산 영역의 산업적 커뮤니케이션을 위해서는 "침입-탐지-시스템"(Intrusion-Detection-System) 같은 식의 상용화된 상품들이 존재하지 않는다. 스틱스넷(Stuxnet)과 같은 산업분야 공격들에서 보이듯, 저런 종류의 프로그램들은 발견되기까지 수개월에서 여러 해에 걸쳐 활동할 수 있다.

   기업들은 노-하우-보호-이유에서 정보를 얻고 대처할 수 있는 능력을 갖추는 데 관심이 크다. 이에 따라 위와 같은 "맹점"들은 보안카드에서 식별하여 체계적으로 해소시킬 수 있다. 그것은 또 조직, 인력, 기술 등과 관련한 보안에 대한 투자들이 지금까지 신경 쓰지 않았던 분야들에서도 이루어질 수 있다는 뜻이기도 하다.

5. 인더스트리 4.0에서는 데이터의 분산 저장이 보안의 핵심 과제가 된다.

   빅데이터, 예측 분석, 지능형 센서 기술 등을 이용하게 됨으로써 인더스트리 4.0안에 새로 생기는 일자리며 서비스들이 많아질 수 있다. 데이터 전문가들과 분석 내지 평가 프로그램들의 도입은 잠재적 효율성을 실현해야 한다(예컨대 금속 프레스에서 데이터 지원의 스탬핑 공정(stamping process)으로 자재의 낭비를 최소화하는 것). 여러 가지 평가를 위해서는 프로세스, 기계, 시설 등에 대한 매우 특수한 노하우가 필수 불가결하다. 즉, 운영자는 경우에 따라 자신의 데이터를 외부 서비스 수행자 및/또는 생산자에게 분석하라고 넘겨주거나 인터페이스를 통해 데이터 트래픽에 통합시켜야 한다는 말이다. 그 밖에도 클라우드 플랫폼이나 그 밖의 기타 데이터플랫폼들이 위치에 구애받지 않는 산업제어와 생산을 가능케 한다.

   생산과정에서 데이터 생성, 데이터 전송, 데이터 가공 등의 작업은 경우에 따라 디지털로 외부 플랫폼을 통해 이루어질 수도 있다. 그로 인해 운영자는 기술적 및 보안과 관련한 문제와 아울러 법적인 도전들에 직면하게 된다. 기업은 경우에 따라 추가로 주요기반시설을 사용하고, 또 추가로 외부의 관련자를 끌어들이되 데이터에 대한 그의 영향을 조건적으로만 통제한다. 데이터 플랫폼 제공자가 자국의 법적 영역 외부에 있다면 계약 조건들이며 인가도 이루어지기 어렵다. 그런 식의 플랫폼들의 경우 필수적이고 지속적인 기술적 접근성 때문에 수직·수평적 네트워크를 갖춘 가치창출 네트워크의 요구사항에 상응하여 가능한 공격 벡터 수가 많아진다. 포괄적인 데이터 보안이나 정보보호 등의 확보 없이는 인더스트리 4.0에 데이터를 분산 저장하는 것은 실현할 수 없다.

보안-개발의 원칙: 보안의 실행은 각 기업의 출발점이 되는 상황에 따라 유동적으로 구체화된다.

여기서 제시된 가설은 문맥에 비추어 보면, 출발점이 되는 기존의 상황과 단절되지 않고 보안이 실행된다는 것을 뜻한다. 보안의 관념은 모두 기존의 시스템과 시설에 바탕을 두고 구축된다. 하위 체계에 추가적인 테마로서의 보안이 "Security-by-Design" 원칙으로 바뀌는 근본적인 변화는 시설 및 구성요소들의 세대교체를 통해

단계적으로 이루어지게 된다. 보안-표준의 계속적인 개발도 똑같다. 완전히 새로운 표준을 책정하는 대신에 기존 규정의 수정이 필요한 곳이 많다. 기업의 의사결정에 있어서 보안기능을 순수한 비용요소로 파악하는데에는 앞으로도 변화가 없을 것이다. 규모가 큰 기업들의 경우 규모의 경제원칙에 따라 장치를 교환하거나 새로운 보안장치를 구축하기 위한 투자를 실행하기가 비교적 쉽다. 그러나 소규모와 중간 규모의 기업들은 보안에 본격적인 투자를 하기 어렵다.

아직까지 고립되어 있는 지적재산의 영역들, 그로 말미암아 조작이 밝혀지지 않고 남아 있는 분야들이 많이 있는데, 스마트 센서체계와 같은 기술발달을 통해 보안관련 빅데이터(Big Security Data)와 조합하면 그런 영역에 보안조치를 투입할 새로운 가능성들이 열린다.

7.3 인더스트리 4.0의 위협 구도

오늘날 세계에서 Office 영역과 생산영역에서 IT에 대한 위협들이 존재한다는 사실은 더 이상 논란의 여지가 없다. 지난해만 해도 응용분야와 시스템들의 취약지점들이 드러난 경우가 많았다. 그 결과 기업들에 대한 성공적인 다양한 공격들이 공개되기도 하였다. 그런 공격의 한 사례가 2014년에 알려진 악성코트 "Havex"다. 이 악성코드는 산업적 제어 및 조종체계들에 대한 정보들만 노리고 모아들였다. 생산지시와 관계된 것일 수도 있고 또 다음 공격에 사용될 수 있는 인프라구조에 대한 데이터들일 수도 있다. 계속해서 경우에 따라 시설에 피해를 줄 수 있는 다른 모듈을 다운로드할 가능성도 있다.

이 공격의 범위 안에서 여러 시설 생산자의 웹사이트들이 조작되었다. 이제 소프트웨어-업데이트를 목적으로 어떤 시설이 제조사 웹사이트에 접속하면 그 커뮤니케이션을 공격한다. 따라서 고객의 시각에서 보자면 그 공격은 그럴듯하고 또 시설과 제조사 사이의 합법적인 커뮤니케이션처럼 보이기 때문에 짐작컨대 처음에는 눈에 띄지 않았을 것이다. 현대의 다른 공격들 역시도 합법적인 액세스로 가장하기 때문에 보안사고들을 식별하는 문제는 기업들에게 새로운 도전거리가 된다. 식별한다고 하더라도 그저 소급해서 적용할 수 있을 뿐일 때가 많다. 그래도 그러는 편이 여전히 전체 인프라구조를 완전히 새로 설치하는 것보다는 훨씬 비용이 적게 들 수 있다. 예상 수치이긴 하지만 기업들에 대한 또 다른 공격들 수가 상당할 것으로 보인다. 그 과정에서 피해는 데이터 절도에서부터 공갈협박에다 운영 및 생산 과정에 대한 직접적인 피해에까지 이르게 된다.

이로 보아서 생산시설에 대한 위험은 오늘날에도 이미 존재하고 있고, 기업들은 그 위험에 대처해야만 한다는 사실이 분명하게 드러난다. 인더스트리 4.0은 앞의 도입부에서 설명한 경향과 함께 프로세스와 시설의 생산성과 가능성들을 향상시키기 위한 새로운 가능성들을 제공한다. 인더스트리 4.0 구성요소의 관리 셸 역시 거기에 속한다. 점점 더 역동적으로 변해가는 커뮤니케이션과 참여한 서비스 수행자들로 말미암아 안타깝지만 새로운 공격가능성들도 생겨나고 그에 따라 새로운 위협들도 발생한다. 이러한 위협들은 관리 네트워크와 자동화 네트워크 둘 다에 똑같이 적용된다.

특히 더 보호할 가치가 있는 시스템들이 인터넷으로부터 접속할 수 없게 한 경우가 많다. 생산 분야에서도 그런 경우가 많다. 공격자들은 이런 자리에 2단-도약-기술을 즐겨 쓴다. 먼저 어느 한 컴퓨터에서 보호가 덜한 영역을 공격하여 거기에 악성코드를 설치한다. 그런 다음 이 컴퓨터로부터 기업의 깊은 영역에 다른 공격들을 실행한다. 이런 종류의 침투는 장기적으로 작용하는 경우가 많아 급속히 퍼지지 않기 때문에 나중 또는 사후에서야 알려지기도 한다. 그에 해당하는, Stuxnet처럼 의도적으로 노리고 하는 공격들을 "Advanced Persistent Threat (APT)"로 나타낸다. 이른바 "Air Gap"은 더 이상 충분한 보안을 제공하지 못한다.

공격자들은 종종 정보기관, 사이버 범죄자, 사이버 활동가 등 3가지 유형을 구분하기도 한다. 사이버 범죄자들은 자신들의 활동을 통하여 불법적으로 돈을 벌고자 한다. 기업 또는 사적 개인에 대하여 특정 데이터를 지우거나 시스템이 작동되지 못하게 한다고 위협하면서 공갈협박을 통해 돈을 요구하는 것이다. 사이버-활동가들의 경우 정치적 또는 이념적 목표들을 추구한다. 이 경우 기업 내부 정보의 절도와 공개에서부터 디도스-공격(DDos attack)

혹은 시스템 불능화 등이 진행된다. 이 두 개의 그룹에 대해서 자기 기업을 보호하는 것이 중요하다. 정보기관과 관련한 공격자들의 경우 기업을 위한 리소스가 거의 무한하기 때문에 그들의 공격 루트 전체를 차단한다는 것은 경제적으로 받아들이기가 어렵다.

이처럼 의도적으로 노린 공격들 외에도 기업들은 우연하게 발생하는 문제들, 이를테면 사람의 잘못된 행동이나 드라이브-바이-다운로드-공격(Drive-by Download-attack)[13] 처럼 표적으로 삼지 않은 공격들에 대해서도 대비해야 한다. 이런 공격은 관리네트워크와 자동화 네트워크 사이에 악성코드를 퍼뜨리는 것이거나 아니면 원치 않는 시스템의 환경설정 오류(구성의 오류)일 수도 있다.

공격-소프트웨어의 개발은 갈수록 전문화되고 특히 자동화 영역을 노리는 일이 주목할 만큼 늘고 있다. 그 목적은 우선 스파이 행위다. 그에 대한 하나의 예로 "BlackEnergy"란 악성코드다. 이 코드는 특정 제조사의 HMI-시스템을 노리는데, 노출된 시스템들은 악성코드로 인한 변화 이후에도 눈에 띄지 않은 채 계속된 분석에 악용된다. 현재 나도는 이 악성코드는 대략 2008년부터 여러 차례에 걸쳐 개작된 것으로 오늘날에는 모듈식으로 추가 기능을 보충할 수 있도록 보완되었다. 이 코드는 스파이-그룹[14]에 속하는데, 이 그룹은 최근에 HMI 시스템과 SCADA-시스템을 위한 프로그램소프트웨어를 타깃으로 한 바 있다.

독일의 어느 제철소 용광로에 대한 성공적인 공격[8] 이전에도 이미 스파이-단계가 펼쳐졌으리라고 전제할 수 있다. 아무튼 지금까지 공격 진행경로에 대한 지식이 없다는 점이 그걸 암시한다.

7.3.1 기업 내에서의 가치

계속해서 위협들에 대해 파악하기 위해서는 어떤 기업이 가치가 있는지 보아야 한다. 보안의 맥락에서 기업 보호의 핵심은 시설, 시설의 일부 또는 합금 데이터와 처방 데이터 혹은 어떤 서비스에 놓일 수도 있다.

생산시설의 경우 지금까지는 근본적으로 사용성에 집중해왔다. 배합공식(recipe, formular)에서는 신뢰도에 초점을 두었다. 이는 기업에 생존적 의미가 있는 자산에 대한 두 가지 사례일 뿐이다. 이 분야에서 연구 및 개발의 본질적인 비용이 투여되었기 때문이다. 새로 생겨나는 경향들과 생산에 도입되거나 통합되는 신기술들로 말미암아 다른 자산들도 서비스의 형식으로 추가될 수 있다. 이는 그 전까지 핵심적 역할을 하지 못했고, 아직 아예 존재조차 하지 않거나 지금까지 격리된 영역에서만 운영되던 IT-체계들(주문수령이나 생산조정을 위한)일 수 있다. 이에 관한 사례들로 제품이나 구성요소들에 대한 디지털 ID나 자동으로 체결된 계약들의 관리와 법적 승인 등을 들 수 있다.

이어서 트렌드와 개발 상황과 관련된 새로운 위협들에 대해서 좀 더 상세하게 살펴보기로 한다.

7.3.2 가용성과 신뢰도

기업의 프로세스들은 시스템의 지원을 받는다. 시스템이란 예컨대 기계 하나, 시설의 일부 또는 IT-시스템 하나일 수도 있다. 인더스트리 4.0 구성요소의 관리 셸도 마찬가지로 이 영역에 들어 있다. 인더스트리 4.0에서는 운영에 필수적인 시스템과 기업들을 아우르는 통신의 인터페이스의 증가와 운영프로세스 역동성의 증가에서부터 출발해야 한다.

이들 시스템들이나 그 인터페이스들을 이용할 수 없게 되면 이는 기업 프로세스, 가치창출은 물론 그로 인해 재정적 측면에도 다소간에 직접적인 영향을 끼친다. 생산이나 다른 서비스에 심각한 장애가 일어나면 기업의 직접적인 위험이 된다. 예컨대 물리적 손해를 방지하기 위하여 각종의 장치를 일시에 정지시킬 필요가 발생하는 위험도 생각할 수 있다.

외부에서 접속할 수 있는 인터페이스에 대한 위험은 예방하기 힘든데, DDoS(Distributed Denial of Service)공격이 그 예다. 이 공격의 경우 이를테면 엄청난 조회를 하여 수신자가 과부하에 걸리거나 사용 가능한 네트워크 대역

13) 미리 준비해둔 웹사이트로 이용자를 유도하여(악성코드로 오염시킨 다음), 거기서부터 웹브라우저의 취약점을 이용하여 이용자의 시스템을 위험하게 만드는 공격.

14) (러시아의) "Sandworm"

폭 전체를 차지하여 합법적인 조회들을 더 이상 처리할 수 없게 만든다. 시스템 접근과의 연결과 관련한 장기간에 걸친 DDoS-공격으로 파산해버린 기업 사례들도 이미 있다[8].

인더스트리 4.0에서는 시간 임계적 프로세스나 서비스들이 더 많이 생기고, 그와 함께 DDoS의 추가 공격지점들이 생겨난다.

고도로 동적인 데이터들이 있는 산업 환경에서 거의 실시간으로 처리가 이루어지면 Office IT 보안에서 흔하게 이루어지는 나머지 교정조치들을 위한 여지가 거의 없게 된다. 이때 처리되어야 할 데이터들은 정확해야 할 뿐만 아니라 상황에 따라서는 여러 시스템들이 시간적 동기화를 이루어 동시에 사용하여 처리해야만 할 때도 있다. SCADA 시스템[(감시제어 데이터 수집 시스템(supervisory control and data acquisition system)]은 여러 시스템들이 가지고 있는 여러 가지 프로세스데이터들을 자동화 하여 계산하고 제어명령들을 컴퓨터를 써서 전달한다. 제어명령 처리를 위해 필요한 데이터들에 통신장애가 발생하면 동적인 인더스트리 4.0 환경(예컨대 에너지 분야 기업)에 커다란 문제가 될 가능성이 있다.

7.3.3 표적으로서의 안전

앞서 언급한 바와 같이, 한 기업 내에서 네트워크화와 리소스의 공동 사용 현상이 증가함에 따라 제한된 범위지만 안전 요소들에서도 그런 현상이 이루어지고 있다. 이에 따라 공동 네트워크에서 다른 시스템들과 함께 운영되는 경우가 늘어나는 추세다. 그 결과 다른 요소들과 마찬가지로 안전-요소들도 네트워크를 통한 똑같은 공격들에 노출된다. 여기서 공격들은 안전 관련 기능들을 향하기도 하지만 아울러 사용 가능성에 대한 간접 공격들도 역시 생각할 수 있다.

가용성에 대한 간접적 공격

안전기능에 대한 공격은, 이를테면 시설이나 기계의 긴급-차단 기능을 위협하게 된다. 이는 예컨대 아주 많은 트래픽을 통해 해당 구성요소의 과부하나 이용되는 네트워크의 과부하 또는 그 구성요소 안의 소프트웨어 오류를 통해 일어날 수 있다. 그럴 경우 애초 계획된 안전-기능의 중지를 야기한다. 그러나 안전-요소의 본래 기능만큼은 이런 경우에도 유지되어 사람이나 환경에 위험이 없도록 하지만, 그럼에도 제품 생산 과정에 제한을 초래한다.

안전을 위한 기능에 대한 공격

아주 심각한 경우 안전-구성요소 안의 취약점을 이용하여 이를테면 한계-값(threshold value)이 변화되는 것과 같은 기능의 조작으로 이어지기도 한다. 그 결과 기능상의 안전(보안과 안전 모두 포함한)이 더 이상 보장되지 않는다. 사람과 환경에 대한 손상은 이 경우 오직 기계적 장치와 같은 추가 보호조치를 통해서만 막을 수 있다. 이에 해당하는 보호기능들은 법규정(예컨대 기계지침)을 통해 강제되기 때문에 표준화 위원회에서 이미 안전-요구사항들의 충족을 위한 보안-요건의 통합안을 작성하였다.

7.3.4 완전성(integrity)

생산에 사용되는 데이터의 완전성은 물론이고 표시된 데이터의 완전성 역시 매우 중요하다.

생산에 사용되는 데이터에 대한 공격을 통해 생산된 제품의 품질이 부정적인 영향을 입을 수 있다. 극단적인 경우에는 이를테면 안전에 중요한 제품 성격의 변화로 나중에 인적 또는 물적 손실을 초래할 수 있다.

생산과정을 다시 추적해보기 위한 기록의 완전성도 마찬가지로 중요한데, 업종 분야나 제품에 따라 법적 책임 문제가 제기될 수 있거나 심지어는 제약-산업에서처럼 규제요건이 될 수 있다.

위에서 언급한 이유에서 보듯이 거의 모든 분야가 완전성에 대해 최고의 의미를 부여한다. 다만 함의적으로만 그럴 때도 많고 또 관계자들 생각에는 후술하는 신뢰도가 더 중요한 측면처럼 보이는 경우도 있다.

나아가 기업들을 망라하는 인더스트리 4.0의 가치창출 네트워크 안에서는 진정성[15]이라는 문제가 추가적으로

15) "아이디 절도" 위협 참조.

대두된다.
인더스트리 4.0 안에서 프로세스의 조율을 위해 훌륭한 동기화가 필수적이기 때문에 시간의 완전성 역시도 중요하다.

7.3.5 기밀성

오늘날 기업에게는 특정 정보들(많은 경우에 시간적 제한이 있음)을 기밀로 다루는 것이 중요하다. 여기에 속하는 것으로, 예컨대 배합공식, 구축 데이터 또는 제어 프로그램 같은 것들이 있다. 이 데이터들은 한 기업에 엄청난 가치가 된다. 그 데이터를 만들어내는 데 많은 비용과 지식이 소요되었기 때문이다.

의사에 반하는 정보유출에 대하여 보통 "데이터 절도"(data theft)라는 개념이 쓰인다. 그러나 데이터가 실제로 도난당한 게 아니라 복사되었고, 그에 따라 원본이 아직 남아 있다는 점에서 안타깝지만 이 개념은 적확하지 않다. 따라서 "데이터 절도"에서 본질적인 문제는 알려지지 않은 채 넘어갈 수 있다는 점이다.

절도나 데이터에 대한 부당한 액세스의 경우 남는 문제는 특히 이 경우 이 과정을 되돌리거나 대안적 보호조치를 취할 가능성이 없다는 사실이다. 처음 데이터를 잃어버린 순간부터 기업은 그 다음 계속해서 이루어지는 부당한 액세스에 대한 완전한 통제권을 상실하고 만다. 여기에는 안전의 경우와 같은 최후의 보루가 없다. 따라서 계획 단계에서부터 그에 합당한 조치를 고려하고, 무엇보다 기업에 아주 중요한 데이터들은 해당 표시를 하고 그 취급에 관한 명확한 규정을 두는 것이 필요하다.

지금까지 정보를 도둑질당하지 않거나 공개되지 않도록 하는 책임은 오로지 해당 기업에게만 있었다. 인더스트리 4.0에서는 이 책임이 그 기업과 관련된 다른 기업들에게도 넘어간다. 따라서 극히 중요한 데이터들을 신뢰할 수 있게 다루는 것을 보장하기 위해 그에 상응하는 표시나 처리 및 책임소재에 대한 계약 규정들을 마련하는 것이 중요하다. 자격 분류 과정에서 이를테면 몇몇 데이터는 하나의 최종 제품 또는 하나의 기계 자체를 통해 자체 제어로 주어지도록 고려해야 한다. 최종 제품의 사양(spec)은 경쟁사가 스스로 측정하는 것이 가능하다. 이 경우 기밀성이 특히 중요한 것은 그 제품이 공개되기 전이다. 그 다음에는 기존 제품만 가지고도 복제가 얼마든지 가능하기 때문이다.

이처럼 민감한 데이터를 가공하는 것에 대한 사례가 바로 주문자 위탁 생산지(OEM)에게 설계 데이터를 건네주는 경우다. 주문자 위탁 생산자는 정해진 수의 제품만 제작해야 한다. 여기서 확실히 보장되어야 하는 게 주문한 수의 제품만 제작되고 그 이후 정보는 다시 사용될 수 없어야 한다는 점이다.

또 다른 예가 유지보수를 위한 원격 제어다. 이 경우 기계 제작자는 기계나 생산 네트워크에 대한 광범위한 액세스가 주어질 수 있다. 충분한 안전조치가 없을 경우 이런 방식으로 시스템으로부터 가동률과 생산제품 수 그리고 다른 데이터들을 생산네트워크로부터 얻어낼 수 있다.

민감한 기업 관련 데이터들과 무관하게 직원들과 관련한 정보들도 고려해야 한다. 특히 인더스트리 4.0에서 추구하는 로트 사이즈 1의 경우 신상관련 정보들도 생산계약에 맞물려 처리된다는 걸 감안해야 한다. 여기서 법-규정들을 고려해야만 하고 안전이 보장되어야만 한다.

7.3.6 조작(의도적인 경우와 비의도적인 경우)

사보타주와 사람의 잘못된 행동은 익히 알려진 문제다. 이런 문제들은 오늘날에도 이미 일어나고 있다. 기업 내의 네트워크화가 점점 더 진척됨에 따라 그리고 가치창출 사슬에 연결되는 기업들이 늘어감에 따라 문제의 결과가 미치는 파장은 점점 더 광범위해지고 제어 가능성은 작아진다. 특히 (프로세스와 관련한) 더욱 역동적인 조회들로 인하여 충분한 책임처리와 소통 통로 및 (기술적으로) 충분한 네트워크 분할이나 액세스 콘트롤이 이루어지지 않을 때 그런 문제가 심각해진다.

가능한 액세스 포인트 숫자가 더 늘어남에 따라 공격자에 의한 승인 받지 않은 접속의 위험성도 더 높아진다. 위험한 액세스 포인트에 속하는 것으로는 무엇보다 관리자 없는 스테이션들, 개방되거나 보안 조치 없는 네트워크 액세스와 다른 기업들과의 연결점들(예컨대 유지보수나 주문처리를 위한 것)이다. 인더스트리 4.0의 도입과 함께 기업들을 아우르는 네트워크화와 그 역동성이 커지면서 위험성도 새로운 수준에 다다른다. 연결된 기업들로부터 계약 상대를 겨냥하는 공격들이 점점 더 늘어날 수 있다. 그에 따라 공격에 대한 분석에서 계약 상대방의 보안매니지먼트 분석 필요성도 더 커진다.

위험요소로 등장하는 것으로 특히 정보 유출이 있는데, 그럼에도 조작된 주문 데이터나 생산 데이터가 끼어들어올 수 있다는 점도 생각할 수 있다. 그 결과는 민감한 정보에 대한 승인 없는 액세스와 기계 및 시설에 대한 조작을 비롯 차단이나 파괴에까지 이를 수 있다.

7.3.7 아이디 도난

신뢰관계라는 것이 보안조치에서 아주 특별한 역할을 한다. 예컨대 어느 웹사이트를 방문할 경우 이용자는 거기서 받은 주소가 전혀 엉뚱한, 위험한 – 어쩌면 바로 그 목적을 위해 준비된 – 웹사이트로 유도하지 않을 거라고 믿는다. 웹서비스에서도 마찬가지로 신고된 이용자가 신고한 당사자일 것이라고 믿는다. 이 신뢰관계는 사적으로나 사업적으로나 마찬가지로 통용되며 보통은 여러 가지 보안조치들(기밀에 해당하는 등록정보-인증데이터, 키-토큰, 생체정보 등)을 통해 확인된다.

그런데 아이디 도난의 위험은 한편으로는 공격자가 정당한 사람인 척하며 그 사람의 합법적인 액세스권한을 갖게 되는 것으로 발생한다. 다른 한편으로는 인증절차가 예컨대 액세스 프로토콜에서 합법적인 이용자의 것과 구분되지 않으면서 발생한다. 여기서 이 위험을 막아낼 원칙들이 여러 가지 있다. 그래서 오늘날 공개적으로 다다를 수 있는 서비스(이를테면 Gmail)들은 Geo-IP를 이용해 이용자가 실제로 위치하는 곳이 어디인지 확인하고 – 다른 여러 나라에서 액세스가 이루어질 경우에도 – 이용자에게 급히 알린다. 진짜 이용자가 시스템에 신고를 하여 그 잠재적 보안사고에 대한 정보를 받으면 이를 확인하거나 부정할 수 있다. 여기서 해당 당사자와 함께 하는 검증을 위한 상호작용이 필요할 때가 많다. 그럴 경우 회신(피드백)으로 검증 절차가 개선되어 언젠가는 완전히 기계적으로 자동화가 이루어진다.

인더스트리 4.0에서 아이디 도난은 다음 두 가지 이유로 시스템의 이용성과 정보의 신뢰성에 대한 심각한 위험이 된다.

관련된 사람, 서비스, 시설, 센서 등의 위상이 동적으로 변할 수 있다. 그 변화는 많은 아이디와 아울러 많은 공격 가능한 벡터들을 의미한다. 더 나아가 기계는 유연하게 의사결정을 내릴 가능성을 활용하지 못한다. 그럼으로써 보안조치들의 식별과 개선 및 자동화가 어려워진다. 여기 이 문제는 기계-대-기계-아이디에서 생기는 경우는 별로 없고, 그보다는 공격자가 기계인 척 하는 데에 있다. 여기서 중앙 관제소가 필요하다는 걸 예상할 수 있다. 관제소는 등록정보, 커뮤니케이션 행태나 교환된 정보량 등을 파악하고 감시하며 잠재적인 아이디 도난의 경우 검토하여 확인하도록 전달하는 역할을 한다.

7.4 인더스트리 4.0을 위한 보안 목표와 안전관련 요구사항

수평적 및 수직적인 가치창출 사슬을 포함하는 인더스트리 4.0은 기계와 시설의 네트워크화와 기업-IT와 인터넷 연결의 결합을 대대적으로 촉진한다. 외부로부터의 공격에 대한 보호와 이른바 내부자에 의한 조작에 대한 보호는 인더스트리 4.0의 높아진 요구사항들을 감안해야 한다.

인더스트리 4.0에서는 산업 보안(industrial security, 즉 생산에서의 보안)과 IT 보안(Office) 사이의 마찰 없는 협력이 근본 전제가 된다. 이 협력은 공동의 표준화된 안전한 IT인프라구조라는 목적으로 구축될 수 있다.

7.4.1 일반적 보호 목표

오늘날 생산 환경에서 널리 알려진 다음의 보호 목표들은 인더스트리 4.0에서도 똑같이 높은 비중을 차지한다.

- 가용성
- 완전성
- 노-하우의 보호/기밀성

여기에 다음 사항들이 추가된다.

- 진정성
- 시간의 완전성 – 특히 여러 기업들을 망라하는 가치창출 네트워크에서의 완전성
- 추적성(traceability)
- 법적 확실성(legal certainty)

진정성은 가치창출 네트워크에서 본질적인 특징인데, 여러 회사들을 아우르는 커뮤니케이션이 이루어지는 경우에 특히 더하다. 추적성에 대한 요구는 사람(예컨대 직원이나 고객)에 대한 신상 데이터들이 처리될 경우 즉시 제기되는 정보보호의 필요성에서 비롯한다. 전체적으로 볼 때 보안 메커니즘을 통한 프라이버시/정보보호의 기술적 지원이 중요한 역할을 한다.

이 보안 목표들은 운영기능, 감시기능 및 보호기능(예컨대 안전 Safety)에 대해서도 똑같이 적용된다. 시스템에 대한 기능상 안전(functional safety)에서 중요한 것은 적절한 조치들을 통해 어느 기계나 시설의 기능에서 사람이나 환경에 아무 위험이 생기지 않도록 보장하는 일이다. 여기서 특별한 현상("프로필")의 경우 일일이 보안의 부작용이 없도록 하는 것도 신경 써야 한다.

7.4.2 인더스트리 4.0을 위한 Security-by-Design

인더스트리 4.0-시나리오의 실현을 위해서는 정보안전의 보호를 위한 조치들을 미리부터 고려하는 것이 꼭 필요하다. 여기서 중요한 것은 사후적으로 기술적 메커니즘을 보안에 통합하는 것이 아니라, 그보다는 제품개발과 프로세스 과정에 시설과 인프라구조의 보호에 대한 통합원리가 필요하다는 사실이다.

목표는 필요한 보안-기능들을 제품 내지 솔루션의 통합 부분으로 실현하는 것이다. 해당 표준에 보안을 명확히, 그것도 처음부터 정착시키는 일 외에도 시설의 제조사와 운영자에 대한 중요성도 제기된다.

기존 프로세스들에 대한 포괄적인 보완이 필요하다.

기존의 개발과정들도 맞게 수정되어야 한다. 보안-장비들을 목표가 되는 지점에 장착하기 위해서는 특히 나중에 나온 제품을 제대로 사용하는 경우를 고려한 위협과 위험의 분석이 필요하다. 어느 제품을 위한 보호조치들의 보호목표들은 해당 제조사, 통합-완성한 기업, 운영자 등의 보호 가치가 있는 자산과 경우에 따라 (국가 별 사정에 따른) 관청 측의 규제요건(예컨대 아주 중요한 인프라구조에 장착할 게 기대될 수 있을 경우)에 바탕을 둔다.

보안 디자인은 생산시설의 생애 – 10년에서 15년까지 -를 고려해야 한다.

보호되어야 할 자산의 식별이 끝난 다음에는 위협 및 위험 분석을 실시한다. 확인된 위험들에 따라 가능한 안전조치들을 선정한다. 이때 경제적 측면도 중요한 역할을 한다. 보안-조치들은 목표 아키텍처의 사업모델에 적합하고 그와 결부되는 금융비용을 감당할 수 있을 때 비로소 시장에 수용된다.

암호작성(cryptographical) 구성요소를 선정할 때에는 수출 가이드라인과 그와 결부된 절차들을 고려해야 한다. 특히 데이터 암호화 기능이 여기에 해당하며, 순수한 인증메커니즘이나 통합메커니즘은 덜 중요하다.

통합된 안전조치가 이루어진 제품들이 여러 영역에 장착되어야 할 때 이행되어야 할 조치들 – 역시 여러 가지 안전수준을 지원해야 하는 경우 – 의 선택폭으로 이어지기도 한다.

오늘날 안전성 검토의 초점은 방화벽(Firewalls), VPNs, 원격 네트워크 액세스 등 네트워크 보안의 영역에 포함된 기능들에 놓인다. 인더스트리 4.0과 함께 이런 사정은 분명 달라진다. 복잡하고 분산된 사용들은 Security by Design으로 사전적 안전조치들을 포함하고 있어야 한다. 보안 프로필은 "민첩"(agile)해야 한다. 즉 역동적

으로 변경할 수 있어야 하고 조정할 수 있어야 한다. 내포된 보안은 신속한 (재)구성이 가능해야 한다.

익숙한 품질관리 조치들에 전형적인 보안조치들을 보완해야 한다. 특히 다음과 같은 것들이 여기에 속한다.

- 취약성 테스트와 침투 테스트
- 생산과정의 완전성 확보, 특히 보안-프로토콜과 암호화의 경우
- 필요한 자격(예컨대 IEC 62443에 따른 인가 등)의 취득은 개별적인 경우 의도하는 보안수준에 따라 장기간의 시간과 다액의 추가 비용을 야기한다.

명확한 보안기능의 절차적 수행 그 자체 외에도 특히 소프트웨어 품질이란 의미에서 소프트웨어 기반의 적용을 확실하게 구현하는 것 역시 담보해야 한다. 확실한 실현을 위해서 관계된 소프트웨어 엔지니어의 교육과 결과 및 취약지점에 대한 목적 관련 품질 테스트도 필요하다. 품질관리 경험도 평가하고 이를 디자인 프로세스에 적용해야 한다.

7.4.3 아이디 관리

인더스트리 4.0-가치창출 네트워크에 참여하는 기계, 이용자, 제품 등을 위하여 필요한 것은 명확하고 위조방지 처리된 아이디로 이것은 디지털 인증을 통해 확인된다. 이 디지털 인증은 신분인증을 위한 열쇠도 되지만, 그 밖에 암호화와 암호 해독화 때에도 꼭 필요한 정보를 담고 있다.

보안에 중요한 정보들을 보관하기 위해서는 신뢰도가 높고 안전한 저장장치가 필요하다. 보안 프로토콜과 통합 보안의 사용은 그에 따라 요구되는 인증데이터(credentials)를 이용해 확실히 보호되어야 한다. 그에 대한 전제가 가치창출 네트워크를 따라가며 명확하고 한결같은 ID확인(identification)과 어느 참여자의 ID 할당을 책임지며 ID를 바탕으로 인증과 권한의 부여를 지원하는 아이디 인프라구조[(복잡성의 정도에 따라 하나 또는 그 이상의 기관(instance, authority)]이다.

인더스트리 4.0-가치창출 네트워크에 참여하는 모두의 디지털 ID를 관리하는 당국으로서 신뢰할 수 있는 인증기관(Certification Authorities, CA)이 요구된다.

효율적인 아이디 관리를 확보하기 위해서는 등록 정보/참여자의 인증을 안전한 ID로 개별화하거나 기기에 연결해야 한다.

아이디 관리는 언제 어디서나 지적 재산의 보호(IP 보호)를 지원해야 한다. 여기에 속하는 것으로 무엇보다 제품모델과 생산모델이 있다. 이를 위해 중요한 전제가 되는 것이 이용자가 받아들여 사용할 수 있는 디지털 권한 관리(rights management)다.

7.4.4 가치창출 네트워크의 동적 구성 가능성

효율적인 가치창출 네트워크에는 인더스트리 4.0-시설의 동적 구성/재구성이 요구된다. 보안-관리는 인더스트리 4.0-시설이 역동성을 지원해야 한다. 그러기 위해서는 표준화된 보안 언어(security semantic)를 이용한 인더스트리 4.0-구성요소의 보안-성격의 기술(보안-프로필)이 불가피하다. 이 프로필에는 또 커뮤니케이션-인터페이스/-프로토콜과 그것의 보안-성격에 대한 명시적인 기술도 담겨 있다.

보안-성격은 참조아키텍처 의미론의 구성요소로서 존재해야 한다.

그 기술에서 인더스트리 4.0-구성요소에 어떤 보안-역량이 있는지 그리고 가치창출 네트워크 안에서 요구되는 보안-수준이 어떤 절차로 도달될 수 있는지 제시되어야 한다.

구성요소들 안의 보안-기능들은 가치창출 네트워크와 관련하여 그때그때 요구되는 것들을 제대로 처리할 수 있기 위해 원칙적으로 여러 보안-수준들을 지원할 수 있어야만 한다. 이 전제조건들로 인더스트리 4.0-구성요소의 보안-프로필의 집성을 통해 인더스트리 4.0-시설의 결과로 도출되는 보안-수준에 대한 간략한 평가가 가능해야 한다.

보안 프로필은 그에 따른 적절한 보호기능을 통해 동적으로 변화하는 가치창출 네트워크에 요구되는 유연성을

지원할 수 있어야 한다. 인더스트리 4.0의 이질적인 시스템 환경에서 이 유연성을 지원하기 위하여 표준화의 필요성을 크게 높인다(참조: KITS Roadmap– Normungs–Roadmap IT–보안, DIN/DKE, 2015년 2월 17일).

전체적으로 볼 때 (커뮤니케이션 보안과 네트워크 중심 보안에 대한) 종래의 시각은 사용 층위를 위한 복합적인 보안 아키텍처로 이동하게 된다.

7.4.5 가상 인스턴스를 위한 보안

인더스트리 4.0에서 생산의 "가상 인스턴스"(virtual instance)는 중요한 역할을 한다. 보안요구사항의 물리적 실현 외에도 이 가상의 재현을 위한 그에 합당한 보안이 동시에 요구된다.

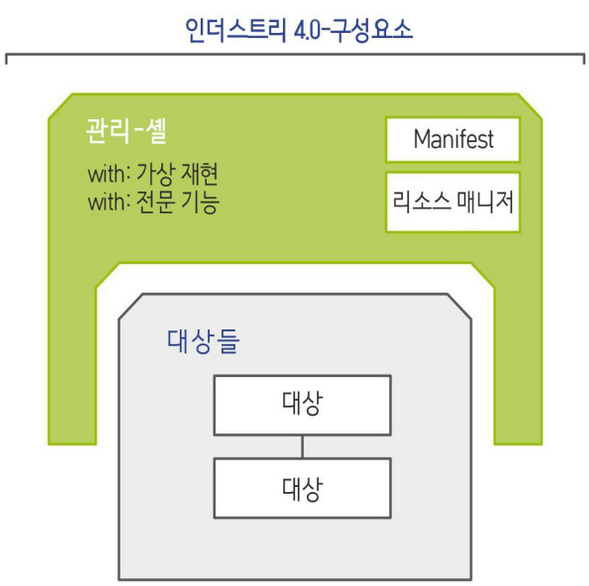


그림 33: 인더스트리 4.0–구성요소

논리적 시각에서 볼 때 인더스트리 4.0–구성요소는 하나 또는 그 이상의 대상들과 관리–셸을 포괄하며, 이 관리–셸에는 가상 재현의 데이터와 전문 기능성의 기능들이 포함된다.

요구사항:

상위 체계들의 종류에 따라 관리대상들은 하나 이상의 상위 IT–체계에 분산될 수 있어야만 한다.

(Office–플랫폼 내지 클라우드에 대한) "가상 인스턴스"의 분산에 따라 보안의 물리적 실현에서와는 다른 보안 경계–조건들이 생긴다. 당연히 물리적 층위와의 상호작용 역시 안전하고 추적 가능하게(traceably) 구성되어야 한다. 그럼으로써 사용–층위를 위한 복합적인 보안–아키텍처들이 요구된다. 여기서 특히 중요한 요구들이 노–하우–보호와 완전성이다. 보안에 대한 고전적인 도메인 경계들이 그저 "가상 모델"로 모사될 수 있는 게 아니다. 종단간 보안(End–to–End–Security)이 중요한 측면이 된다. 보안아키텍처의 구현에 매우 긍정적인 기여를 할 수 있는 것이 복구기능의 범위 안에 있는 "가상 인스턴스"다. 보안 사고가 일어난 다음 물리적 환경의 복구에 없어서는 안 될 정보들도 모두 거기에 들어 있어야 하기 때문이다.

7.4.6 예방과 대응

예방과 대응은 똑같이 불가피하다 : 더 이상 작업의 필요성이 없게 마무리된 인더스트리 4.0 보안 솔루션이란 존재할 수 없다.

공격자들의 노–하우와 장비들이 갈수록 증가하는 추세다. 그에 따라 공격 벡터도 지속적으로 변화하기에 효과적인 대응조치를 효과적으로 계속 개발하는 일이 필요하다.

예방적인 보호조치들 외에 대응 메커니즘들 역시 절대적으로 필요하다 [예컨대, 모니터링과 이벤트 처리(Event Handling) 및 돌발 상황 관리(Incident Management)]. 규칙에 기반한 평가를 포함하는 보안–메시지를 위한 표준화된 언어(semantic)로 적극적인 대응 관리를 위한 전제조건들이 마련된다. 365일 24시간 체제의 보안운영센터(SOC: Security Operation Center)에 활동들을 모아 놓으면 목표로 삼은 파악, 분석 및 보안 관련 모든 측면에 대한 평가를 위한 업무체제가 정비된다.

보안은 "일회성 주제"가 아니다 : 보안이란 것이 단 한 번의 액션으로 달성되는 게 아니다. 위협의 상황은 잠재적 공격자를 위한 새로운 기술적 가능성이 생김에 따라 혹은 표준화 재품과 제품 구성요소들의 취약점이 발견되고 공개되면서 끊임없이 변화한다. 제조사들과 운영자들은 이에 대해 패치와 업데이트로 대응할 수 있어야 한다. 새로운 보안-버전 장착을 위한 가능성들을 확인하고 절차에 따라 계획해야 한다. 보안을 위한 비용은 제조사들에게나 운영자에게나 사소한 문제가 아니기 때문에 관련된 모든 프로세스에서 오버-엔지니어링(Over-Engineering)은 철저하게 피해야 한다.

검토의 목적은 언제나 전체를 망라하는 보안-아키텍처의 실현하는 것이다. 이때 고려해야 하는 것이 사용환경의 전체 아키텍처와 표준화, 개발, 생산 및 관리 영역의 모든 프로세스들이다.

보안은 중요 사안에서 프로세스 문제(process issues)이고 앞으로도 그럴 것이다. 아울러 단 하나의 보안-칩으로 보장되지 못한다.

생산 환경의 특별한 경계조건들을 고려하여 IT-구조들을 고쳐나가는 일은 계속적으로 추진해야 한다.

7.4.7 인식(awareness), 직업훈련, 사원교육

핵심적인 작용을 하는 것이 조직 차원의 조치들이다. 보안-조치와 그 필요성에 대한 의식의 강화를 위한 관계 인력의 인식-교육은 관계된 모든 조직(제조자, 시설 제작-구축자, 운영자)에서 이루어져야 한다. 그럼으로써 이 조치들에 대한 이해가 쉬어지고 실현한 대책의 질이 향상된다.

보안 관리 기능과 프로세스(키-관리Key Management, 회계기능, 이벤트 처리)를 위해서는 인프라 구조와 해당 교육을 받은 인력이 있어야 한다. 사용자-가이드라인은 제품과 솔루션 제조자 쪽에서 마련하는데 이 프로세스에 통합되어야 한다. 여기에 속하는 것으로 예컨대 암호관리, 데이터와 데이터 (저장)매체(data media), 정기적인 데이터 백업 등이 있다.

7.4.8 운 용

산업 보안 기능의 이용은 포괄적인 사전지식 없이도 가능해야 한다. 특히 유지보수와 다른 서비스들에서 장애가 있을 때 그 장애의 제거와 관련해서도 마찬가지다. 보안-솔루션에서는 특히 Plug&Operate를 추구해야 한다.

7.4.9 표준과 사양

인더스트리 4.0에 있어서 산업 보안은 현재 협회들이며 표준화위원회에서 논의의 대상이 되고 있다.

국제 표준 IEC 62443 "산업 제어체계와 네트워크 및 시스템의 보호를 위한 IT-보안"은 4종류의 보안 기준을 바탕으로 한 산업 보안 평가 척도를 갖춘 뼈대가 되고 있다. 산업 자동화 체계에 대한 7가지 근본 요구사항(Foundational Requirements, FR)이 시스템 요구사항(SR)과 개선요구(Requirement Enhancements, RE) 안에서 상세히 설명된다. 보안 수준(SL 1.4)의 기반은 SR, RE로 구성된 하나의 세트다.

어느 시스템에 통합될 때 요구되는 보안 수준에 상응하는 구성요소들의 보안 역량이 고려되어야 한다. 동시에 프로세스는 요구되는 보안 수준에 도달할 수 있도록 구성해야 한다.

IEC 62443이 장래에 인증서 부여를 위해 사용될 것으로 기대된다.

VDI-지침 2182에서 알려진 산업 자동화의 정보보안을 위한 절차모델(procedure model)은 구성요소 제조자, 기계제작자, 운영자 등의 활동들이 맞물리도록 한다. 운영자는 위험분석의 범위 안에서 잠재적으로 취약한 위치들을 찾아 확인하고 평가한다. 제조자는 통합자/기계제작자 및 운영자를 위해 꼭 필요한 정보들(특히 중요한 네트워크 특성들)을 보안 개념 및 솔루션 작성을 위해 표준에 입각하여 제시하여 사용하게 해야 한다. 이 지침은 IEC 62443에 편입되었다.

보안 프로세스를 확립하고 실현할 수 있는 조직의 역량은 적절한 기준에 의해 판정할 필요가 있다.
인더스트리 4.0-가치창출 네트워크에서 동적 구성에 대

한 요구는 규제와 표준을 담은, 유효한 지침들과 서로 독립적인 관계에 있어서, 변화가 생길 경우 인증/운영허가를 상실하게 된다. 따라서 이 동적 특성을 고려한 규칙이 요구된다. 그 전제는 부작용 없는 보안메커니즘으로 모든 참여자들의 철저한 자체 보안이다.

7.5 모범적인 IT 보안조치

이 장에서 소개되는 모범적인 조치들은 IT, 전문 부서 및 보안-역량-센터와 같은 중앙 부서들이 기업의 IT-보안 개선을 위해 어떤 방향으로 효과적인 조치들을 개발하여 실현시킬 수 있는지 선정된 술루션-원칙들을 소개하는 "만능 공구 상자"(generic toolbox)로 이해될 수 있다. 여기서 특히 상세하게 설명되는 원칙들은 미래에 있어 그 중요성이 이미 오늘의 시각에서도 개연성이 높을 것으로 생각되지만, 그 반면에 오늘날 그것을 확산시켜 실현하기는 취약한 모습을 보이는 것들이다. 이로써 그 자세한 설명은 인더스트리 4.0을 위해 수행해야 할 산업 보안의 변신과 관련한 현재의 토론을 가려 정리한 초록의 모습을 보이며, 완성된 조치목록을 제공하는 것은 아니다. 대량생산 역량을 갖추기 위한 차원에서 계속적인 개발을 하기 위해서는 무엇보다 더욱 더 근본적이고 상세한 사항들이 요구된다.

7.5.1 보안-아키텍처

인더스트리 4.0을 위한 보안 개념에서 고려해야 할 아키텍처 차원의 조치들이 몇 가지 있다(Security by Design).

오늘날 생산에서의 직능 분장("segregation of duties" / "separation of duties")은 대부분 관리자 권한과 이용자 권한 사이에서만 이루어지는 게 보통이다. 통상 구성요소는 완전한 권한을 다 가진 관리자의 액세스[슈퍼유저(Super-User)]를 통해 가동되는데, 흔히 생산영역을 초월한 권한을 보유한 경우도 적지 않다. 그것은 이제까지 생산에 있어서의 초점이 보호의 목표인 데이터의 가용성과 완전성에 두고, 기밀성과 진정성에는 그다지 초점을 두지 않았다는 사실에 기인한다. 그러던 것이 인더스트리 4.0과 함께 달라지게 되고, 달라 질 수밖에 없는데, 그 이유는 인터넷과 연결되어 있으면서 보호되지 않는 구성요소에 대한 성공적인 사이버 공격의 개연성이 아주 높기 때문이다. 더 나아가 그 구성요소가 완전한 관리 권한을 지니고 자체 도메인의 경계를 넘어서까지 운영되는 경우 그 파급 효과들 역시 그만큼 더 커진다. 신뢰성과 진위성이라는 보호 목표들이 소홀히 다루어지는 한 이는 단기, 중기, 장기적으로 (예컨대 인터넷을 통한 사이버 공격을 통해) 데이터의 가용성과 완전성에 대해서까지 영향을 미칠 수 있다. 이 예에서 알 수 있듯이 예컨대 모듈, 기계, 전체 생산시설로부터 가치창출 네트워크에 이르기까지 몇 가지 서로 분리된 영역으로 시스템 디자인을 분할하는 것이 아키텍처의 불가피한 조치이다. 여기서 이 분할은 논리적 및/또는 물리적 성격일 수 있는데, 저장 또는 복사(전송) 형식의 정보-자산의 존재와 관련될 수 있거나 액세스와 관련하여 분할된 도메인과 관련된 수도 있다. 후자의 경우 도메인 경계에서 진정성을 위한 것으로 귀결된다. 이 분할은 다시금 동일한 모듈에서 수직적일 수도 있고 (관리자 로그인 대 이용자 로그인) 아니면 수평적일 수도 있다(여러 가지 모듈에 대하여 관리자 이용 계정과 이용자 이용 계정의 분리). 여기서 의미하는 것은 분석 후의 조치로서 올바른 자리에 이루어져야 할 분리의 경계를 특히 보안에 중요한 부분들처럼 알려진 위험 측면들의 구분과 조합하여 디자인에 포함시켜야 한다는 것이다. 아마 실현 가능성이 없을지 모르지만 이런 특성의 최대치에서라면 저마다의 기능이 자체 보안-도메인을 나타내고, 자체 액세스 통제와 권리와 다른 보안-기능들을 사용할 것이다.

이와 긴밀하게 관련되고 보안에서는 이미 자주 정기적으로 주제가 되는 것이 바로 네트워크 분할이다. 그러나 인더스트리 4.0-시나리오에서는 (하위)구성요소-층위에서의 점점 더 세분화되기 때문에 "내부"와 "외부" 사이 내지는 신뢰도가 서로 다른 네트워크 영역들이나 보호 필요성 정도가 다른 구역 사이에서 명확히 정의된 구분은 약화되는 추세다. 방화벽은 인터넷을 통해 커뮤니케이션해야 하는 수많은 시스템들로 말미암아 구멍이 뚫려 무력화되거나 아니면 너무 복잡해서 수많은 규정들을 개관할 수 있는 사람을 찾아보기 어려운 상황이 된다. 그러나 많은 규정들은 서로 충돌하거나 상쇄되어 버릴 위험까지 내포한다. 정확한 규칙들이라 하더라도 그 수

가 워낙 많이 늘면 진행되는 커뮤니케이션에 대하여 적시에 검토하는 일이 점점 더 어려워진다. 이런 경향은 인더스트리 4.0과 더불어 더욱 더 심화되는데, 자동화의 정도가 확대됨에 따라 시간 간격이 전체적으로 촘촘해지기 때문이다. 그 결과 이제까지의 방화벽 형식의 경계선 보호와 설계상의 보안 조치들은 점점 더 그 효과를 잃고 그에 따라 중요성도 잃는다. 그렇기 때문에 인더스트리 4.0과 함께 달라지는 미래의 전제들을 개별 구성요소들과 작업 흐름의 디자인에서부터 미리 감안하는 일이 중요하다. 그에 대한 조치로 더욱 중요해지는 것이 커뮤니케이션 층위의 분할의 세분화 정도를 근본적으로 높여 조직하는 것이다. 그러면서 방화벽을 통해 형식적으로 작업되는 전형적인 분할을 제대로 정적인 규칙들을 이용해 다음 원칙들을 조합하는 시스템으로 넘어가는 일이다. 규칙들의 관용성을 더 키우고 커뮤니케이션을 위해 통과할 수 없는 분리대를 정해놓은 방화벽 – 여기에서는 이를테면 외부의 상위 통제 센터에서 내부의 분산된 작동기를 제어하기 위한 잠재적 접속 같은 모든 것을 다 막는데, 인더스트리 4.0에서는 결코 허용될 수 없다. 보완 역할을 하는 또 다른 조치 하나는 통신을 위한 규칙들이 모드에 맞춰 허용하거나 금지시키면서 생산 구성요소들의 여러 가지 모드들 사이의 경계를 정하는 것이다. 이에 대한 예로 고전적인 원격유지보수 상황을 들 수 있다. 원격 유지보수가 진행되는 동안에 다른 생산요소들과의 커뮤니케이션은 차단된다. 통신제어를 이처럼 세분화하는 것은 다른 차원들로도 확장시킬 수 있는데, 자세한 것들은 미래의 생산커뮤니케이션-네트워크에 대한 요구사항들에 따라 정해진다.

"심층방어"(Defense-in-Depth)도 아키텍처 조치의 하나에 해당하는데, 이는 한편으로는 적대적 침투나 액세스로부터의 보호가 필요한 생산시설을 고립된 섬처럼 생각하는 습관을 깨고, 다른 한편으로는 각각의 대처 방안마다 필수적인 보호수준에 다다를 수 있다는 가설을 깨고 있. 그보다는 개개의 구성요소(component), 궁극적으로는 개개의 정보-자산이 독자적이고 보호되어야 할 요소로 간주되어야 한다. 이 요소들은 이를테면 인증이나 암호화를 통해 보호하는 게 중요하다. 동시에 고려되어야 하는 것이 다양한 공격자들의 다양한 공격 능력에 대비하는 것이다. 심층방어를 통하여 각각의 공격자 유형을 가능한 조기에 개별적으로 차단조치를 하여 실패하게 하는 것이 중요하다. 따라서 비용 효율적이고 수행 효율적으로 최적의 보호조치를 취하기 위해 여러 층위에서 적절한 대응조치들의 조합을 사용한다. 인프라구조 외에도 전송경로들이며 데이터 전송에 사용되는 프로토콜 등도 여기에 속한다. "심층 방어"는 구성요소들 내에서 처리되고 (사이사이) 저장되는 데이터의 암호화로 시작할 수 있는데, 데이터에 대한 접속의 인증과 승인을 위한 특수한 데이터-전송-프로토콜을 통해 종단간 암호화에 이를 수 있다. 여기서 접속이 사람에 의한 것이냐 아니면 기계에 의한 것이냐는 사소한 문제다. 대응조치들의 어떤 조합으로 전체 보호를 최적화시켜야 하느냐 하는 문제는 개별 분석에서 통일된 전체-전략과 함께 결정되어야 한다.

엄격한 규칙 이행과 함께 동시에 유연성을 유지하는 것이 필수적인 아키텍처 패러다임으로 예상된다. 그것의 의미는 협상의 여지가 없는 "분리대"(crash barrier)가 있게 되어 생산에서 보안 정책으로 엄격하게 관철된다는 것을 뜻한다. 이에 대한 예로 (이용자) 신상 관련 정보들의 포괄적 암호화를 들 수 있다. 이 암호화는 신상정보 보호를 근거로 기업 크기나 지역 등과 무관하게 최소한의 조치로서 언제나 필수불가결하다. 그런데 이 분리대를 통해 정의되는 경기장 내부에서는 다양한 기준들과 관련하여 높은 유연성(위의 보호 목표들에서 "동적 구성가능성" 참조)이 필요하다. 위의 사례에서 이것이 의미하는 바는, 예컨대 지역에 따라 신상관련 데이터들 중에서 어느 것을 수집하고, 저장하며 (어디로) 전송하는 게 허용되고 또 (얼마 동안이나) 저장되어도 되는가와 관련한 다양한 (법적) 규정들을 보여주어야 한다는 것이다. 아울러 조치들의 보호 수준(예컨대 간단한 비밀번호에 대해 중복인자-인증을 통해 공격에 대한 저항력의 고양은 물론이고 수행 품질의 향상까지)은 물론이고 보호-조치들에 대한 시간적 요구사항들과 아울러 커다란 영역에서 적용 사례에 따른 다른 여러 가지 추가 보안 특징들도 변동하리란 점도 역시 기대할 수 있다. 추가적으로 자율시스템(중간수준을 위한 자율적이고 시뮬레이션 베이스 시스템)과 나중의 (기대하는 계약의) 변경들로 이벤

트와 커뮤니케이션의 예견할 수 없는 변동은 없을 것이다. 이런 방식의 역동성(dynamic)은 오늘날 생산현장에서 흔히 보이며 그로 인해 특히 보안-조치들이 새로운 도전에 봉착하였다. 유연한 보안을 안전하게 실현시킬 수 있는 것으로 생각 가능한 길이라면 본래의 생산 통신과 독립적인, 실행 중에 보안 관련 중요한 재구성이 가능한 보안-관리-네트워크다. 그와 같은 방식들에 대한 상업적 평가를 위해서는 평가된 위험에 비용을 대입할 수 있도록 해당 위험에 대한 분석이 필요하다.

마찬가지로 엄격한 규칙의 이행을 (재구성 가능한) 소프트웨어 알고리즘의 동적(動的) 설정을 통해서가 아니라 정적(靜的) 설정 내지 하드웨어를 통해 실현할 수 있다.

7.5.2 아이디 관리

어느 이용자가 어느 시점에 어느 기계에 액세스하고 또 액세스할 자격이 있는지 알고 있을 때에만 자격이 없는 액세스들을 효과적으로 확인하여 막아낼 수 있다. 여기서 아이디관리로 이어진다.

사람과 기술적 독립체를 위한 전자 아이디의 전면적인 도입은 그 바탕에 구축되는 인증 및 승인 절차와 맞물려 위에서 요구되었던 기능들의 분할 내지 그에 대한 액세스 및 강제접근제어(MAC: Mandatory Access Control)와 최소 사용 권한(Least Privilege)과 같은 보안-원칙들을 구현한다. 액세스할 때마다 인증과 승인이 이루어져야 하고 적용 사례가 요구하는 최소한의 권한으로 이행된다.

인더스트리 4.0의 자동화 및 자율화가 진행됨에 따라 여기서 설명된 조치들이 시스템, 기계, 시설 등에도 도입되어야 하며, 다른 구성요소들을 제어하는 작용이 있는 것에서는 특히 그렇다.

이와 같은 일관된 액세스에 대한 인증을 받기 위한 전제조건은 생산네트워크 전반에 걸쳐 관찰 대상의 프로세스 안에서 인가를 받은, 리소스 액세스 권한을 가진 사람들과 기계들 전체 목록의 존재는 물론이고 필요한 활동을 나타내는 세분화된 역할과 권한들의 모델링이다. 결국은 현재 적용되는 접속규정을 확정하는 하나의 정책이 시스템 전체에 걸쳐 사용 가능하고 완전해야 한다. 이런 사정이 다름 아닌 국제적 기반의 다국적 대기업들에게 진정한 도전거리가 되는데, 프로세스, 역할, 권한, 아이디 등의 양이 단 한 곳에 자리 잡고 관리할 수 있기에는 너무 많기 때문이다. 세계적으로 분산된 소재지들이며 이 목록에 대한 액세스로 중앙집중식 솔루션이 불가능해 보인다. 기업 전체에 걸쳐 중복 없는 아이디를 부여할 수 있으려면 예컨대 새로 지정되어야 할 아이디가 기업 내에 존재하는지 체크할 수 있고 또 이어서 새로운, 분명한 식별자를 수여할 수 있도록 기업 내에서 사용되는 모든 아이디들에 액세스할 수 있어야 한다. 여기서 분산된 데이터뱅크가 여러 개의 아이디를 관리하게 하는 것을 충분히 생각해볼 수 있다. 이 분산 형에서는 새 아이디를 부여하고 기존 아이디를 관리할 때 해당 아이디가 이미 존재하는지 내지는 어느 곳에서 관리가 이루어져야 하는지 기존하는 데이터뱅크 전체를 다 체크할 수 있도록 보장되어야 한다. 이 분산형은 부하 균형과 오류 해결 메커니즘이 있는 고가용성 아키텍처를 전제로 한다. 그럼으로써 사용된 데이터뱅크 전체를 언제든지 이용할 수 있게 보장된다. 이때 유지보수 작업을 위한 시간의 창(time-window)도 고려하여 자체 기업 내에서 예컨대 사내 신분증과 자격증을 발행하고, 검증하고 취소할 수 있도록 아이디를 안전하게 관리해야 한다. 여기 설명된 과제들은 비슷한 방식으로 거론된 다른 데이터들에도 마찬가지로 적용된다. 따라서 이를테면 필수적인 역할이며 권한들을 지역적으로 다르게 조직하면서 그럼에도 중앙집중식 통제와 기록이 가능해진다. 시스템과 그 구송요소들을 위한 아이디 수가 곧 사람들의 아이디 수보다 훨씬 많아지리란 것도 예상할 수 있다.

예컨대 사내 신분증은 기업 내 사람의 아이디를 기록하여 신분증의 성격에 따라 출입 장소와 건물 및 소프트웨어 액세스 등을 제어할 수 있다. 사내 신분증을 발행할 때 사람의 아이디는 법정 서류들(신분증, 여권 등)을 통해 인증되고 사내 신분증 번호는 기업 전체에서 중첩되는 일이 없도록 부여되는 사람의 아이디와 맞물린다. 분리된 승인절차를 통해 출입권한과 액세스 권한이 부여될 수 있고, 사내 신분증의 성격에 따라 그에 상응한 권한

인증이 칩에 저장될 수 있다. 자격증의 유효기간은 원칙적으로 제한되어 무엇보다 정기적인 검증(자격증 갱신)도 강제된다. 아이디와 연계된 권한들을 이용해 예컨대 고용관계의 종료 시 각각의 아이디에 부여된 권한들을 박탈할 수도 있다. 사내-신분증을 잃어버렸을 때 해당 사내 신분증에 대해 권한들을 박탈하거나 그 신분증을 완전히 차단하는 것도 마찬가지로 가능하다. 이런 절차는 각 기업 내에서 신분증의 교부, 검토, 박탈에 이용되는 중앙 플랫폼을 통해 이루어진다.

시스템 디자인에서 복수의 이용자에 대하여 중요한 권한(최소 권한, 업무 분장)을 분리·분할시킴으로써 외부 공격자의 공격시도를 한층 더 어렵게 만들 수 있는데, 이 분리와 분할은 (암호화된) 정보들을 통해 이루어질 수 있다.

7.5.3 암호 작성법 – 기밀성 보호

저장장치에 저장된 기밀 정보 대부분은 권한 없이 그 정보에 대해 알려고 노리는 관심 대상이라는 사실에서 출발해야만 한다. 권한이 없는 제3자가 이 정보에 접속하더라도 예컨대 일관되고 충분한 정도의 암호화를 함으로써 정보의 활용 자체를 확실히 어렵게 만들 수 있다. 훌륭한 암호화 알고리즘은 권한 없는 암호해독(열쇠 없이)에 필요한 비용을 키움으로써 정보의 신뢰도 보호를 강화시킨다. 데이터 전송은 여러 곳을 거쳐 이루어질 때가 많다. 개별 전송의 경우 암호화되어 이루어진다 하더라도 중간 저장의 경우 보통의 언어로 이루어질 경우 자격이 없는 제3자에 의한 데이터 도난이나 데이터 조작의 위험이 있다. 종단간 암호화는 승인 받지 않은 접속이나 데이터 절도(secure-the-weakest-link)가 이루어진 경우에도 데이터 조작과 활용을 어렵게 만들지만, 데이터 도난 자체를 막지는 못한다.

데이터는 예컨대 비대칭 암호화 기술로 발신자가 수신자의 공개 열쇠를 가지고 암호화하고 추가로 암호화하여 전송하고 암호화하여 저장한다. 비대칭 내지 대칭 암호화기술의 사용 방식은 사용 특징들을 고려한 개념들을 통해 정해진다. 이에 대한 예로 생산기계에서 교환 가능한 제조자-배합공식들을 사용하는 경우를 들 수 있다. 여기서 이용자에 대하여 인더스트리 4.0에서 점차 가치를 부여하거나 비용 의무가 있는 배합방식의 공개를 저지하기 위해서 제조사는 암호화된 전송을 사용자에게 보내고 다시 기계에 적용되도록 한다. 사용자는 기계에 대해 전형적으로 관리권한을 갖기 때문에 기계에 배합공식을 저장하는 것 역시 마찬가지로 암호화하여 적용시켜야 한다(아니면 제조사에 의해 그리고 제조사가 서명한 코드로 읽을 수 있는 저장영역에서 사용할 수 있다). 배합공식 기반에서 프로그램의 진행이 암호화될 수 있는지 또 될 수 있다면 어떤 방법으로 가능한지의 물음과 관련하여 사용자나 외부 공격자에 의한 런타임-분석 같은 위험들은 더 많은 비용을 들여 그에 대해 보호하는 것이 정당한지 평가되어야만 한다. 대칭 암호화 기법을 사용할 경우 지역의 개인적 열쇠를 위한 안전도 적절한 저장장치와 적절한 인프라 구조가 필요한데, 여기에는 곧바로 특수한 하드웨어-보안-요소가 필요해진다. 추가로 또는 대안적으로 어느 공격의 파급효과는 기계-각각의 열쇠를 사용하여 제한시킬 수 있다. 그럴 경우 라이센스-매니지먼트의 의미에서 각 기계에 배합공식을 사용하는 것의 제한도 가능해진다.

7.5.4 암호화 기술 – 데이터의 완전성 보호

암호화 기술은 적절한 형식의 검증-값이 서명과 함께 쓰이면 데이터 완전성 보호에 탁월하게 쓰일 수 있다.

인더스트리 4.0에서 암호화 기술은 보안 조치로서 완전성과 진위성을 효과적으로 보호한다. 그에 대한 예로는 시스템별 소프트웨어(내장된 운영체계)가 있다. 안전한 시작 프로세스로만 내장 시스템을 디자인하는 것을 전면적으로 추구할 만하다. 이를 위해 현장에서 변경 불가능한(기록이 가능하지 않은 저장장치, TPM 또는 그 비슷한) 최초의 소프트웨어-부분에서부터 그 다음에 있는 소프트웨어가 시작하기 전에 그 코드의 완전성을 해시와 서명으로 검증한다. 필요한 경우 여러 단계에 걸쳐 수행할 수 있고 운용에서 신뢰할 만한 부호-식(Code-Basis)으로 이어진다. 하드웨어-모호-모듈은 높은 신뢰도를 위해 공격 저항력에 쓰면 의미가 크다. 인더스트리 4.0에는 이 조치들이 전면적으로, 특히 비교적 높은 비용이 요구되는(예컨대 간단한 센서들) 곳에 실현될 수 있는지 해명하는 것이 중요하다.

위에서 언급한 배합공식의 예로는 계산 시간에 대한 요구가 작을 경우(통상의 대칭 절차들은 비대칭에 비해 강도가 비슷할 경우 계산이 더 빠르다.) 또는 적절히 안전성 높은 저장장소가 지역에서 쓸 수 없을 때(대칭 절차의 경우 비밀 열쇠가 필수) 그리고 신뢰도에 비해 배합공식의 진위성이 더 전면에 부각될 때 비대칭 암호화기술이 쓰이는 경우를 들 수 있다. 공개적이기 때문에 보관소로 안전한 저장영역이 요구되지 않는 제조사의 경우 진위성 통제에는 그 공개된 열쇠로 충분하다.

개별적으로 사용된 암호화 절차와 암호화 알고리즘은 다음 여러 가지 기준들에 따라 정해진다. 즉 요구되는 보호 기간, 사용 가능한 리소스(계산수행), 암호 보관을 위한 로컬 비밀저장장치 대 중앙 인프라구조(Public-Key-Infrastructure)의 사용 및 도입 가능성, 온라인-연결(중앙 관리, Revocation)의 사용 가능성, 알려진 공격들 등이 그것이다.

암호화 기술은 전체로서의 보호 업무를 쉽게 만들기는 하지만, 그 대신에 열쇠 데이터를 다루는 데 조심해야 한다. 열쇠를 잃어버릴 경우 데이터 상실 위험이 있고, 열쇠가 엉뚱한 사람 수중에 들어가면 암호화된 데이터에 들키지 않고 액세스하리란 생각도 충분히 가능하다. 그렇지만 암호화 없이 전면적인 보호 대신에 열쇠를 몇개 되지 않는 장소에 집중하여 보호하는 것이 더 간단하다. PKI처럼 자리 잡힌 프로세스를 사용할 수 있다. 전용 하드웨어-구성요소(광범위한 보안-기능들과 여러 공격 방법들에 대해 강력한 보호 기능이 있는 보안-칩)도 마찬가지로 사용할 수 있다. 다만 사용과 위험상황에 맞춘 개념에서라면 암호화기술의 효력이 제대로 발휘될 수 있다.

7.5.5 안전한 원격 액세스와 빈번한 업데이트

인터넷을 통해 원격으로 기계나 로봇의 유지보수를 수행하는 것은 제조회사들에게 관행적인 일이다. 이때 제조사의 기술자는 인터넷을 통해 기업 내 유지보수 되어야 할 기계에 직접 액세스하여 펌웨어-업데이트를 하거나 성능 개선을 위한 설정을 실시한다. 여러 기업들의 (경우에 따라 공통으로 이용되는 플랫폼을 통한) 협력 과정에서는 여러 이용자들에 대한 정확한 인증절차라는 커다란 문제가 도사리고 있다. 자체 기업의 직원들은 인사시스템을 통해 보통 명확히 확인할 수 있지만, 협력 기업들의 직원이나, 고객 또는 제조사 등은 그렇지 못하기 때문이다. 참여한 기업들 저마다 자체 아이디—관리가 있기는 하지만, 그럼에도 협력사들 사이에는 기술 차원에서 확립된 신뢰관계가 없는 게 보통이다.

이러한 기밀 관리는 이른바 연합 아이디 관리(FIM)로 해결될 수 있다. 여기서 참여한 기업들 전체가 신뢰하는 (신뢰할 수밖에 없는) 외부의 아이디—브로커는 요청하는 아이디가 (그게 사람인지 기계인지 구분하는 것은 중요하지 않다.) 그것으로 제시되는 존재인지 검증 작업을 수행한다. 이 검증은 다음 요인들 중 둘이나 그 이상을 조합하여 사용하는 가운데 중복(멀티)-인자-인증으로 이루어질 수도 있다. 소유(동글, 스마트-카드, 토큰), 지식(패스워드, 키-구문) 및/또는 생체정보(지문, 홍채인식) 등. 인증에 성공한 다음에는 기업 안에서 둘째 단계에서 다음 사항이 검증될 수 있다. 즉 승인된 액세스가 그 아이디에 허용되는지, 허용된다면 어느 액세스가 그런지, 또 바라는 체계에 대한 액세스가 허용되어도 좋은지 등이 그것이다. 늦어도 이 지점에서 전체를 망라하는 표준들이 필요하지 않을 수 없게 된다. 신뢰에 대한 똑같은 물음이 사용되는 컴퓨터 시스템과 관련하여 중요하

다. 이를테면 악성프로그램, 바이러스의 위험 또는 심지어 백도어의 위험이 사용자에 의해 통제되지 않는, 원격 유지보수에 동원된 제조자의 시스템을 통해 초래되지 않도록 확실하게 하기 위해서 예컨대 (사실상) 표준화된 가상화기술이 쓰일 수 있다. 이때 사용자와 제조사는 사용하게 될 이미지를 공동으로 정해서 검증한다. 사용자의 경우 무엇보다 자신의 생산에 대한 위험을 피하는 데 관심이 있지만, VM 인터페이스와 VM 운영환경에서 꼭 필요한 유지보수 툴의 사용가능성이 특히 운영과정에서 제조사에게 중요하기 때문이다. 인더스트리 4.0-혁신과 함께 생산체계에 대한 지속적인 관찰, 관리, 분석 등의 지속적인 서비스를 위해 이 조치가 지속적으로 더욱 개발되어야만 한다. 그에 대한 예로는 생산에서 나오는 운용 데이터 흐름에 대한 제어를 들 수 있다.

잦은 업데이트 내지는 필요성이 발생할 때마다 소프트웨어의 허점을 보완하는 것은 갈수록 소프트웨어에 의존하는 네트워크 시스템에 대한 요구사항이다. 이런 네트워크화된 시스템의 경우 생산현장에서는 예컨대 기업의 안전에 대한 인증의 내용과 충돌한다. 안전에 대한 가능한 대응조치라면 네트워크에 대하여 인증된 시스템들을 보안-게이트웨이를 통해 캡슐화하는 방법이다. 그 기능범위는 매우 다양할 수 있지만, 핵심은 가시성이고 아울러 캡슐화된 시스템에 대한 공격성의 위치를 확인하는 일이다. 점점 더 모듈화가 진행되는 것과 관련하여 보면 이것의 의미는 산업-관련 중요한 프로토콜과 보안기제들의 지원은 점점 더 확산되는 가운데 그와 동시에 게이트웨이는 갈수록 더 소형화될 수밖에 없다는 사실이다. 점점 더 많은 프로토콜과 ISO/OSI(국제 표준화 기구 개방형 시스템)- 레이어에서 평가 오류를 피하면서 동시에 실시간 통신 검사를 할 가능성의 경계를 이전시켜야 할 수밖에 없게 될 것이다. 조합에 쓰일 수 있는 다른 조치들로서 인증에도 불구하고 현장에서의 업데이트를 허용하는 절차들이 요구된다. 그런데 이것은 예컨대 적절한 모듈화를 사용하여 적어도 가시화가 가능하여 공격부위를 인증절차의 핵심과의 연결을 끊고 업데이트를 할 수 있게 한다.

인증 메커니즘은 오직 권한이 있는 사용자 식별번호만이 보호 대상의 데이터에 액세스하는 것을 확실하게 한다. 물론 종전부터 써오던 패스워드나 아니면 소유를 수단으로 단일-요인-인증(single-factor authentication)도 사용자식별번호가 인증되었는지를 검사하지만, 정확히 그 이용자가 이 식별번호를 사용하고 있는 것인지는 검사하지 못한다.

수신자의 개인 키(Key)가 위태롭지 않다는 사실이 확인되는 한에는 원하는 수신자만이 메시지 암호를 해독하여 읽을 수 있다. 키를 깨는 것이 원칙적으로 불가능하지는 않지만, 비용이 비교적 많이 들기 때문에 오늘날의 기술수준에 비추어 보면 전면적으로 시행하지 않고 목표만 골라서 시행할 수 있다.

일관된 암호화를 사용하려면 발신자뿐만 아니라 수신자도 저마다 인증기관의 유효한 키를 보유하고 사용한다는 전제와 또 사용된 인프라구조를 이용한 암호화된 전송 및 암호화된 저장이 기술적으로 가능하다는 전제가 필요하다. 암호화로 인해 높아지는 연산능력과 수행능력-감소의 위험을 견딜만한 최소한으로 제한하기 위한 적절한 프로토콜, 하드웨어, 소프트웨어 등이 그 전제에 속한다.

이것은 기업 내의 프로세스를 위해서뿐만 아니라 생산된 제품 내의 프로세스와 데이터 흐름을 위해서도 적용된다.

7.5.6 프로세스와 조직 차원의 조치들

기업 내에서 정보보안의 위험에 대한 관리는 이상적인 경우 위험 관리체계와 돌발 상황 관리체계를 포함하는 적절하고 포괄적인 보안-관리에 의해 지원된다. 위험-관리의 과제는 존재하는 위험들을 식별, 확인하고 처리하여 그 위험들이 분명하게 드러나도록 만들어 전문 부서와의 협력으로 그리고 준수 사항을 고려하여 이 위험을 디스플레이하는 것을 가능하게 만드는 일이다. 확인된 IT-보안-위험을 다루는 가능성은 원칙적으로 다음 4가지가 있다. 즉 수용(acceptance), 완화(mitigation), 제거 또는 이전(transfer)이 그것이다. IT 보안 위험을 적절히 대처할 수 있으려면 그 위험이 알려져야만 한다. 알려진 위험만이 효과적으로 위치를 확인할 수 있다. 기

업 내에서 참여한 부서들과 영역들이 상호 조정 없이 저마다 자기 관할을 스스로 정하여 개별 주제들 가운데 다루어지지 않거나 아무도 포괄적인 주제에 대한 책임감을 느끼지 못하는 위험에 처하게 되는 일을 피하려면 크로스 오버 기능들에 대해 조직적으로 신경 쓰고 존재하는 관할과 역할을 기업 차원에서 명확히 정하는 것이 중요하다. 아직까지 그렇게 하지 못하고 있다면 이를 위한 전문 보직["최고정보보호책임자"(Chie Information Security Officer) 등]을 마련하는 것이 권장된다. 이들 자리의 업무는 아주 긴밀한 협조와 조정 속에서 IT-보안을 기업 전체의 전체 프로세스로 보는 것이다.

포괄적인 모니터링 개념을 개발하여 실현하는 것이 보통은 위와 같은 중앙 부서들의 최초 행동에 속한다. 여기에 더하여 기존의 모니터링 조치들이 경우에 따라 계속해서 쓰이거나 편입시킬 수 있다. 예컨대 보안에 중요한 중앙체계(키 보관/저장 센터) 액세스 제어에 대한 기록과 평가처럼 보안에 중요한 분야들이면서 신경 쓰지 않던 것들이 많은데, 그러나 적어도 생산과정에서만큼 일상적이지 않기 때문에 새로 마련해야 한다.

그 밖에도 인더스트리 4.0과 함께 불가피하게 필요해진 것은 경우에 따라 기업들 경계와 국경을 넘어서까지 공동 사용되는, 사건과 그에 대한 식별-확인과 기록에 대한 독립적인 평가가 허용되는 플랫폼을 통해 프로세스 차원에서의 협조를 위한 솔루션을 찾아내는 일이다.

조율된 보안-관리가 있어야만 비로소 투명성, 이상탐지 및 기록에 도달하기 위한 조치로서 생산 과정에서 안전도 향상에 긍정적인 영향을 줄 수 있다.

7.5.7 인 식(awareness)

결국에는 전체 직원은 물론이고 경영자와 관리자들까지도 IT-보안과 예컨대 잠재적 데이터 상실이나 데이터 조작이 초래하는 파급효과의 의미에 대해 의식하고 그 결과 IT-안전규정을 이해하여 주의하여 지키는 일이 불가피하다. 이해가 부족하다 보면 심지어 IT-안전조치들마저 의식적으로 회피할 수도 있다. 보안-조치들이 일의 진행을 쉽게 하거나 빠르게 하지 않기 때문이다. 그렇기 때문에 직원 전체에 대한 정기적인 교육과 계속교육이 중요한 조치가 된다.

7.5.8 기업 전체 차원의 보안(cover)

그런데 IT-보안은 설치와 함께 비로소 시작되는 게 아니고 생산 구성요소의 계획과 조달에서 이미 시작된다. 생산을 위해 안전한 IT-환경을 구축할 수 있으려면 계획, 조달, 제작 사이의 긴밀한 협력이 꼭 필요하다. IT-안전규정들은 조달된 제품이 안전과 보안을 기술적으로도 수행할 수 있을 때 비로소 지켜질 수 있다. 조달된 구성요소들에 대한 기술적인 요구사항들을 알기 위해서는 제작, 계획 및 구매부서 사이의 대화가 요구된다. 고객 측으로부터의 구체적인 설명이나 요구가 없다면 제조자로서는 제품에 안전장치를 구현할 필연성이 없을 때가 많다. 경우에 따라 생산비용이 높아지기도 하고 또 성능상 손실이 생기기도 하기 때문이다. 제조자의 적절한 제안이 없을 경우 고객들은 시장에서 일견 양자택일의 상황을 맞은 것처럼 보인다. 이런 악순환의 영향으로 IT 안전규정들이 현재까지 제조자의 제품에 구현되기까지 시간이 오래 걸린다. 따라서 구매지침에 규정되어 있는 제조자의 제품에 대한 최소 요구조건을 정기적으로 수정하여 적응되도록 하여야 한다.

여기 소개된 모범적인 조치들 전부가 기업 내 IT-안전의 단계적인 개선에 기여할 수 있다. 구체적인 경우에 이 조치들 가운데 어느 것을 쓰는 게 의미 있을지는 개별 경우에 맞게 개발되거나 모범사례를 통해 수정-보완하는 게 바람직하고 또 그래야만 한다.

7.6 전망과 요구 사항들

인더스트리 4.0은 정보의 세계를 기업의 경계를 넘어서 사무실에서 센서까지 연결한다. 이 정보세계의 안전은 오늘날 흔히 쓰이는 Office-IT와 자동화 사이의 정보처리와 정보보안에 대한 책임의 분리를 통하여 비로소 확보할 수 있다.

오늘날 Office-IT 영역에 대한 표준화와 규격 통일화는 이미 존재하여 정보보안(ISO 27000-시리즈)에서부터 인프라구조 매니지먼트(ITIL)를 넘어 사업에 중요한 IT 조치들(Cobit)에 이르기까지 제기된 많은 의문점들을 규정한다. 자동화 기술에서 분야들에 따른 권고들[16]이 많이 있지만, "정보의 보안"이란 주제와 관련해서는 아직도 민감화, 위험 인지, 보안조치 실현 등에서 만회할 부분이 많다.

단기적으로 독일어로 된 VDI-지침 2182로 산업 자동화에서 정보 보안을 위한 절차모델이 이용될 수 있다. 이 절차모델에서는 제조자, 통합자, 운영자들이 서로 맞물리는 것이 고려된다.

한편으로는 기업 네트워크는 물론이고 전체 가치창출 네트워크까지, 다른 한편으로는 여러 가지 보호 관련 요구들과 가능성들이 갈수록 모두 융합되어감에 따라 전체 기업 내의 보안-조치들과 서비스 제공자들에 결정적인 의미가 부여된다. 절차모델과 자동화 특성들(ISA-99[17]이 있는 관리-IT 조치들(ISO 27000 시리즈의 형식으로)을 효과적이고 안전하게 연결시킨다는 목적이 현재 사용되고 있는 IEC62443[18]과 연결된다. 인더스트리 4.0에게 필요한 새로운 요구사항들과 조치들은 그에 맞게 표준안에서 처리될 수 있다. 그런 경우에 새로운 규정들을 통하는 것이 나은지 아니면 기존의 표준들을 고치고 보완하여 실현시키는 게 나은지는 인더스트리 4.0의 범위 안에서 다른 표준화 주제들의 맥락 속에서도 평가되어야 한다.

16) 예컨대 ISA99, NIST SP800-82, NERC CIP, CPNI Good Practice Guide 같은 것들(모두 영어로).
17) https://www.isa.org/isa99/ 참조.
18) https://www.dke.de/DE/STD/INDUSTRIE40/Seiten/IEC62443.aspx 참조.

여기서 조화를 이룬다는 것은 Office-IT의 안전관리와 자동화 기술의 안전관리가 접근해야만 한다는 것을 의미한다. 그러기 위해 꼭 "양 쪽" 편 모두가 움직일 필요는 없다.

자동화에는 있는 지침이 Office-IT에는 해당하는 것이 없다는 사실이 예컨대 기계지침 2006/42EG에서 볼 수 있다. 이 지침은 유럽 차원에서 사람과 환경 보호를 위한 규제의 영역을 나타낸다. 운영의 안전과 신뢰도 확보 외에도 인더스트리 4.0에서 동적 가치창출 네트워크 영역에서의 위험성 없는 기능의 확보 역시 업데이트된 기계지침에 있어서 커다란 과제가 되고 있다.

합당한 구성요소들을 사용하여 위험성 없는 기능을 확보하기 위해서는 적절한 통합의 조치들과 검사절차가 요구된다. 정보의 안전에 있어서는 목표로 하는 보안 수준에 도달하여 동적으로 변화해가는 가치창출 네트워크에서도 그 수준을 유지하는 적절한 절차와 메커니즘들을 개발해야 한다.

신뢰할 만한 인증기관과 명확하고 위조 위험이 없는 아이디 체계를 구축하는 것이 가치창출 네트워크를 관통하는 아이디 인프라구조를 위한 전제조건이다. 이 인프라구조는 명확하고 일관된 아이디의 확인과 참여자의 아이디 할당을 보장하고 아이디를 토대로 한 인증과 권한 할당을 지원한다.

보안은 제품 생성 과정의 필수 구성요소가 되어야 한다 (Security by Design).

분야들마다 구체적인 요구사항들과 경계 조건들이 서로 다를 수 있을지 몰라도, 그래도 공통의 방법들과 개념들을 이용해 만들어낼 수 있다. Office-IT와 자동화에서 나오는 노-하우를 함께 통합함으로써 상당한 시너지효과를 얻을 수 있다.

여기에 자동화에서 요구되는 사항들에 대한 Office-IT 쪽에서의 내용 공개와 계속 교육도 자동화에서의 IT-노하우와 특히 보안-노-하우의 업그레딩과 마찬가지로 필수적이다.

안전과 보안 상황이 정적일 리 없다. 위협상황은 끊임없

이 변화하고, 안전(보안)은 따라서 불가피하게 지속적인 과정이요 기껏해야 초기 단계에서만 시간적으로 제한된 프로젝트로 이해되어야 한다. 참여자들 모두는 제품 생성과 운영 시작 단계에서 알려지지 않았던 새로운 안전-요구들을 다룰 수 있어야 한다.

특별한 과제는 중소기업의 수요를 고려한 디자인일 것이다. 제품과 서비스가 이미 표준화된 (기업 프로세스에 간단히 접목시키기 위해 적절한 인프라구조가 갖추어진) 보안 특성을 고려하여 제공될 때에만 부담 가능한 보안 환경이 성립하게 된다. 이 방향으로 나아가는 단계로 생각할 수 있는 것으로, 자동화제품의 통신 및 보안 데이터시트를 통일하고, 보안 사건에 대한 보고를 통일된 언어에 의해 표준화함으로써 중앙에서 데이터의 수집 및 평가를 용이하게 하는 것을 들 수 있다.

새로운 가치창출 네트워크에서는 정보와 네트워크가 핵심적인 자산이 된다. 정보를 공유하거나 제공함으로써 새로운 가능성들이 창출된다. 그러나 동시에 이 정보에 대한 소유권 문제와 참여자들의 역할 및 법적 책임에 대한 문제가 당연히 제기된다. 거래처와 납품업자들로부터 나오는 정보의 분석을 통해 얻어지는 부가가치와 노-하우 유출의 위험성간의 비교형량이 필요하게 된다.

부 록

8. 부 록

8.1 참고문헌

[1] VDI/VDE-Gesellschaft Mess-und Automatisierungstechnik: Statusbericht; Industrie 4.0; Wertschöpfungsketten. Düsseldorf: VDI e.V., April 2014 (측정 및 자동화 기술 현황보고서)

[2] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik: Statusbericht; Industrie 4.0; Gegenstände, Entitäten, Komponenten. Düsseldorf: VDI e.V.,April 2014. (측정 및 자동화 기술 현황보고서)

[3] Acatech Studie, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, Abschlussbericht des Arbeitskreises Industrie 4.0. http://www.bmbf.de/pubRD/Umsetzungsempfehlungen_Industrie4_0.pdf ("미래 프로젝트 인더스트리 4.0의 실현을 위한 권고 사항들" – 작업팀의 결과 보고서)

[4] IEC TR62794: Industrial-process measurement, control and automation - Reference model for representation of production facilities (Digital Factory), 2012

[5] IEC CD 62832 Digital Factory

[6] IEC 61987-10

[7] GMA Definitionen: http://www.iosb.fraunhofer.de/servlet/is/48960/

[8] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile (연방정보기술안전청: 2014년 독일 내 IT-보안의 현황)

[9] www.iosb.fraunhofer.de/?BegriffeI40

[10] https://www.dke.de/de/std/informationssicherheit/documents/nr%20industrie%204.0.pdf

[11] http://docs.oracle.com/javase/7/docs/technotes/guides/jar/jar.html#JAR_Manifest

[12] http://www.plattform-i40.de/sites/default/files/140326_Broschuere_Industrie_0.pdf

8.2 인더스트리 4.0 용어

인더스트리 4.0에서는 나름 생산관련 용어와 ICT(정보·통신·기술) 언어들이 생겨나 발전하였다. 그러나 인더스트리 4.0과 관련한 중요한 용어에 있어서 역사적인 이유에서 비롯된 개념의 차이와 불분명한 점들이 여전히 존재한다. 전문위원회 VDI/VDE-GMA 7.21 "인더스트리 4.0" 내의 작업그룹 "개념"에서는 프라운호퍼 IOSB의 미리암 슐라이펜(Miriam Schleipen)의 통솔 하에 언어와 사상적 구성의 의미에서 인더스트리 4.0의 공통 "기반"(용어)을 만들어 세우는 노력을 경주하였다. 또한 이 작업들은 DKE의 제9 전문에서 이 문제를 담당하는 각 위원회(예컨대 DKE/UK 932.1)와 긴밀한 협력 하에 이루어지고, 플랫폼 인더스르티 4.0의 제2작업팀 "참조 아키텍처"와도 조율을 거쳤다.

목표는 근간이 되는 개념들에 대한 공통적인 이해다! 여기서는 ICT와 생산 영역에서 나온 기존의 규격과 표준을 기초로 하였다.

인더스트리 4.0에서는 상이한 여러 도메인에서 나온 개념과 용어가 유입된다[예컨대, ICT분야에서 나온 서비스 지향환경에서의 서비스들의 조율(Orchestration of services) 같은 표현]. 그러나 관련 도메인들에서 서로 다르게 쓰이는 개념들이 많았다(예컨대 ICT 분야에서 말하는 서비스는 생산과는 다르다). 다른 개념들은 심지어 한 도메인 안에서조차 여러 의미로 쓰이거나 애매하였다(이를테면 요소/구성요소 components). 이러한 언어와 개념적 차이와 불명확한 점들 및 "다른 전공의 개념들"에 대한 설명의 필요성 등이 인더스트리 4.0을 위한 복잡한 기술적 솔루션의 개발과 규격화 과정에서 일종의 장애가 된다.

이 용어정리는, 여러 다른 시각과 요구들을 고려하여 인더스트리 4.0 관련 용어 대한 공통의 기반을 조성하기 위한 것이다. 이는 기업과 업종의 경계를 넘어서는 협동작업을 용이하게 하고, 규격화를 위한 전제조건이 된다.

현재의 개념정의들은 [9]에서 볼 수 있다.

8.3 집필위원

이 「실현 전략」의 작성을 위한 전문적인 노력은 「플랫폼 인더스트리 4.0」의 작업팀에 의하여 이루어졌다. 아래 거명되는 위원들이 이 보고서 상 해당 내용의 집필을 담당하였다.

1–4장 집필위원:

- Wolfgang Dorst (BITKOM e.V.)
- Carsten Glohr (Detecon International GmbH)
- Thomas Hahn (Siemens AG)
- Frank Knafla (Phoenix Contact Electronics GmbH)
- Dr. Ulrich Loewen (Siemens AG)
- Roland Rosen (Siemens AG)
- Thomas Schiemann (T–Systems International GmbH)
- Friedrich Vollmar (IBM Deutschland GmbH)
- Christoph Winterhalter (ABB AG)

5장 집필위원:

- Dr. Bernhard Diegner (ZVEI e.V.)
- Johannes Diemer (Hewlett Packard GmbH)
- Dr. Mathias Dümmler (Infineon Technologies AG)
- Stefan Erker (Huber + Suhner GmbH)
- Dr. Werner Herfs (RWTH Aachen, WZL – Lehrstuhl für Werkzeugmaschinen)
- Claus Hilger (HARTING IT Services GmbH & Co. KG)
- Dr. Lutz Jänicke (Innominate Security Technologies AG)
- Prof. Dr.–Ing. Jürgen Jasperneite (Institut für industrielleInformationstechnik / inIT, Hochschule OWL, Lemgo und Fraunhofer IOSB–INA)
- Johannes Kalhoff (Phoenix Contact GmbH & Co. KG)
- Prof. Dr. Uwe Kubach (SAP AG)
- Dr. Ulrich Löwen (Siemens AG)
- Georg Mattis (Huber + Suhner GmbH)
- Georg Menges (NXP Semiconductors Germany GmbH)
- Frank Mildner (Deutsche Telekom AG)
- Mathias Quetschlich (MAN Truck & Bus AG)
- Ernst–Joachim Steffens (Deutsche Telekom AG)
- Dr. Thomas Stiedl (Robert Bosch GmbH)

6장 집필위원:

- Dr. Peter Adolphs (Pepperl+Fuchs GmbH)
- Dr. Heinz Bedenbender (VDI e.V.)
- Martin Ehlich (Lenze SE)
- Prof. Ulrich Epple (RWTH Aachen)
- Martin Hankel (Bosch Rexroth AG)
- Roland Heidel (Siemens AG)
- Dr. Michael Hoffmeister (Festo AG & Co.KG)
- Haimo Huhle (ZVEI e.V.)
- Bernd Kärcher (Festo AG & Co.KG)
- Dr. Heiko Koziolek (ABB AG)
- Reinhold Pichler (VDE e.V. DKE)
- Stefan Pollmeier (ESR Pollmeier GmbH)
- Frank Schewe (Phoenix Contact Electronics GmbH)
- Thomas Schulz (GE Intelligent Platforms GmbH)
- Dr. Karsten Schweichhart (Deutsche Telekom AG)
- Dr. Armin Walter (Lenze SE)
- Bernd Waser (Murrelektronik GmbH)
- Prof. Dr. Martin Wollschlaeger (TU Dresden)

7장 집필위원:

- Dr. Lutz Jänicke (Innominate Security Technologies)
- Michael Jochem (Bosch Rexroth AG)
- Hartmut Kaiser (Secunet Security Networks AG)
- Marcel Kisch (IBM Deutschland GmbH)
- Dr. Wolfgang Klasen (Siemens AG)
- Jörn Lehmann (VDMA e.V.),
- Lukas Linke (ZVEI e.V.)
- Jens Mehrfeld (BSI)
- Michael Sandner (Volkswagen AG)