Journal of The Korea Society of Computer and Information
Vol. 20, No. 3, March 2015

www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.3.009

자동차 기능안전성을 위한 온톨로지 기반의 위험원 분석 및 위험 평가

노 경 현*, 이 금 석*

An Ontology-Based Hazard Analysis and Risk Assessment for automotive functional safety

Kyung-Hyun Roh*, Keum-Suk Lee*

요 약

본 논문에서는 자동차 기능안전 표준인 ISO 26262에서 요구하는 위험원 분석 및 위험 평가에서 온톨로지와 추론 규칙을 적용하는 방법을 제안한다. 위험원 분석 및 위험 평가는 일반적으로 수작업으로 수행되어 많은 노력이 소요되고 오류가 발생하기 쉬우며 일관성과 정확성이 부족한 문제점이 있다. 이러한 문제를 해결하기 위해서 본 논문에서는 위험원을 온톨로지로 표현하고, 평가를 위한 온톨로지 규칙을 정의하여 자동화하고 일관성 및 정확성 문제를 개선한다. 본 제안 방법을 검증하기 위해서 ESCL(electronic steering column lock) 시스템에 적용하였다. 온톨로지 규칙 적용 결과를 DL(Description Logics) Query를 실행하여 제대로 동작하는지 확인하였으며, 이를 통해 위험 평가 시에 발생할 수 있는 오류를 파악할 수 있었다.

▸ Keywords : ISO 26262, 온톨로지, 자동차 기능 안전성, 위험원 분석 및 위험 평가

Abstract

The ISO 26262 standard requires a preliminary hazard analysis and risk assesment early in the development for automotive system. This is a first step for the development of an automotive system to determine the necessary safety measures to be implemented for a certain function. In this paper, we propose an ontology-based hazard analysis and risk assessment method for automotive functional safety. We use ontology to model the hazard and SWRL(Semantic Web Language) to describe risk analysis. The applicability of the proposed method is evaluated by the case study of an ESCL(electronic steering column lock) system. The result show that ontology deduction is useful for improving consistency and accuracy of hazard analysis and risk assessment.

▸ Keywords : ISO 26262, Ontology, Automotive Functional Safety, Hazard Analysis, Risk Assessment

•제1저자 : 노경현 •교신저자 : 이금석
•투고일 : 2015. 1. 28, 심사일 : 2015. 2. 5, 게재확정일 : 2015. 2. 12.
* 동국대학교 컴퓨터공학과-서울(Dept. of Computer Science and Engineering, Dongguk University-Seoul)

I. 서 론

최근 차량에 장착되는 소프트웨어의 비중이 증가하고 복잡해짐에 따라 소프트웨어의 결함으로 인해 발생할 수 있는 운전자와 탑승자 및 보행자의 안전 문제가 중요해졌다. 이에 따라서 차량의 소프트웨어 및 전기 전자장치의 기능 문제로 생기는 안전 문제를 개선하기 위해 ISO 26262가 제정되었다[1]. ISO 26262는 국제 표준으로 차량에 장착되는 소프트웨어 및 전기전자 장치 개발 절차에서 안전 측면에서 수행되어야 하는 위험 분석, 개발 절차 및 적용 기법에 대해서 요구하고 있다. 기능 안전의 대한 전기/전자 표준인 IEC 61508[2]을 자동차 개발 프로세스에 적합하게 보완하였으며, 3.5 톤 이하의 양산 차량에서 소프트웨어가 탑재된 전기전자 부품의 개발을 대상으로 한다. 유럽, 일본, 미국을 비롯한 해외와 국내 현대기아 자동차, 모비스 등의 자동차 완성차 업체(OEM) 및 부품 협력업체에서는 ISO 26262의 개발 프로세스 및 요구 사항을 개발에 반영하고 있다. 이를 미준수 시에 국내 제품의 경우 해외 수출의 장벽이 될 수 있으므로 자동차 소프트웨어 및 제품 개발 시에 필수적인 규격이 되고 있다.

ISO 26262에서 기능 안전의 위험원 분석 및 위험 평가는 개념 단계에서 수행된다. 위험 등급은 ASIL(Automatic Severity Integrity Level)로 정의되며 ASIL A부터 D까지 4개 등급으로 구성되며, ASIL A가 가장 낮은 등급이며 ASIL D가 가장 높은 등급이다. ASIL이 결정되면 아이템 개발에 필요한 개발 절차와 적용 기술이 해당 등급별로 구성되므로 ASIL 평가가 전체 자동차 기능 안전 시스템에서 중요한 활동이 된다.

ISO 26262에서 요구하는 위험원 분석 및 위험 평가는 위험 상황 분석 및 식별, 위험 사건 분류, ASIL 결정의 단계로 수행된다. 위험 사건 분류는 식별된 위험원에 대해서 심각도, 노출도, 통제도의 수준을 결정하고 각 위험원과 위험 사건에 대해서 ASIL을 결정한다. 이중에서 가장 높은 ASIL이 개발 항목의 위험등급으로 정해진다. 그러나 이러한 분석 및 평가 방법이 ISO 26262 표준에서는 구조화 및 형식화가 부족하여 일반적으로 관련자들이 모여서 엑셀 시트를 이용한 수작업으로 평가한다. 이로 인해 분석의 일관성과 정확성이 부족하며 많은 노력이 소요되며, 분석 관점에 따라서 평가 결과가 달라질 수 있다.

본 논문에서는 이러한 문제를 해결하기 위해서 위험원 분석 및 위험 평가를 온톨로지와 추론 규칙을 정의하여 수행하는 것을 제안한다. 온톨로지 모델링과 추론규칙을 정의하여 위험원 분석의 일관성 및 불일치 여부를 판별하고 위험원 분석 및 위험 평가의 정확성을 높일 수 있다. 또한 위험원 분석 및 위험 평가는 차량 운영 환경 조건과 시스템의 특징, 위험원 시나리오에 대해서 다양하게 파악할수록 정확성이 높아지는 도메인 지식에 의존하는 특징이 있기 때문에 온톨로지를 통해 지식 베이스를 구축하여 위험원 분석을 효율적으로 수행할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 기존 연구들을 살펴보고, 3장에서 온톨로지를 이용한 위험 평가 방법에 대해 설명한다. 4장에서는 본 논문에서 제안한 방법에 대한 실험 및 평가에 대해서 기술하고, 5장에서 결론을 맺는다.

II. 관련 연구

1. 온톨로지 개념

온톨로지는 실제 사물을 형식화하는 "개념의 형식적이고 명확한 명세"[3]이며 개념, 개념간의 관계, 개념의 속성 등으로 표현된다. 형식적 시맨틱 온톨로지는 온톨로지 모델의 일관성을 검증하고 논리 추론을 수행할 수 있는 추론 엔진에 적용된다[4]. 온톨로지 표현은 컴퓨터 응용프로그램 사이의 커뮤니케이션 정보로써 사용되고 사건 데이터의 재사용을 용이하게 할 수 있다[5].

2. 위험원 분석 및 위험 평가

위험원 분석 및 위험 평가는 개발하려는 시스템의 기능을 분석하여 오류가 발생할 수 있는 부분을 식별하고, 이것이 실제 운영 상황에서 영향을 미칠 수 있는 위험 정도를 위험 등급으로 파악한다.

2.1 모델링을 이용한 위험원 분석 및 위험 평가

Mader[6]는 차량의 위험원 분석 및 위험 평가를 위해서 도메인 언어인 EAST-ASL을 사용해서 분석 절차를 모델링하고 오류를 검증하는 방법을 제안하였다. 오류 검증을 위해 모델링 도구에서 사용하는 플러그인을 개발하였다. Beckers[7]는 UML을 사용해 모델링하고 OCL에 규칙을 정의하여 위험 분석을 수행하는 방법을 제안하였다.

2.2 온톨로지를 이용한 위험원 분석 및 평가

위험원 분석 및 위험 평가 방법에 온톨로지를 적용하는 방법도 연구되었는데 Mazouni[8]는 일반적인 위험 평가에 온

톨로지를 활용한 방법을 제안하였다. 그러나 차량의 기능 안전에 대한 위험원 분석 및 위험 평가 방법은 고려되지 않았다. Mehrpouyan[9]는 시스템 환경 및 서브 컴포넌트의 상호작용 시에 발생할 수 있는 위험원을 온톨로지와 SysML을 활용해 식별 및 검증하는 방법을 제안하였다. 그러나 이 방법은 개발 초기 단계가 아닌 설계 단계가 진행되어야 가능하기 때문에 초기 위험원 분석 및 위험 평가 방법으로 적용하기는 한계가 있다.

3. ISO 26262의 위험원 분석 및 위험 평가

그림 1. 자동차 기능 안전성의 위험원 분석 및 위험 평가 절차
Fig. 1. Hazard Analysis and Risk Assessment of Automotive Functional Safety

ISO 26262가 2011년에 국제 표준으로 제정된 이후 실제 적용을 위한 다양한 연구가 수행되었다. Kyung-Hyun는 ISO 26262 프로세스와 CMMI 표준 프로세스와 통합하는 방법[10], ISO 26262 적용을 위한 테스팅 방법[11,12], 오픈 소스 기반의 공학 도구 적용 방법 연구를 수행하였다[13].

ISO 26262에서 요구하는 차량의 위험원 분석 및 위험 평가는 Part 3 Concept Phase에서 정의하고 있으며, 전체 수행 절차는 그림 1과 같다. 아이템 정의 활동에서는 개발하려는 아이템의 기능 요구사항을 도출하는 활동이다. 아이템은 하나 이상의 센서와 콘트롤러, 엑츄에이터로 구성된 시스템의 집합이며 하드웨어와 소프트웨어가 모두 포함된다. 아이템의 기능 정의가 완료된 후에 잠재적으로 아이템의 오동작을 발생시킬 수 있는 기능을 도출하고, 기능 오동작이 실제 차량 시나리오에서 발생할 수 있는 상황 분석 및 위험원을 식별하여 위험 사건을 분류하고 위험 평가를 수행한다. 위험 사건 분류는 각 기능별로 차량 위험 무결성 수준인 ASIL을 결정하기 위해 오동작 기능이 미치는 심각도와 발생 가능성, 운전자의 통제 가능성을 평가하게 된다. 심각도는 운전자를 비롯한 탑승자와 보행자에게 해당 기능의 오류로 인해 미치는 정도이며 발생 가능성은 위험 시나리오가 발생할 수 있는 빈도를 평가하게 된다. 통제 가능성은 해당 위험 시나리오에서 운전자가 위험을 회피할 수 있는 정도이다. 세 가지 구성 요소를 조합하여 ASIL을 결정하게 된다. ASIL이 A 이상인 경우는 위험을 예방할 수 있는 최상위 요구사항인 Safety Goal을 정의한다.

이러한 과정들은 검증 활동을 통해서 위험원 분석 및 위험 평가 활동의 오류가 없는지 확인하도록 되어 있다. Safety Goal은 요구사항 분석이 진행됨에 따라서 기능 안전 요구사항, 기술적 안전 요구사항, 하드웨어 요구사항, 소프트웨어 요구사항으로 상세화된다. ISO 26262 Part 8 지원 프로세스의 요구사항 관리 부분에서는 이러한 요구사항들이 서로 추적성을 갖도록 요구하고 있다. 본 논문에서는 자동차 기능 안전성 분석 및 위험 평가 과정을 온톨로지로 모델링하고 온톨로지 추론을 통해서 일관성을 검증한다. 검증은 위험 분석을 수행한 분석가 외에 제3자가 수행하도록 되어 있으며 본 논문의 제안 방법을 통해서 검증을 자동화하여 효율적으로 수행할 수 있다.

III. 온톨로지를 이용한 위험원 평가

1. 온톨로지 클래스 설계

위험원 온톨로지 설계는 온톨로지 개발 방법론 중에서 Natalya[14]가 제안한 방법론을 적용하였으며 이 방법론은 온톨로지 저작 도구를 활용할 수 있도록 구성되어 있다. 개발 방법론은 온톨로지의 도메인과 범위 결정, 온톨로지의 재사용 여부 결정, 중요한 용어 목록 결정, 클래스와 클래스의 계층 구조 결정, 클래스 속성 결정, 속성의 특징 결정, 인스턴스 생성 단계로 구성된다.

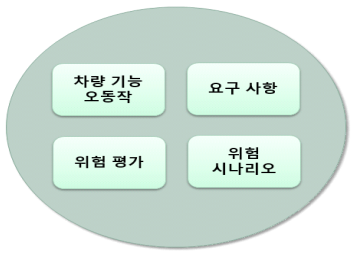

그림 2. 온톨로지 표현 범위
Fig. 2. Ontology representation domain

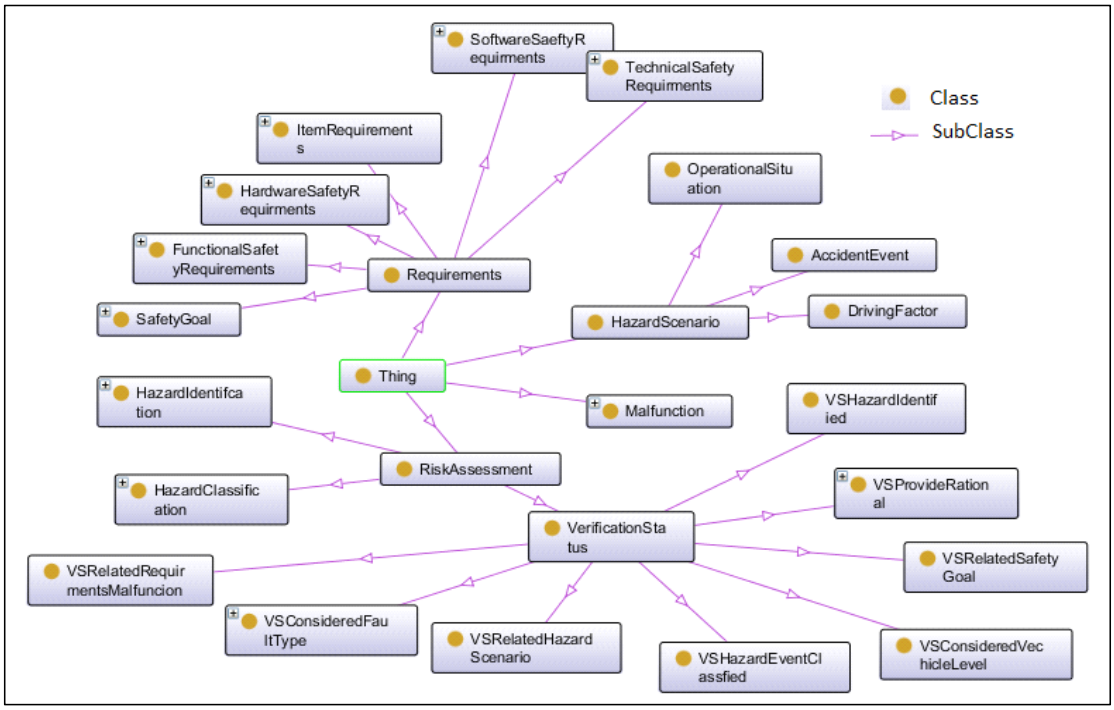

그림 3. 온톨로지 클래스 구성
Fig. 3. Ontology Class architecture

온톨로지 표현 범위는 그림 2와 같이 차량 기능 오동작, 요구사항, 위험 평가, 위험 시나리오를 대상으로 하였다. 전체 클래스는 그림 3과 같이 구성된다. Thing 클래스는 모든 온톨로지 규약에 정의된 최상위 클래스이다. 차량 기능 오동작은 Malfunction 클래스로 표현되며 개발 항목의 요구사항을 바탕으로 하여 오동작을 발생시킬 수 있는 기능을 정의한다. 오동작을 식별할 때 ISO 26262에서 권고하는 위험원 식별 방법인 HAZOP(Hazard and operability)[15]를 참고로 하여 아이템 기능 중에서 No, Unintended, early, late, more, less, intermittent에 해당되는 오동작을 파악하게 된다. 요구사항은 아이템 요구사항 뿐만 아니라 기능 안전 요구사항, 기술적 안전 요구사항, 소프트웨어 요구사항을 표현하여 요구사항들 간의 추적성을 갖도록 온톨로지 관계를 설정한다. 위험 시나리오는 HazardScenario에 구성되며 하위 클래스로 위험원의 심각도와 관련된 사고를 표현하는 AccidentEvent, 위험원의 노출 빈도를 표현하는 OperationalSituation, 위험원에 대해서 운전자의 통제도를 표현하는 DrivingFactor 클래스로 구성된다. 위험 평가는 RiskAssessment 클래스로 표현되며 하위 클래스에 위험원 식별에 해당하는 HazardIdentification, 위험원의 위험 파라미터를 결정하는 HazardClassfication, 위험 평가시 오류 검증을 위한 VerificationStatus로 구성된다. VerificationStatus 하위 클래스에는 검증에 사용하는 규칙의 유형별로 하위 클래스를 정의하였고, 온톨로지 추론 규칙을 정의하여 자동적으로 오류가 검증되도록 하였다.

2. 온톨로지 속성 설계

온톨로지 속성은 클래스의 상태를 표현하는 데이터 속성과 클래스의 연관 관계를 표현하는 객체 속성으로 구분된다. 표1은 속성의 일부분이다. 위험원 분석 및 위험 평가 시에 각 상태를 표현하도록 구성하였다. 이러한 속성들은 온톨로지 추론을 위한 규칙 생성에 사용된다.

표 1. 객체 및 데이터 속성
Table 1. Object and Data Properties

구분	속성명
Object Properties	- hasFuncionalSafetyRequirement - hasHazardClassfication - hasHazardIdentification - hasHazardScenario - HasItemRequirement

	- hasMalfunction - hasSaeftyGoal
Data Properties	- hasASILValue - hasControlRationalValue - hasControlValue - hasExposureRationalValue - hasExposureValue - hasGoalDescValue - hasHazardDescValue - hasHazardEffectVehicleLevelValue - hasMalfunctionDescValue - hasMalfunctionType - hasSeverityRationalValue - hasSeverityValue

3. 온톨로지 관계 제한

온톨로지 추론을 위해서는 클래스 간의 논리 관계를 제한해야 한다. 이 과정은 ASIL 결정을 위한 지식 베이스를 구축하는 단계이다. 사용된 제한의 종류는 온톨로지에 정의된 규약 중에서 Universal 제약과 Existential 제약을 사용하였다.

Universal 제약은 ASIL 결정 시에 단 한가지만의 관계만 사용되는 것이며 심각도 클래스인 AccidentEvent, 노출도 클래스인 Operational Situation, 통제도 클래스인 DrivningFactor에 적용하였다. existential 제약은 적어도 한 가지 이상의 관계 정의에 사용되며 Malfunction이 각각의 파타미터 평가에 적용된다.

4. 온톨로지 추론 설정

온톨로지 추론은 시멘틱 웹의 스택 구조에서 온톨로지 위 단계에 해당하며 LP(Logic Programs)와 FOL(First Oder Logic)로 구분된다. 본 논문에 적용된 추론 규칙 언어인 SWRL(Semantic Web Rule Language)[16]은 LP 일부분인 Horn Logic 정보를 표현할 수 있다. SWRL을 활용하여 ISO 26262에서 요구하는 위험원 분석 및 위험원 평가 등급을 결정하는 규칙을 정의하였다. ASIL을 자동으로 결정하기 위해서 심각도와 발생 빈도, 통제 가능성에 대해서 각 위험 파라미터를 적용해 규칙으로 정의하였다. 또한 분석 과정에서 오류를 검증하기 위한 규칙을 정의하였다. 그림 4는 위험원 평가 규칙의 하나의 예제이다. 예제에서 Hazard Classification은 위험원 분류 클래스이며, 이 클래스의 인스턴스는 변수 ?r에 할당이 된다. 인스턴스 ?r에서 통제 가능성 파라미터를 hasControlValue 값 속성을 통해서 ?c에 할당하고, 심각도 파라미터는 ?s 변수에 할당하며, 노출도 파라미터는 ?e 변수로 가져온다. 이 값이 ISO 26262의 평가 기준에 부합되는지 확인하여 해당 ASIL 결정을 자동으로 수행하게 된다.

```
HazardClassification(?r), hasControlValue(?r, ?c), hasExposureValue(?r, ?e),
hasSeverityValue(?r, ?s), equal(?c, "C3"), equal(?e, "E3"), equal(?s, "S1") ->
hasASILValue(?r, "ASIL A")
```

그림 4. 위험원 평가 규칙 예
Fig. 4. Example of Risk Assessment Rule

IV. 실험 및 평가

1. 온톨로지 구축

온톨로지 모델링은 오픈소스 기반의 온톨로지 모델링 툴인 Protege[17]를 사용해 구축하였다. 추론 엔진은 Pellet[18]을 사용하여 SWRL로 정의된 규칙을 해석하고, 온톨로지 추론을 수행하도록 하였다. 그림 5와 같이 위험원 및 SWRL 규칙을 Protege에서 정의하고 위험원 분석 및 위험 평가 시에 정의된 온톨로지와 온톨로지 규칙이 자동으로 적용된다. 결과는 DL(Description Logics) Query를 통해 사용자가 확인할 수 있다. DL Query는 온톨로지의 클래스와 인스턴스, 서브 클래스 관계 등의 연관 관계를 표현하여 추론 결과를 확인할 수 있는 질의 처리 도구이다. 논리적 수식으로 정보를 표현하고 데이터와 스키마의 서술적 표현에 활용할 수 있다. 실험을 위해 아이템 요구사항과 예상 오동작 기능, 위험원 식별, 위험 시나리오 클래스에 대한 인스턴스를 Protege에서 생성하여 DL Query를 통해서 질의를 입력하여 결과를 확인하였다.

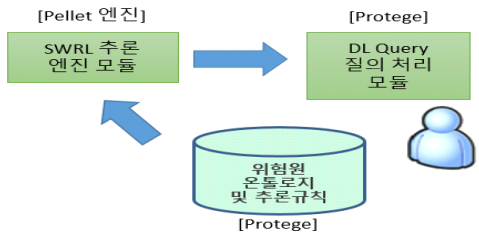

그림 5. 위험원 분석 및 검증 시스템
Fig. 5. Hazard Analysis and Verification System

2. 위험원 분석 및 위험 평가 규칙

실험을 위해서 구축한 온톨로지와 SWRL 규칙을 DL Query를 통해서 제대로 동작하였는지 확인하였다. SWRL 규칙은 위험원 분석 및 위험 평가 절차를 검증하는 검증 규칙과 위험 등급을 결정하는 규칙으로 개발하였으며 표 2에 규칙

을 일부를 기술하였다. 위험 평가 검증 규칙은 위험원 분석 및 위험 평가 수행 과정에서 ISO 26262에서 요구하는 과정이 수행되었는지 확인하는 규칙이며 전체 16가지 규칙을 개발하였다. 1번 규칙의 경우 아이템 정의를 기반으로 오동작 기능을 식별할 때 HAZOP을 참조로 하여 Unintended(의도하지 않는 기능) 상황을 식별하였는지 검증하는 규칙이다. 이러한 식별이 잘 수행되었으면 해당 기능에 대한 인스턴스를 오류 클래스 타입으로 정하고, 그 결과를 DL Query를 통해 추론 결과를 확인할 수 있다. 표 2에서 번호 10에서 12번까지 규칙은 ISO 26262에서 정의된 위험원 평가 규칙을 반영하여 차량 위험원의 무결성 등급인 ASIL을 결정하기 위한 것이다. 위험 등급 결정 규칙은 전체 36개를 정의하였다.

3. 제안 방법 적용 사례

제안 방법의 적용은 차량에 기본적으로 장착되고 있는 전기 전자 장치인 ESCL(electronic steering column lock) 시스템을 대상으로 하였다. 기계식 키를 이용하여 차량 핸들의 잠금과 해제를 하는 것을 ESCL 내부 모터와 전자장치를 통해서 전자식으로 작동시키는 시스템이다. ESCL은 키 대신에 버튼을 사용하여 차량의 도난 방지를 개선하기 위해 잠금 엑센츄어에 잠금과 열림 명령을 자동으로 해주는 기능을 수행한다. 운전자가 차량을 움직이거나 정지하기 위해 차량 시동 버튼을 누르면 이 상태를 감지하여 잠금과 열림 명령에 따라서 엑센추어가 핸들을 움직일 수 있도록 핸들 잠금을 해제하거나 잠그는 기능을 수행한다. 센서와 컨트롤러, 엑센추어로 구성되어 ISO 26262의 아이템 정의와 위험원 분석 및 위험 평가 대상에 부합된다.

표 2. 위험원 온톨로지 SWRL 규칙 예제
Table 2. Example of SWRL Rule of Hazard Ontology

번호	분류	규칙
1	위험 평가 검증	Malfunction(?f), hasMalfunctionType(?f, ?v), equal(?v, "Unintended") -> VSFaultTypeUnintended(?f)
2		Malfunction(?f), hasMalfunctionType(?f, ?v), equal(?v, "No") -> VSFaultTypeNo(?f)
3		ItemRequirements(?r), (hasMalfunction min 1 Malfunction)(?r) -> VSRelatedRequirmentsMalfuncion(?r)
4		HazardClassification(?r), hasControlRationalValue(?r, ?cr), hasControlValue(?r, ?c), equal(?c, "C3") -> VSProvideRationalC3(?r)
5		HazardClassification(?h), (hasSafetyGoal min 1 SafetyGoal)(?h) -> VSRelatedSafetyGoal(?h)
6		HazardClassification(?r), hasSeverityRationalValue(?r, ?sr), hasSeverityValue(?r, ?sv), equal(?sv, "S3") -> VSProvideRationalS3(?r)
7		Malfunction(?f), (hasHazardIdentification min 1 HazardIdentifcation)(?f) -> VSHazardIdentified(?f)
8		HazardClassification(?c), hasControlRationalValue(?c, ?cr), hasControlValue(?c, ?cv), hasExposureRationalValue(?c, ?er), hasExposureValue(?c, ?ev), hasSeverityRationalValue(?c, ?sr), hasSeverityValue(?c, ?sv) -> VSHazardEventClassfied(?c)
9		Malfunction(?f), hasHazardEffectVehicleLevelValue(?f, ?v) -> VSConsideredVechicleLevel(?f)
10	위험 등급 결정	HazardClassification(?r), hasControlValue(?r, ?c), hasExposureValue(?r, ?e), hasSeverityValue(?r, ?s), equal(?c, "C3"), equal(?e, "E3"), equal(?s, "S1") -> hasASILValue(?r, "ASIL A")
11		HazardClassification(?r), hasControlValue(?r, ?c), hasExposureValue(?r, ?e), hasSeverityValue(?r, ?s), equal(?c, "C3"), equal(?e, "E4"), equal(?s, "S3") -> hasASILValue(?r, "ASIL D")
12		HazardClassification(?r), hasControlValue(?r, ?c), hasExposureValue(?r, ?e), hasSeverityValue(?r, ?s), equal(?c, "C3"), equal(?e, "E4"), equal(?s, "S1") -> hasASILValue(?r, "ASIL B")

위험원을 분석하기 위해 먼저 아이템의 요구 기능을 기반으로 하여 오동작을 발생할 수 있는 기능을 식별하였다. 아이템의 기능 요구사항은 "스티어링 컬럼은 운전자가 차량을 움직이지 않기를 원할 때 잠겨야 한다.", "스티어링 컬럼은 운전자가 운전하기 원할 때 잠금해제 되어야 한다." 이다. 여기서 기능 오동작을 도출하기 위해 HAZOP의 결함 유형 식별 키워드를 사용했다. "No"인 경우 ESCL이 기대하지 않은 상황에서 스티어링 컬럼의 잠금을 하지 않는 것이다. "unintended"인 경우 허용되지 않는 상황에서 ESCL이 스티어링 컬럼을 잠그는 것이다. 이러한 영향의 파악은 ESCL 장치 차원이 아닌 차량 시스템 차원에서 검토되어야 한다. 의도하지 않은 잠금인 경우에 ESCL이 스티어링 컬럼을 잠글 때 차량 수준의 영향은 차량을 조향할 수 없는 것이다. 이것을 온톨로지의 인스턴스로 추가하고, 추론 규칙에 반영하여 DL

Query로 확인한 결과는 그림 6과 같다.

그림 6은 ESCL의 아이템 요구사항을 ItemRequirements 클래스의 객체로 선언하고 Malfunction 클래스의 객체로 식별된 오동작을 "No" 유형으로 추가하여 DL Query로 결과를 확인한 것이다. VSConsideredFaultType은 결함 유형의 상위 클래스이고, VerificationStatus의 하위 클래스로 위험원 분석 및 위험 평가의 상태를 확인하는데 사용된다.

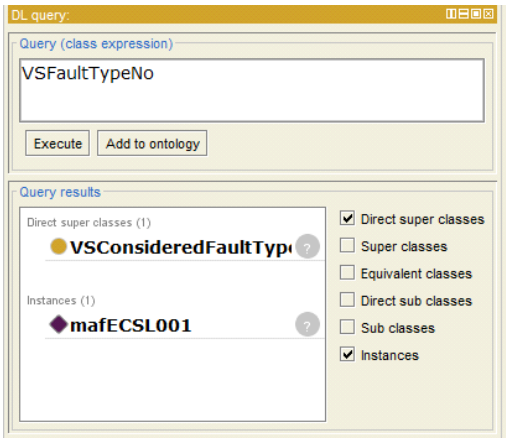

그림 6. 결함 유형 검증 화면
Fig. 6. Verification example of fault type

기능 오동작이 식별된 후에 영향을 미칠 수 있는 위험 시나리오를 파악하여 위험원 평가를 수행한다. ESCL 오동작과 관련된 시나리오는 차량이 정차 또는 주차한 경우, 저속으로 움직이는 경우, 고속으로 움직이는 경우가 되며 이것을 HazardScenario의 하위 클래스인 AccidentEvent, DrivingFactor, OperationalSituation의 인스턴스로 추가하여 시나리오를 구성한다. 구성된 모든 시나리오는 위험원을 식별하고 위험원 분류를 수행한다. 위험원 분류는 위험원의 심각도, 노출도, 통제도를 고려하여 평가한다. 식별된 기능 오동작은 구성된 시나리오와 함께 모두 위험원을 파악하고 결과를 기록한다. 예를 들면 차량이 움직이는 경우에 의도하지 않은 스티어링 컬럼 잠금이 발생하는 경우 차량을 조향할 수 없는 상황이 위험원으로 식별하게 된다. 그림 7은 위험 평가 결과 ASIL D로 평가된 결과를 추론을 통해 확인한 화면이다.

이 경우는 스티어링 컬럼이 의도하지 않게 잠금해제 되지 않은 상황에서 차량이 움직이는 위험 시나리오를 평가한 것이다. 위험 평가 기준은 ISO 26262 Part 3에서 요구하는 방법을 기준으로 하였다. 심각도는 AIS[19] 등급 기준 5~6 10%에 해당하며 운전자에게 심각한 영향을 줄 수 있으므로 가장 높은 심각도 등급인 S3이 된다. 노출도는 운전 상황에서 항상 노출되며 운전 시간의 10% 이상에 해당되기 때문에 E4가 된다. 통제도는 핸들이 고정되어 운전자가 전혀 통제하기 어려운 상황이 되므로 C3가 된다. 이러한 분류 파라미터를 기준으로 ASIL D가 자동으로 추론 규칙에 의해서 계산되고 DL Query에서 조회할 수 있다.

ASIL A 등급 이상의 기능 안전 평가 결과는 안전 목표(Safety Goal)를 설정하고 이것을 기준으로 기능 안전 요구사항과 기술적 안전 요구사항, 하드웨어 안전 요구사항과 소프트웨어 안전 요구사항을 도출해야 한다. 그리고 각 요구사항은 추적성을 갖고 있어야 한다. 본 예제에서 안전 목표는 차량이 이동하는 경우에 스티어링 컬럼의 잠김이 방지되어야 한다는 것이다. 이러한 과정은 검증 단계에서 확인되어야 하며 본 논문에서 제안된 방법을 통해 표 2 온톨로지 추론의 결과 조회가 가능하다.

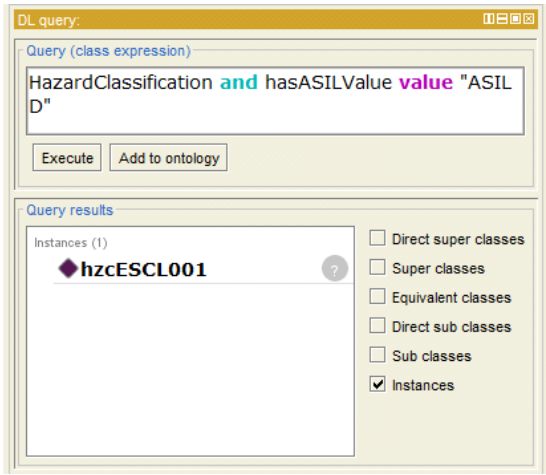

그림 7. 위험 평가 확인 화면
Fig. 7. Example of Risk Assessment

4. 기존 연구 결과 비교

Mader와 Beckers는 위험원 분석 및 위험 평가를 위해서 도메인 언어와 OCL을 이용하는 방법을 제안하였다. 그러나 위험원 분석 및 위험 평가의 결과를 지식 DB로 구축하기 어려운 점이 있다. 위험원 분석 및 위험 평가는 차량 운영 환경 조건과 시스템의 특징, 위험원 시나리오에 대해서 다양하게 파악할수록 정확성이 높아지기 때문에 지식 베이스를 구축하고 재사용할 수 있어야 한다. 본 논문의 제안 방법은 도메인 언어 대신에 온톨로지를 사용하여 온톨로지 추론을 통해 분석

방법의 오류를 검증할 뿐만 아니라 분석 결과를 재사용 및 조회를 용이하게 할 수 있도록 하였다. 또한 분석 방법이 변경될 때마다 별도 플러그인을 개발하지 않고 추론 규칙만 변경하면 바로 적용이 가능하다. 그리고 Beckers는 OCL을 사용하였는데 대신에 온톨로지 추론을 사용하여 추론 규칙의 결과를 DL Query를 통해 바로 확인하여 분석 결과의 파악 및 조회가 더 편리하다. Mehrpouyan는 위험원 온톨로지와 SysML을 사용하는 방법을 제안하였는데 설계 단계가 수행되어야 적용 가능하여 개발 초기 단계인 개념 단계에서는 적용할 수 없는 문제점이 있다. 본 논문의 제안 방법을 통해서 설계 단계뿐만 아니라 개념 단계에서도 위험원 분석 및 위험 평가 수행이 가능하다.

V. 결 론

차량의 위험원 분석 및 위험 평가는 실무에서 대부분 엑셀을 활용한 스프레드시트를 작성해서 수작업으로 수행한다. 그렇기 때문에 분석의 일관성이 떨어지고 수작업으로 인한 정확성의 문제, 위험원에 대한 지식 축적을 위한 지식베이스 구축이 어렵다. 본 논문에서는 이러한 문제점을 보완하기 위해 위험원 분석 및 위험 평가 방법을 온톨로지를 이용해 모델링하고 수행하여 분석 과정의 오류를 온톨로지 추론을 통해 검증하고, 위험 평가를 자동으로 수행하도록 하였다. 제안 방법은 ESCL 시스템에 적용해 ISO 26262에서 요구하는 기능 안전성의 위험원 분석 및 위험 평가에 적합한 것을 확인하였다.

향후 연구 과제는 분석의 편의성을 위해 추론 결과를 쉽게 확인할 수 있는 사용자 인터페이스를 가진 시스템을 개발하는 것이다. 또한 다양한 위험 시나리오에 대해서 추론 규칙을 추가하여 식별할 수 있도록 SWRL 규칙을 확장하는 것이다.

REFERENCES

[1] ISO, ISO 26262 Road vehicles- Functional safety, ISO Std, 2011.

[2] IEC, IEC 61508, Functional safety of electrical/ electronic/ programmable electronic safety-related systems, IEC Std. 2010.

[3] Vladan Devedzić, "Understanding Ontological Engineering", Communications of the ACM - Supporting community and building social capital, Vol. 45, No. 4, pp. 136-144, April 2002.

[4] Jost, H., Kohler, S., Koster, F., "Towards a safer development of driver assistance systems by applying requirements-based methods", 14th International IEEE Conference on Intelligent Transportation Systems, pp. 1144-1149, Washington, USA, Oct. 2011.

[5] Rafael Batres, Shinya Fujiharaa, Yukiyasu Shimadab, Testuo Fuchinoc, "The use of ontologies for enhancing the use of accident", Process Safety and Environmental Protection, Vol. 92, No. 2, pp. 119-130, March 2014.

[6] Mader, R., Griessnig, G., "A Computer-Aided Approach to Preliminary Hazard Analysis for Automotive Embedded Systems", IEEE 18th International Conference and Workshops on Engineering of Computer Based Systems, pp. 169-178, Las Vegas, USA, April 2011.

[7] Beckers K., Paluno, "Structured and Model-Based Hazard Analysis and Risk Assessment Method for Automotive Systems", IEEE 24th International Symposium on Software Reliability Engineering, pp. 238-247, Pasadena, USA, Nov. 2013.

[8] Mazouni M., Aubry J., "A PHA based on a systemic and generic ontology", IEEE International Conference on Service Operations and Logistics and Informatics, pp. 1-6, Philadelphia, USA, Aug. 2007.

[9] Mehrpouyan, H., Bunus P.,, "Model-Based Hazard Analysis of Undesirable Environmental and Components Interaction", IEEE Aerospace Conference, pp. 1-8, Montana, USA, March 2012.

[10] Kyung-Hyun Roh, Keum-Suk Lee, "An effective evaluation of automotive functional safety using ISO 26262 and CMMI Integration Framework", Korean Computer Congress, pp. 514-516, Yeosu, Korea, June 2013.

[11] Kyung-Hyun Roh, Keum-Suk Lee, "A Study on embedded software testing evaluation method using ISO 25000 and ISO 29119", Proceedings

of the 16th Korea Conference on Software Engineering, Vol. 16, No.1, pp. 127-130, Feb. 2014.

〔12〕 Kyung-Hyun Roh, "Software testing method for ISO 26262", Automotive electronics, pp. 90-94, January 2013.

〔13〕 Kyung-Hyun Roh, Mu-Won Lee, "Using Open source software engineering tool for automotive software quality improvement", Proceedings of the 16th Korea Conference on Software Engineering, Vol. 16, No.1, pp. 349-352, Feb. 2014.

〔14〕 Natalya F.,Deborah L., McGuinness, "Ontology Development 101: A Guide to Creating Your First Ontology". Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, March 2001.

〔15〕 IEC, ISO/IEC 61882, Hazard and operability studies, ISO/IEC Std. 2005.

〔16〕 SWRL, *http://www.w3.org/Submission/SWRL*

〔17〕 Protege, *http://protege.stanford.edu*

〔18〕 Pellet, *http://clarkparsia.com/pellet*

〔19〕 Association of the advancement of Automotive medicine, "Abbreviated injury scale 2005", 2005.

저 자 소 개

노 경 현

1996: 동국대학교
식물자원과 농학사
1998: 동국대학교
컴퓨터공학과 공학석사
현 재: 티큐엠에스 컨설팅사업부 이사
관심분야: 소프트웨어 기능 안전
(ISO 26262, IEC 62304)
소프트웨어 테스팅
소프트웨어 품질평가
소프트웨어 프로세스 개선
Email : khroh@dongguk.edu

이 금 석

1971: 서울대학교
응용수학과 공학사
1978: 한국과학원
전자계산학과 이학석사
2001: 건국대학교
컴퓨터정보통신학과 공학박사
현 재: 동국대학교
컴퓨터공학과 교수
관심분야: 운영체제,
소프트웨어 품질평가
Email : kslee@dongguk.edu