복합 실시간 계통의 요구사항 명세와 안전성 분석을 위한 정성적 정형기법

(A Qualitative Formal Method for Requirements Specification and Safety Analysis of Hybrid Real-Time Systems)

이 장 수 † 차 성 덕 ††

(Jang Soo Lee) (Sung Deok Cha)

요 약 산업현장에서 복합 실시간 계통(HRTS: Hybrid Real-Time Systems) 개발을 위한 정형기법 사용의 주된 장벽은 인지적 어려움이며 이는 또 다른 위험을 초래할 수 있다. 이러한 문제를 극복하기 위해 HRTS 요구분석과 안전성 분석 시 사용자의 인지적 부담을 줄여줄 수 있는 정성적 요구분석 체계를 제안한다. 이 체계는 요구사항 명세를 위한 정성적 정형기법(QFM: Qualitative Formal Method)과 인과정보에 의한 요구사항 안전성 분석기법(CRSA: Causal Requirements Safety Analysis)으로 구성되어 있다. QFM에서는 인공지능 분야에서 연구된 정성추론 이론을 정형명세에 도입하여 요구사항 설계자와 분석자의 인지적 부담을 줄일 수 있도록 하였다. CRSA는 QFM에서 도출한 HRTS 동작의 인과 정보에 따라 체계적으로 위험 원인을 추적할 수 있도록 하여, 기존 결함 트리 분석(FTA: Fault Tree Analysis) 기법의 단점인 분석자의 주관에 의존하는 문제를 해결한다. 월성 원자력 발전소 자동정지계통(Shutdown System 2) 소프트웨어 요구사항 명세와 안전성 분석에 QFM과 CRSA를 적용하여 그 실효성을 입증하고자 하였다.

Abstract Major obstruction of using formal methods for hybrid real-time systems in industry is the difficulty that engineers have in understanding and applying the quantitative methods in an abstract requirements phase. While formal methods technology in safety-critical systems can help increase confidence of software, difficulty and complexity in using them can cause another hazard. In order to overcome this obstruction, we propose a framework for qualitative requirements engineering of the hybrid real-time systems. It consists of a qualitative method for requirements specification, called QFM (Qualitative Formal Method), and a safety analysis method for the requirements based on a causality information, called CRSA (Causal Requirements Safety Analysis). QFM emphasizes the idea of a causal and qualitative reasoning in formal methods to reduce the cognitive burden of designers when specifying and validating the software requirements of hybrid safety systems. CRSA can evaluate the logical contribution of the software elements to the physical hazard of systems by utilizing the causality information that is kept during specification by QFM. Using the Shutdown System 2 of Wolsong nuclear power plants as a realistic example, we demonstrate the effectiveness of our approach.

1. 서 론

원자력 발전소 보호계통, 인공위성, 미사일 등에 탑재된 컴퓨터 제어계통과 같이 비선형 연속성을 갖는 제어대상 계통과 이산상태 변화에 의해 실시간으로 상호작용 해야 하는 계통을 복합 실시간 계통 (HRTS: Hybrid Real-Time System) 이라고 하며 그 안전성 보장이 필수적이다. 실제 산업현장에서 HRTS 개발을 위한 정형기법 사용의 주된 장애요인은 기법의 인지적 어려움이다. 개념적이고 정성적인 요구사항 도출단계부터 엄격하고 정량적인 사고를 강요한다. 안전계통 개발

† 종신회원 : 한국원자력연구소 MMIS팀 연구원
jslee@kaeri.re.kr
†† 종신회원 : 한국과학기술원 전산학과 교수
cha@salmosa.kaist.ac.kr
논문접수 : 1998년 12월 24일
심사완료 : 2000년 1월 6일

에 정형기법을 사용하고자 하는 이유는 안전성 제고임에도 불구하고, 사용상의 어려움과 복잡도는 엔지니어의 자유로운 사고를 방해하여 설계 오류로 인한 또 다른 위험을 초래할 수 있다.

정형기법만으로는 원자력 발전소 제어계통과 같은 복잡한 소프트웨어의 물리적 안전성 여부를 증명하는 데는 한계가 있기 때문에 소프트웨어 안전성 분석이 별도로 수행되고 있다. 소프트웨어 안전성 분석은 소프트웨어의 논리적 요소가 계통의 물리적 안전에 어떠한 영향을 미치는가를 분석하는 것이다. 소프트웨어는 기계적 부품에서와 같은 노후화, 충격 등에 의한 고장은 없기 때문에, 하위 부품의 고장으로부터 원인을 추적하는 구조적/확률론적 안전성 분석은 부적절하다. 소프트웨어로 인한 계통의 위험은 소프트웨어 동작의 이상 상태 변화를 추적함으로써 밝혀질 수 있다. 따라서 제어대상 계통, 제어기 소프트웨어, 요구명세 사이의 상태 인과관계를 추적하여 안전성을 분석하는 것이 효과적이다. 그러나 기존의 소프트웨어 안전성 분석 기법들은 제어대상 계통 동작의 물리적 현상에 대한 분석자의 주관적 이해 능력에 의존하기 때문에 분석결과의 객관성이 결여되고 있다.

이러한 문제를 극복하기 위해 복합 실시간 안전계통 요구명세와 안전성 분석 시 사용자의 인지적 부담을 줄여줄 수 있는 정성적 요구분석 체계를 제안하고자 한다. 이 체계는 정성적 정형기법 (QFM: Qualitative Formal Method)과 인과정보에 의한 요구사항 안전성 분석기법 (CRSA: Causal Requirements Safety Analysis)으로 구성되어 있다.

QFM의 특징은 인공지능 분야에서 연구된 정성추론 이론을 HRTS 요구사항 정형명세에 도입한 것이며, 이는 요구명세 작성자와 분석자의 인지적 부담을 줄일 수 있는 장점이 있다. 연속시간과 이산시간 속성을 복합적으로 가지는 HRTS 동작을 물리적으로 단순화하여 표현하기 위해 정성적 정형 언어인 합성명세언어 CML (Compositional Modeling Language) [1]을 사용한다. 또 요구되는 기능 및 안전요건을 인과관계에 따라 목표 기반으로 명세하기 위해 원인결과 기능표현언어 CFRL (Causal Functional Representational Language) [2]을 사용하였다. CML로 표현한 HRTS의 동작특성을 DME (Device Modeling Environment) [3]를 이용해 시뮬레이션함으로써 계통 상태의 원인결과 정보를 도출한다.

CRSA는 고전적인 결함 트리 분석기법(FTA: Fault Tree Analysis)을 소프트웨어 요구분석 단계에 적용한 안전성 분석 기법이다. CRSA는 QFM에서 생산한 인과정보를 사용하여 결함 트리(fault tree)를 작성하기 때문에 이전의 소프트웨어 FTA 기법들이 가지는 분석자의 주관과 계통 이해능력에 의존하는 단점을 보완한다.

이 논문의 구성은 다음과 같다. 2장에서는 먼저 기존 HRTS 정형명세 기법의 문제점을 해결하기 위한 정성적 정형기법(QFM)을 제안하고, QFM의 각 단계를 자동정지계통 예를 사용하여 설명한다. 3장에서는 소프트웨어 안전성 분석을 위한 기존 비 정형적 기법을, QFM으로부터 도출한 인과정보를 활용하여 체계화 한 요구사항 안전성 분석 기법(CRSA)을 제안한다. 마지막으로 4장에서는 결론과 향후 연구방향을 제시한다.

2. 정성적 정형명세 (QFM)

2.1 Hybrid Real-Time System (HRTS) 정형명세

HRTS와 같은 공정제어 계통의 제어기 소프트웨어는 제어대상 계통과 연동되어 동작하기 때문에, 제어기 소프트웨어 동작모델의 요구사항 만족여부만으로는 전체 계통 동작을 검증할 수 없다. 따라서 이를 위한 정형명세 기법은 제어대상 계통(P)과 제어계통(C)의 통합된 동작모델(P∧C)이 요구사항(Sp)을 만족함을 보여야 한다[4]. 즉. 명제 (1)의 만족여부를 입증하여야 한다.

$$P \wedge C \rightarrow Sp \qquad (1)$$

디지털 제어기(C)의 이산 상태변화는 주로 유한상태기계(Finite State Machine: FSM)로 모델링 되어 왔다. 그러나 물리적 법칙에 따라 연속상태변화 동작특성을 가지는 제어대상(P)은 일반적으로 미분방정식에 의해 모델링 된다. HRTS의 요구사항 명세와 검증을 어렵게 하는 요인은 이러한 연속상태와 이산상태변화 사이의 상호 작용이다.

FSM으로 모델링 되는 이산 상태변화 제어기와 연동하면서 통합된 모델이 될 수 있도록 하기 위해, 연속 상태 변화를 FSM에 통합시킨 복합 오토마타 (hybrid automata) 기법들이 제시되고 있다 [5, 6]. 근본적으로 비선형 연속성을 가지는 제어대상을 수학적으로 완전하게 모델링하는 것은 불가능하다. 물리적 현상을 정량적 미분방정식을 이용하여 수학적으로 표현하더라도 엔지니어들이 이를 이해하기 위해서는 정성적/물리적으로 다시 해석해야 한다.

대부분의 엄격한 정형 기법들은 부분적인 검증에서는 효과적이지만 요구사항 도출, 명세단계에서는 인지적 어려움이 발생한다. 즉, 주어진 문제에 대해, 계통 엔지니어와 소프트웨어 엔지니어간의 정성적인 인과 관계 대

화를 통해 요구사항을 도출, 명세할 때, 기법들이 엄격히 정량화 된 논리적 사고를 요구하기 때문에 문제이해를 위한 대화수단으로 부적절하다.

실제 산업현장에서는 HRTS 모델링을 위해 연속 상태변화 제어대상의 동작을 이산 값 샘플링하거나, 이를 이산상태변화 디지털 제어기 동작의 제한조건으로 모델링하는 방법이 사용되고 있다. 예를 들어, 그림 1과 같이 SCR(Software Cost Reduction) 방법의 하나인 사변수(Four-variable) 기법은 캐나다 Darlington 원자력 발전소와 한국의 월성 원자력 발전소 자동정지계통(SDS2)의 요구사항 명세와 검증을 위해 사용되었다.

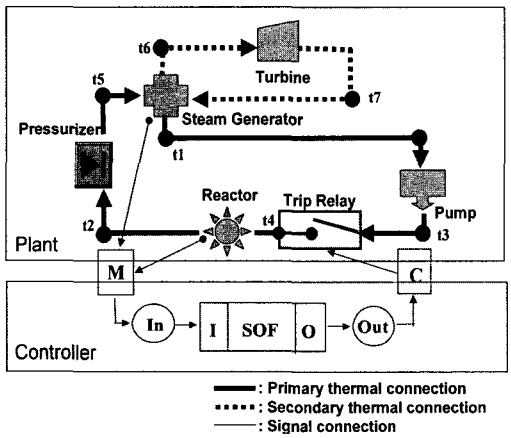


그림 1 월성 원자력 발전소 자동정지계통 (SDS2)

월성과 Darlington 원자력 발전소의 자동정지계통 요구사항을 이러한 사변수 기법에 따라 체계적으로 명세하였지만, 검증을 위해 필요한 명제 (1)의 만족여부 즉, 통합 모델(P∧C)의 요구사항(Sp) 만족여부를 입증하지 못하였다. NAT 관계는 제어대상(P)의 동작을 모델링하는 것이 아니라, 물리적 외부환경에 의한 제어기(P) 동작의 제한조건만을 표현하기 때문에 연속상태변화 제어대상(P)과 이산상태변화 제어기(C) 동작의 상호작용을 파악하기 어렵다.

제안한 QFM과 CRSA기법의 효과를 검증하기 위해 월성 원자력 발전소 자동정지계통을 예제로 사용한다. 월성 원자로 자동정지계통은 크게 제1정지계통(Shutdown System1: SDS1)과 제2정지계통(Shutdown System2: SDS2)으로 구성되어 있다. 이들은 비상운전상태가 감지되면 연쇄 핵반응을 정지시키고 원자로를 안전한 상태로 유지하기 위한 계통이다. SDS2의 5가지 주요 비상운전상태 중 증기발생기 저수위로 인한 SGLL (Steam Generator Low Level) 트립(trip) 현상에 대한 자동정지계통 소프트웨어 요구분석을 위해 QFM과 CRSA를 적용한다.

2.2 정성 추론과 HRTS 요구분석

인공지능 연구의 한 분야인 정성물리 (Qualitative Physics) 이론은 문제를 정성적으로 단순화(approximation)하여 추론하는 방법들을 총칭하며 여러 가지 세부이론, 기법, 도구들이 제시되고 있다[5]. 특히, 정성물리 이론은 HRTS와 같이 물리적 법칙의 지배를 받는 공학 장치의 물리적 특성을 정성적으로 모델링 및 시뮬레이션 하여 그 장치의 동작을 예측, 진단, 추론하기 위해 사용되고 있다.

본 논문에서는 복합 오토마타[6], 시간 오토마타[7] 등 HRTS 요구분석을 위한 기존 정형기법 사용의 어려움을 경감시키기 위해 이를 정성화 시킨 정성 복합 오토마타(Qualitative Hybrid Automata: QHA) 개념을 제안한다. QHA 개념에 근거하여 HRTS 제어대상(P)과 제어기(C) 동작을 표현하고 요구사항(Sp)을 명세하기 위하여 정성물리 이론에서 개발된 언어와 도구를 사용한다. 본 논문에서는 HRTS 요구분석 단계에서의 이와 같은 정형명세 기법을 정성적 정형기법 (Qualitative Formal Method: QFM)이라고 부른다.

정성물리 이론은 HRTS를 위한 기존 정형 기법들 [6, 7]의 정량적인 미분방정식과 시간함수 대신에 정성 미분방정식과 인과관계를 이용하여 정성적으로 모든 물리적 현상을 표현할 수 있게 한다. 이 점을 활용하여 기존 복합 오토마타에서 상태 표현에 사용되는 미분방정식, 정량적 상태변수, 정량적 시간 등 모든 정량적인 요소를 정성화 시킨 QHA는 다음과 같이 정의된다.

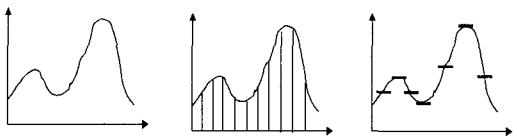
정의1: 정성 복합 오토마타 (QHA)는 <Q, V, C, T>의 네 가지 요소로 표현되며 각각은 다음과 같이 정의된다.

- 상태 값 공간(Quantity Space: Q): 상태변수가 취할 수 있는 정성 값(qmag)의 유한 순서 집합과 이들 값의 변화방향(qdir), 여기서 정성 값을 물리적 주요 상태 변환 점 (landmark)이라고 부른다.
- 변수 (Variables: V): 정성시간에 따라 변하는 정성 상태변수
- 제한조건(Constraint: C): 정성상태 동작을 표현하는 정성 미분방정식
- 상태전이(Transition: T): 정성상태 전이함수(transition-function)

정량적 기법과 정성적 기법을 구분하는 근본 요인은 상태변수 값의 공간(Q)에서 찾을 수 있다. 즉, 정량적

정형기법에서는 상태변수가 실수 값(또는 연속 변수)으로 표현되지만, 정성 기법은 이산화 된 상태변수 값의 공간(Q)을 사용한다. 또, 정성물리의 이산(discrete) 상태 값 공간(Q)은 물리적 의미를 가진 다는 점에서 단순 수학적 이산화와 차이가 있다.

물리적 상태변화를 나타내는 정성 미분방정식에 사용되는 상태변수 값의 공간(Q)은 그림 2의 c와 같이 물리적 주요상태 변환 점(landmark)에 따라 이산(discrete)화 되고, 물리적 주요상태 변환 점과 변환 점 사이의 변수 값을 하나의 값으로 취급함으로써 추상화한다. 즉, 상태변수 값의 크기는 두개의 변환 점들 사이 구간에서는 일정한 것으로 단순화하고, 각 구간 변수 값의 변화 방향으로 증가한다(inc), 평형 상태이다(std), 감소한다(dec) 등을 사용함으로써, 이들 변수들에 의해 표현되는 상태의 진행을 나타낸다. 이러한 물리적 주요상태 변환 점의 눈금은 추상화의 정도에 따라 다양하게 변화시킬 수 있다.



(a)제어대상 동작특성 (b)이산 시스템 모델 (c)QFM정성모델

그림 2 QFM 정성모델과 이산 계통 모델 비교

물리적 법칙의 지배를 받는 HRTS 제어대상(P)은 그림 2의 a와 같이 비선형 연속상태 변화를 한다. 이산 계통 모델링 방법에서는 그림 2의 b와 같이 시간 축을 단순히 수학적으로 나누고 (예를 들어, 1초 단위, 퍼지 값, 확률 값 등), 각 시점에서의 물리적 값을 샘플링 한다. 또한 유한 상태 기계와 같은 이산 상태 그래프는 연속 상태변화가 중요하지 않은 문제에 대한 추상화 방법으로는 매우 유용하다. 그러나 정성물리에서는 물리적 주요상태 변환 점 개념에 따라 기호적으로 물리적 이산화를 추구함으로써, 물리적 법칙이 부여하는 연속성의 특성을 그대로 간직한다는 것이 이산상태 그래프 방식과 다른점이다. 실시간 계통 모델링을 위해, QFM에서 그림 2의 c와 같이 시간 축을 물리적 주요상태 변환 점에 의해 물리적으로 나누어 샘플링하는 것이 수학적 이산 계통 모델링 방법과의 근본적인 차이점이다. 실시간 계통이 갖는 절대시간을 모델링하지 않고 시간적 선후관계, 즉 상태의 인과관계를 모델링 한다.

2.3 Qualitative Formal Method (QFM) 체계

Qualitative Formal Method (QFM)은 인공지능의 정성물리 이론을 이용하여, HRTS의 복잡한 동작을 직접 물리적으로 단순화하는 방법을 제시한다. 정형기법이 인지적 균형을 이루기 위해서는 요구분석 단계에서 사용자가 문제해결을 위해 사용하는 사고방법과 부합하여야 한다. HRTS와 같이 복잡한 물리적 계통 개발을 위해 제어대상 모델(P), 제어기 모델(C), 및 요구사항(Sp)을 도출하고 명세할 때, 계통 전문가와 소프트웨어 전문가가 사용하는 대표적인 사고방법은 정성적 사고와 인과적 사고이다.

정성적 사고와 관련하여, 전문가일수록 HRTS 요구분석 단계와 같은 복잡한 문제해결 초기단계에는 추상적인 문제의 전체그림을 도출한 다음, 보다 구체적인 사항에 초점을 맞춰 문제해결 범위를 좁혀나간다. 또, HRTS 요구사항 명세에서 중요한 것은 제어대상(P)을 정확히 이해하고 모델링 해야 한다는 것이다. 그러나 근본적으로 비선형 연속 상태변화를 하는 물리적 계통인 제어대상(P)은 요구분석단계에서 수학적 정형기법만으로는 모델링이 불가능하다. 물리적 단순화를 위해 정성적 정형 언어인 합성명세언어 CML (Compositional Modeling Language) [1]을 사용하여 연속상태와 이산상태변화가 상호 작용하는 HRTS 동작을 표현한다.

인과적 사고와 관련하여, 요구분석 단계에서 엔지니어들은 요구사항 도출 및 명세를 위해 사용하는 전형적인 사고 유형은 "A 상태이면 B 상태를 발생시켜야 한다." 형태를 취하며, 요구사항 검증단계에서는 "주어진 계통 명세에서, A상태가 B상태를 발생시켰는가?"를 질문하게 된다. 이와 같이 인과적 사고와 일치하는 정형명세 기법 제시를 위해, QFM에서는 정성추론의 한 분야인 인과추론 이론을 도입한다. 요구되는 기능요건과 안전요건을

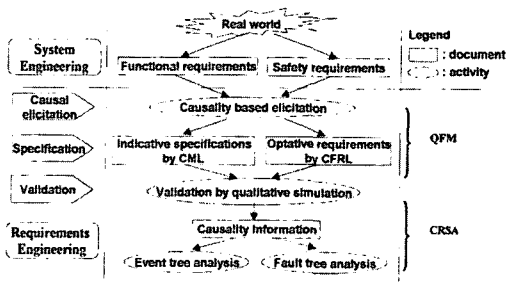


그림 3 HRTS 소프트웨어 요구분석 체계

인과관계에 따라 목표기반으로 표현하기 위해 원인결과 기능표현언어 CFRL (Causal Functional Representation Language)을 사용하였다. CML로 표현한

HRTS의 동작특성을 DME를 이용해 시뮬레이션함으로써 계통 상태의 원인결과 정보를 도출하여 소프트웨어 안전성 분석을 위한 기준으로 사용한다. QFM과 다음 장에서 설명할 CRSA를 사용한 HRTS 소프트웨어 요구분석 체계는 그림 3과 같다.

HRTS를 위한 정성적 소프트웨어 요구분석 체계의 전반부를 구성하는 QFM절차는 다음과 같다. 정성추론을 이용한 QFM의 장점은 요구 분석 시 필수적인 정성적, 인과적 사고를 지원하는 것이다.

- **QFM 1:** CML을 이용하여 통합모델(P∧C)을 명세한다. 주어진 사실인 제어대상의 동작을 정성미분방정식과 인과관계를 사용하여 정성적으로 모델링하고, 제어대상이 가지는 목적 달성을 위해 어떻게 제어할 것인가를 명세 한다.
- **QFM 2:** CFRL을 이용하여 희망사항(optative)인 기능 및 안전 요구사항(Sp)을 인과관계에 따라 목표 기반으로 명세 한다.
- **QFM 3:** CML로 명세 한 HRTS 통합모델(P∧C)의 DME에 의한 시뮬레이션으로 상태궤적을 생산한다.

2.3.1 QFM1: HRTS 통합모델 (P∧C) 명세

정성물리 이론은 기존 정형기법의 정량적인 미분방정식과 시간함수 대신에 정성 미분방정식과 인과관계를 이용하여 정성적으로 모든 물리적 현상을 표현할 수 있게 한다. HRTS의 연속상태 및 이산상태의 정량적 상태변화는 그림 4와 그림 5의 단위모델(model fragment)들을 사용하여 정성적으로 모델링 하였다. 이 모델을 시뮬레이션 함으로써 HRTS의 정량적 상태변화가 표 1과 같이 정성적 시간 축에서 상태변수, 상태의 시간적 선후관계, 인과관계 등으로 추상화 된다는 것을 알 수 있다. CML을 이용한 제어대상과 제어기의 통합모델(P∧C) 명세는 다음과 같은 장점이 있다.

- 정성적 표현은 요구분석단계 엔지니어 사고의 추상화 정도와 일치하며, 자연어에 의한 요구사항 도출 및 명세처럼 쉬우면서 정성적 정형규칙을 유지함으로써 기존 정형기법의 장점도 그대로 가진다.
- 그림 4와 그림 5에서와 같이 제어대상(P)과 제어기(C)를 모델링할 때, CML을 사용하는 QFM에서는 물리적 현상의 주요상태 변환 점(landmark)에 대한 분야지식을 바탕으로 직접 물리적 단순화를 추구하기 때문에, HRTS와 같이 물리적 법칙의 지배를 받는 공학장치의 물리적 현상을 수학적 단순화 방법보다 정확히 모델링할 수 있고, 또한 모델링 결과의 물리적 재해석을 불필요하게 한다.

```
Behavior of Steam Generator
Steam-Generator (SG)
  Pm: (Steam-generator ?s)
  Cm: ((Thermal-energy-steam-out ?s)
       = M+(Thermal-energy-primary-in ?s))
      ∧ ((Heat-transfer-rate ?s) = M+(Level ?s))
      ∧ ((Level ?s) = $IL$ - $SO$ + $FI$
            + M+(Thermal-energy-primary-in ?s))
SG-operating-in-low-reactor-power (SL)
  Pm: (Steam-generator ?s) ∧ (Reactor ?r)
      ∧ ((Level ?s) > $LSP$)
      ∧ ((CAvgPower ?r) < 10 %FP)
  Cm: (Thermal-energy-feed-in ?s) = 0
      /* no recirculation */
SG-operating-in-normal-reactor-power (SN)
  Pm: (Steam-generator ?s) ∧ (Reactor ?r)
      ∧ ((Level ?s) > $LSP$)
      ∧ (10%FP =< (CAvgPower ?r) < 90 %FP)
  Cm: (Heat-transfer-rate ?s) = 35 %
SG-operating-in-high-reactor-power (SH)
  Pm: (Steam-generator ?s) ∧ (Reactor ?r)
      ∧ ((Level ?s) > $LSP$)
      ∧ ((CAvgPower ?r) >= 90 %FP)
  Cm: (Thermal-energy-steam-out ?s) = $Max-S$

Behavior of Secondary Loop
Thermal-load (TL)
  Pm: (Steam-generator ?s)
  Cm: ((Thermal-energy-feed-in ?s)
       = (Thermal-energy-steam-out ?s) - $Work$
       - $Tloss2$)

Behavior of Reactor
Reactor-thermal-energy-generating (RT)
  Pm: (Reactor ?r) ∧ (In-closed-thermal-loop ?r)
  Cm: ((Thermal-energy-hot-leg ?r)
       = M+(d(CAvgPower ?r)/dt) - $Tloss1$
       + (Thermal-energy-cold-leg ?r))
Reactor-in-open-loop (RO)
  Pm: (Reactor ?r) ∧ (In-closed-thermal-loop ?r)
  Cm: (Thermal-energy-hot-leg ?r) = 0

Behavior of Trip Relay
Relay-closed (TC)
  Pm: (Steam-generator ?s) ∧ (Reactor ?r)
      ∧ (Trip-relay ?t) ∧ (Closed-p ?t)
  Cm: ((Thermal-energy-hot-leg ?r)
       + (Thermal-energy-primary-in ?s) = 0)
Relay-opened (TO)
  Pm: (Reactor ?r) ∧ (Trip-relay ?t) ∧ (Open-p ?t)
  Cm: (Thermal-energy-hot-leg ?r) = 0
Relay-closing (CL)
  Pm: (Trip-relay ?t) ∧ (Open-p ?t)
      ∧ (Signal-on (Sig-terminal ?t))
  Dm: (Closed-p ?t)
Relay-opening (OP)
  Pm: (Trip-relay ?t) ∧ (Closed-p ?t)
      ∧ (Signal-on (Sig-terminal ?t))
  Dm: (Open-p ?t)
```

그림 4 원전 자동정지계통 제어대상 단위 모델

그림 1 SDS2의 구조적 정보는 각 부품과 이들의 연결관계를 나타내는 단위 모델들로 표현된다. 이와 같은 정적인 구조를 표현하는 단위 모델은 DME 시뮬레이션 과정에서 항상 활성화되어 사용된다. 그림 4와 그림 5는 월성 원자력 발전소 자동정지계통 중 SGLL 트립 제어

기와 관련 제어대상의 동작을 나타내는 동적인 단위 모델을 보여준다. 여기서 Pm은 조건부를 나타내며, 동작 수행에 필요한 요소들의 상태 값 공간(Q)에 대한 조건들이다. 실제 동작을 나타내는 결과(consequence)는 Cm과 Dm이 있다. 결과로 나타나는 물리적 현상이 연속적인 동작일 때는 Cm으로, 비연속적 상태 변화일 때는 Dm으로 표시한다.

그림 4의 첫 번째 단위 모델 (SG)는 증기발생기의 동작을 정성적으로 표현하고 있다. 즉, 발생된 증기의 열 에너지는 일차계통 냉각수의 열 에너지와 단조증가 함수관계를 가진다. 또한, 증기발생기의 열 전달 효율은 증기발생기 수위에 비례함을 나타내고 있으며, 이 수위는 일차계통 냉각수의 열 에너지, 이차계통으로 보내지는 증기의 양, 되돌아오는 급수의 양에 따라 변한다. 여기서 증기의 양(SO)과 급수량(FI)은 초기 수위(IL)와 함께 상수화 하였다.

두 번째 단위 모델(SL)은, 초기 원자로 출력이 10%FP가 될 때까지 일차계통 냉각수가 순환되지 않기 때문에 증기발생기에서 열 전달이 발생하지 않음을 나타낸다. 단위 모델 (SN)은 정상운전 동작을 나타내는 것으로, 원자로 출력이 10 %FP와 90%FP 사이일 때는 정상 열 전달 율 35%가 유지되고, 90%FP를 넘어서면 포화됨을 나타낸다. 이와 같이 증기발생기 동작을 나타내는 원자로 열 출력 값의 상태 값 공간(Q)은 {0, 10, 90, 120}으로 표현할 수 있으며, 0, 10, 90, 120 등은 주요 물리적 상태 변화를 나타내는 변환 점이다.

```
Behavior of Trip Controller
Trip-signal-on (TN)
  Pm: (Reactor ? r) ∧ (Trip-controller ?tc)
      ∧ ((Signal (Signal-terminal ?tc)) = off)
      ∧ ((CAvgPower ?r) >= 10 %FP)
      ∧ ((Level ?s) =< $LSP$)
  Dm: (Signal (Signal-terminal ?tc)) = on
Trip-condition-out (TT)
  Pm: (Reactor ? r) ∧ (Trip-controller ?tc)
      ∧ ((Signal (Signal-terminal ?tc)) = on)
      ∧ ((CAvgPower ?r) < 10 %FP)
  Dm: (Signal (Signal-terminal ?tc)) = off
```

그림 5 SDS2 트립 제어기 단위 모델

또한 이차계통의 동작, 원자로 동작, 트립-릴레이(trip- relay)의 동작 등을 나타내는 단위 모델들을 사용하여 SDS2의 제어대상(P) 동작을 모델링 한다. 제어대상 단위 모델들은 핵공학, 기계 및 유체 역학 등 기존 공학에서 이미 축적된 분야지식(domain knowledge)의 조각들을 정성적으로 표현한 것이다. 이는 요구분석 단계에서 취득가능 하거나 원하는 추상화의 정도에 따라 점진적/합성적으로 모델링할 수 있게 한다. 또한 물리적 주요 상태 변환 점(landmark)에 대한 분야지식을 활용하기 때문에, 추상적 요구분석 단계에서 필요로 하는 정보의 상세함의 정도에서 볼 때, 정성적이지만 정확한 모델링을 할 수 있으며 기존 방법의 복잡도 문제를 해결한다. 그림 5는 자동정지계통의 트립 제어기 동작을 모델링 한다.

2.3.2 QFM2: HRTS 요구사항 (Sp) 명세

원하는 기능 및 안전 요구사항(Sp)을 CFRL을 이용하여 인과관계에 따라 목표 기반으로 명세 한다. HRTS가 가져야 할 부분 동작을 상태의 인과관계를 나타내는 CPD(Causal Process Description)를 이용하여 목표기반으로 구체화하면서 명세할 수 있다. CFRL은 희망사항(Gf) 을 그 기능과 안전목표가 유지되기 위한 주변의 물리적 환경(Cf)과 물리적 객체의 구조적 특성(Df)을 함께 표현한다. 자동정지계통 제어장치의 초기 요구사항은 CFRL을 이용하여 그림 6과 같이 명세하고, 이를 그림 7과 같이 점차 구체화한다.

```
Ef: F1    /* function name of the trip controller */
Df: Device: (?sglltcs SGLL-trip-control-system)
Cf: Objects: /* context of sglltcs */
     (?pzr Pressurizer)
     (?pump Charging-pump)
     (?t-load Thermal-load-of-2ndary-loop-with-turbine)
    Conditions:
     (Thermally-connected (Thermal-out ?sglltcs)
          (Thermal-in ?t-load))
     (Thermally-connected (Thermal-in ?sglltcs)
          (Thermal-out ?t-load))
Gf: (ALWAYS (AND    /* initial goal of sglltcs */
     (Generating-power ?rx) (Closed-p ?relay)
          (Heat-sinked ?t-load)))
```

그림 6 자동정지계통 초기 요구사항 F1

F1에서 자동정지 계통의 초기목표(Gf)는 "원자로가 열 출력을 생산하는 근원으로 작용하는 일차계통에서 증기발생기는 적절한 열 제거원 역할을 수행해야 한다"이다. 그림 7에 표현한 F11의 Gf는 CPD들을 사용하여 상위 목표를 구체화한다. 이 목표를 기술하기 위해 사용된 CPD들은 그림 8과 같이 표현할 수 있다. F11의 Df는 계통 내부 부품들의 구조적 연결 상태와 구조적 조건들을 기술한다. F11의 Cf는 자동정지계통 제어장치가 작동하는 환경요건을 표현하며, 이는 F1의 Cf 요건을 상속한다.

F11에 구체화된 자동정지계통 제어장치 기능 및 안전 목표(Gf)는 "항상 AND 아래의 세 가지 세부 목표들을

동시에 만족하여야 한다"이며 각 세부 목표의 의미는 다음과 같다.

- (IMPLIES (AND (≥(CAvgPower ?rx) 10%FP) (>(Level ?sg) LSP) (Closed-p ?relay)) CPD1): 원자로의 반응도가 증가하고 증기발생기 수위가 안전기준치 이상일 때, 증기발생기에서 정상적인 열전달이 이루어져야 함을 의미한다.
- IMPLIES (AND (≥(CAvgPower ?rx) 10 %FP) (≤(Level ?sg) LSP) (Closed-p ?t)) CPD2): 원자로 열출력 측정값이 정해진 값 이상인 상태에서, 증기발생기 수위가 안전기준치보다 낮거나 같으면 자동정지 계통이 작동되어야 함을 의미한다.
- (IMPLIES (AND (<(CAvgPower ?r) 10 %FP) (Closed-p ?t)) CPD3): 원자로 열 출력이 정해진 값보다 낮으면, 증기발생기 수위가 안전기준치보다 낮더라도 발생된 트립신호는 제거되어야 함을 의미한다.

이와 같이 CPD는 원하는 일련의 상태변화만을 기술한다. 즉, HRTS가 취하는 전체동작 중 만족해야 하는 부분적 상태변화를 표현한다.

```
Ef: F11        /* refined function name of F1 */
Df: Device: (?sglltcs SGLL-trip-control-system)
      Components:
       (?sg Steam-generator)
       (?rx Reactor)
       (?relay Trip-relay)
       (?tc Trip-controller)
      Conditions:
       (Thermally-connected (Hot-leg ?rx)
            (In-terminal ?pzr))
       (Electrically-connected (Flux-terminal ?rx)
            (Flux-sensing-terminal ?tc))
       (Thermally-connected (Out-terminal ?pzr)
            (Coolant-in ?sg))
       (Electrically-connected (Level-terminal ?sg)
            (Level-sensing-terminal ?tc))
       (Thermally-connected (Inlet ?pump)
            (Coolant-out ?sg))
       (Thermally-connected (Outlet ?pump)
            (Cold-leg ?rx))
       (Electrically-connected (Signal-terminal ?relay)
            (Signal-terminal ?tc))
Cf: Objects: nil              /* inherit the context Cf of F1 */
   Conditions: nil
Gf: (ALWAYS (AND      /* refined goal of Gf in F1 */
       (IMPLIES (AND ( (CAvgPower ?rx) 10 %FP)
            (> (Level ?sg) $LSP$) (Closed-p ?relay))
            CPD1) /* subgoal 1: normal heat-sinked */
       (IMPLIES (AND ( (CAvgPower ?rx) 10 %FP)
            ((Level ?sg) $LSP$) (Closed-p ?relay))
            CPD2) /* subgoal 2: trip when SGLL occurs */
       (IMPLIES (AND (< (CAvgPower ?rx) 10 %FP)
            (Closed-p ?relay))
            CPD3))) /* subgoal 3: condition out trip signal */
```

그림 7 CFRL을 이용한 목표기반 요구사항 F11

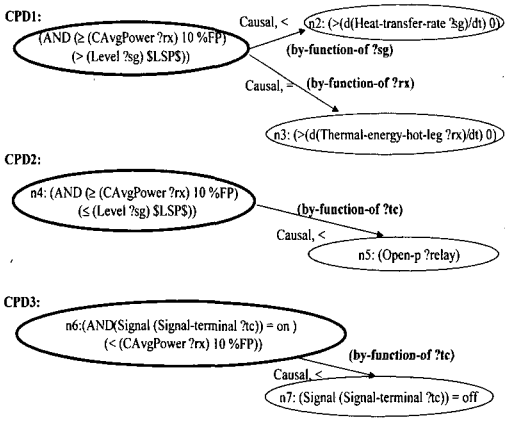


그림 8 CPD로 표현된 기능 및 안전요건 상태변화

2.3.3 QFM3: HRTS 정형명세 시뮬레이션

HRTS 소프트웨어 요구사항의 검증을 위해 정성추론 연구분야에서 물리적 장치의 동작을 예측하고 검증하기 위해 개발된 알고리즘[2]을 사용한다. CML로 명세 된 제어대상(P)과 제어기(C)의 통합 기정사실(indicative specification)이 CFRL로 명세 된 기능 및 안전 요구사항(Sp), 즉 희망사항(optative specification)의 만족여부를 확인한다. 이를 위해, 먼저, CML로 표현된 기정사실(indicative specification)의 동작을 DME(Device Modeling Environment)를 사용하여 시뮬레이션 한다. 통합모델(P∧C)의 동작특성 시뮬레이션 결과는 표 1과 같은 상태 변수들의 인과관계와 동작상태 궤적으로 생산된다.

표 1의 상태궤적은 HRTS 통합모델(P∧C)의 이산상태 변화와 연속상태 변화를 함께 정성적으로 표현하고 있으며 정성 복합 오토마타(QHA)의 상태수행 궤적이다. 또한 희망사항을 표현하는 그림 8의 CPD들은 전체 상태궤적이 만족해야 하는 안전 및 기능 요건의 부분적 상태 변화들을 QHA로 표현한 것이다. 이러한 상태 변수들의 인과관계와 동작상태 궤적을 CFRL의 CPD로 표현된 요구사항(Sp) 동작과 비교하여, 의도한대로 작동하는지 여부, 즉 긍정적 측면에서 기능만족 여부를 부분 검증할 수 있다. 부분 검증이란 특정시나리오 하에서 통합 모델의 동작특성이 주어진 기능 및 안전 요건을 만족하는지를 검증하는 것이다. 이는 통합모델이 항상 요구사항을 만족하는지를 증명하는 것이 아니라 특정 상태궤적에 대해서만 검증하는 것으로 테스팅에 가깝다.

DME 시뮬레이션으로 생성한 표 1 통합 모델 상태

표 1 HRTS 동작상태궤적

Active Models	state	Reactor	Relay	Signal	T1	T5	T6	T7	Level	CAP
SL, TC	**s0**	Heat-up	Close	Off	60-292 inc	60-326 inc	0-1000 std	0-840 std	50 std	0-120 std
SL, TC, **RT**	**s1**				292 inc	292 inc	0 inc	0 inc		
SL, TC, RT, **TL**	**s2**	Start-up					30 inc		52 dec	
SL, TC, RT, TL, **TN**	**s3**						50 inc	15 inc		2 inc
SL, TC, TL, RT, TN, **TT**	**s4**			On	292 std	294 inc				
SL, TC, RT, TL, TT	**s5**			Off					30 inc	10 inc
SN, TC, RT, TL	**s6**									
SN, TC, RT, TL	**s7**									
SH, TC, RT, TL	**s8**									90 inc
SH, TC, RT, TL	**s9**				292 std	326 std	1000 std	840 std	50 std	100 std
SH, TC, RT, TL	**s10**									
SH, TC, RT, TL	**s11**									
SH, TC, RT	**s12**								30 dec	100 std
SH, TC, RT, **TN**	**s13**									
SH, TC, RT, TN, **OP**	**s14**			On						
SH, RT, TN, OP, **TC**	**s15**		Open							
RO, TO	**s16**	Shut Down								
RO, TO	**s17**	Heat Remove			292 inc	327 inc	x dec	x x	20 dec	0

궤적에는 17개의 상태와 9개의 상태변수가 있다. 시뮬레이션은 더 이상 도달 가능한 상태가 없거나 시뮬레이션 초기에 정한 상태 수에 도달하면 끝난다. 표 1에서 상태변수는 상태변화에 직접 관련된 것만 표시한다. 각 상태변수 값이 가질 수 있는 구간과, 그 미분 값의 부호를 표시하고 미분 값의 부호가 결정되지 않는 변수 부분은 x로 표시한다. 상태변수 값의 구간에서 -와 +는 각각 {-∞, 0}과 {0, +∞}를 나타낸다. 미분 값의 부호는 inc, dec, std로 표시하며 각각 미분 값이 증가(increase) 중. 감소(decrease) 중, 변화 없음(steady)을 나타낸다. 표 1의 맨 왼쪽 열은 시뮬레이션 과정에서 해당 상태를 예측하는데 관여된 단위 모델들 중 상태변화에 관련된 것들만을 나타내고 있으며, 각 기호는 그림 4와 그림 5에 있는 단위 모델들의 약어들이다. 굵게 표시된 것은 해당 상태에서 새로 활성화(activate)된 것이며 밑줄 친 것은 비 활성화(deactivate)된 단위 모델들을 표시한다.

이 시뮬레이션에서 원자로에 의한 일차계통 열 출력(T1과 T5)은 온도 값으로 계산하였고, 증기출력의 열 에너지(T6)는 이 증기에 의해 생산되는 전기에너지로 계산하였다. 또한 급수(feedwater)의 열 에너지(T7)는 유속과 온도에 의해 계산되고, 원자로의 출력단위는 %Full Power(%FP)로 표현하였다. 시뮬레이션을 간략화 하기 위해 증기발생기 저 수위 안전 기준치는 고정된 값(30%)을 사용하였다.

이 상태 궤적은 HRTS 제어대상과 제어기 통합모델(P∧C)을 정성 복합 오토마타(QHA)로 모델링하고 그 동작을 시뮬레이션한 것과 같다. 시뮬레이션에 의한 상태의 진행은 단위 모델들의 활성화/비활성화에 의해 결

정된다. QHA 개념을 가지는 QFM은 HRTS 동작 세부 요소별 물리적 현상을 단위 모델로 표현하고, 이들의 집합에 의해 전체 HRTS의 동작을 명세 한다. 각 단위 모델의 활성화/비활성화 조건부분과 결과부분을 표현하고 있는 정성 미분방정식은 상태변수를 포함한 정성 수식으로 물리적 현상을 표현한다. 여기서 상태변수 값의 구간은 다양한 추상화의 정도를 가질 수 있는 주요상태 변환 점(landmark)을 기준으로 이산화 된다. 또 상태변수 미분 값의 부호에 따라 상태변화의 방향성이 결정된다.

증기발생기 수위는 50%, 원자로는 가열모드, 트립-릴레이(trip-relay)는 닫혀있는 상태로 시뮬레이션을 시작하였다. 초기상태(S0)에서 열 에너지 T1과 T2는 그림 1의 t1과 t2위치에서 증가한다. 냉각수 온도 T5가 292C에 이르면(S1) 원자로는 기동모드에 들어가고 이차계통에서 증기가 생산되기 시작한다(S2). 이 시점에서 급수 유량이 증가하고, 증기발생기 수위는 팽창 및 수축(swell and shrink) 현상에 의해 일시적으로 안전기준치를 벗어나게 되고, 이에 따라 트립 신호가 발생한다(S4). 그러나 원자로 출력이 아직 10%FP 미만이었기 때문에 트립 신호는 제거된다(S5). 출력운전모드 동안 원자로 출력은 계속 증가하고, 10%FP에 이르면 증기발생기는 정상운전 상태로 들어간다(S8). 이 때, LOCA(Loss Of Coolant Accident), LOFW(Loss Of main Feed Water), 증기관 파단 사고 등 기계적 고장으로 인해 증기발생기 수위가 낮아지거나, 운전원 오류로 인해 증기발생기 수위가 낮아질 수 있다. 증기발생기 수위가 안전기준치(30%) 보다 낮아지는 순간 트립 신호가 발생하며(S14), 트립-릴레이(trip-relay)가 열린다(S15). 고압헬륨 가스에 의해 중성자 흡수 액이 일차 냉각계통으로 주입되고 원자로는 정지상태로 들어간다(S16). 일차계통의 열에너지는 원자로의 잔열 때문에 증가하기 때문에(S17) 잔열 제거계통이 작동하고, 증기발생기는 저온정지 상태로 운전된다.

이와 같이 정성적 정형명세기법(QFM)은 이산 계통 모델링 기법에서 단순 샘플링에 의한 제어 점 결정이나, 연속 계통 단순화(확률론, 퍼지, 수학적 추상화) 기법들에서의 수학적 단순화와는 다르게 처음부터 물리적 단순화를 취함으로써 HRTS 동작의 물리적 의미를 보존하는 단순화 기법이다. HRTS 모델링을 위한 복합 오토마타 기법에서는 상태를 정량적 상태변수와 연속 시간 축에서 변수간의 관계를 미분방정식으로 표현하고 있는 반면에, QHA 개념을 가지는 QFM은 물리적 주요상태 변환 점(landmark)에 의해 이산화된 정성 상태변수와 정성 시간 축에서의 정성 미분방정식으로 표현하는 것이 차이점이다.

3. 인과정보에 의한 요구사항 안전성분석 (CRSA)

3.1 CRSA 개요

QFM으로 명세 된 HRTS 소프트웨어 요구사항의 안전성 검증을 위해, 인과정보에 의한 요구사항 안전성 분석(Causal Requirements Safety Analysis: CRSA) 기법을 제안한다. CRSA는 부정적 측면에서 원하지 않는 위험요소의 존재여부를 분석하는 안전성 검증이다. CRSA에서는 수단-목표 계층(means-ends hierarchy)에 의한 계층적 사고를 지원하여, 계통 안전성 분석과 연계하여 소프트웨어의 안전성을 체계적으로 분석할 수 있도록 하였다. 소프트웨어 자체는 안전성을 논할 수 있는 대상이 아니며, 소프트웨어 안전성 분석의 목적은 소프트웨어의 논리적 오류로 인한 계통의 위해(hazard) 여부를 분석하는 것이다.

소프트웨어의 논리적 오류는 요구명세, 설계명세, 구현된 코드 등 여러 단계의 소프트웨어 개발 중간 결과물에서 나타날 수 있으며, 개발 공정 후반부로 갈수록 최초 계통 요구사항이 여러번 변환(transform)되기 때문에, 계통 위해 여부에 대한 인과 관계를 추론하기가 어려워진다. 소프트웨어 요구분석 단계에서의 안전성 검증으로 위험요소를 조기 발견하고 이를 설계 및 코드 단계 안전성 분석과 연계시킴으로써 인지적으로 균형을 이룬 소프트웨어 안전성 검증 기법을 제시하고자 한다.

CRSA는 고전적인 소프트웨어 결함 트리 분석기법(FTA: Fault Tree Analysis)[8]을 사용하지만 QFM에서 생산된 인과 정보를 활용함으로써, 이전의 소프트웨어 FTA 기법들이 가지는, 분석자의 주관과 계통 이해 능력에 의존하는 단점을 보완한다. CRSA는 QFM결과 생산된 인과정보 의미와 FTA 의미를 일치시킴으로써, 엔지니어의 주관과 계통 이해능력에 의존하지 않고 안전성을 분석할 수 있게 한다.

소프트웨어 안전성 분석은 물리적 계통 동작의 위험을 유발할 수 있는 소프트웨어 내부 조건을 식별해 내는 것이다. 특히 연속 상태 변화하는 제어대상(P)과 이를 제어하는 이산상태변화 제어기(C)로 구성된 HRTS를 위한 소프트웨어 요구명세의 안전성을 분석하기 위해서는 제어대상(P)과 제어기(C)의 통합모델에서의 위험동작과 이의 원인이 되는 제어기 소프트웨어 동작조건 사이의 인과관계를 분석하여야 한다. 위험요소의 원인을 찾기 위한 기존 FTA 기법들의 구조적 분석과 안

전 전문가의 분야지식 의존 방식은 분석결과의 객관성 보장을 어렵게 한다. 이를 극복하기 위해서는 물리적 계통의 동작모델에 근거한 결함 트리 작성을 수행하여야 하며, 이를 모델기반 FTA라고 한다.

영국 York대학의 Fenelon과 그 동료들은 프로그램의 논리적 구조에 근거한 FTA보다는 소프트웨어와 계통의 고장 유형관계로부터 FTA를 작성할 필요성을 인식하고 HFTA, FPTN 등의 방법을 제시하였다[9]. 그러나, 이 방법들은 위험요소가 데이터에 기인한다고 가정하고 입출력 고장모드 간의 데이터 흐름 관계만으로 원인을 분석하려고 시도하기 때문에 물리적 동작의 인과관계는 분야전문가의 지식에 전적으로 의존하는 단점이 있다.

특히, 실시간 계통 동작의 위험요소는 상태 인과관계를 가짐을 인식하고 상태표(Statechart) 모델로부터 자동으로 결함 트리를 생산하는 연구가 수행되었으나[10], 제시하고 있는 결함 트리 작성 규칙이 아직 애매한 실정이다. 본 논문의 문제 대상인 HRTS는 상태표(Statechart) 모델에 근거한 모델기반 FTA가 불가능하다. 본 논문의 CRSA와 유사한 연구로서 Hansen의 Duration Calculus 모델에 근거한 FTA 기법 [11]이 있으나 요구사항 안전성 분석보다는 안전요건 도출을 위한 방법이며, 아직 이산 실시간 계통 안전성 분석에만 사용되고 있다.

이외에도 Liu[12]는 물리적 계통 모델로부터 결함 트리를 이용한 안전성 분석을 수행하는 모델기반 기법을 제시하였으나 엔티티-관계 모델링 방법을 사용하여 계통의 구조적 요소와 이들간의 관계로 계통을 모델링 하고 있으며 동작의 인과관계는 인위적인 관계들만으로 표현하는 수준이다.

본 연구에서는 소프트웨어 FTA에서 동작의 인과관계를 찾고 주관적인 분야 전문가의 지식에 의존하던 문제를 해결하기 위해 QFM 모델기반 FTA 기법을 제안한다. HRTS의 동작은 물리적 법칙에 의해 결정되고, QFM에 의한 HRTS 소프트웨어 요구명세는 정성물리이론에 의해 분야 전문가의 지식을 대신하여 객관화 시킬 수 있다. 본 논문의 CRSA는 이렇게 객관화된 QFM 모델로부터 도출된 인과관계 정보를 기반으로 한 소프트웨어 요구명세 FTA 기법이다.

3.2 CRSA 체계

3.2.1 CRSA 절차

HRTS를 위한 정성적 소프트웨어 요구분석 체계를 구성하는 CRSA절차의 세부 단계는 다음과 같다. 그림 9는 QFM의 각 단계별 인과관계정보와, 이를 사용하는 CRSA 세부 단계들 사이의 관계를 나타낸다.

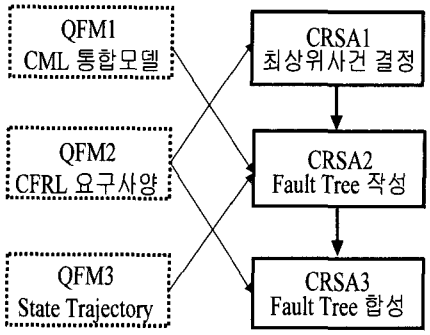


그림 9 CRSA 절차 및 QFM과의 관계

- **CRSA 1:** 최종 안전성 목표 달성을 위해 QFM2에서 작성한 CFRL 요구사항 명세에서 안전목표 트리(safety goal tree)를 작성한다. 안전목표 트리로부터 소프트웨어 FTA 수행을 위한 최상위 사건(top-event)을 도출한다. 이 트리의 최하위 노드들 중 소프트웨어 안전성관련 세부 목표(goal)의 역(negation)은 소프트웨어 위험 특성(hazardous property)이며, 소프트웨어 FTA 수행의 시작이 되는 최상위 사건이 된다.
- **CRSA 2:** 각각의 최상위 사건에 대해 가능한 사전조건 (preconditions) 들을 찾기 위한 세부 소프트웨어 FTA를 수행한다. QFM과 연계하여 객관적인 원인 추적을 할 수 있도록, CML로 표현된 제어대상 명세와 제어기 명세를 DME로 시뮬레이션하여 도출된 HRTS 동작상태의 인과관계 정보를 사용한다. 결함 트리는 계통 위해(hazard)의 모든 가능한 원인을 다루는 안전성 모델이 아니라, 특정 위해가 주어졌을 때 이를 유발할 수 있는 원인을 역추적하기 위한 하나의 표기법이다.
- **CRSA 3:** 각각의 최상위 사건에 대한 소프트웨어 FTA 결과에 대해 Dijkstra의 합성규칙을 이용하여 가능한 부분들을 합성한다. 부분 합성된 소프트웨어 FTA 결과를 CRSA1에서 작성한 안전목표 트리를 상향식으로 추적하면서 소프트웨어 요구사항 부분의 종합 FTA 결과를 합성한다. 이를 하드웨어 및 인적 안전성 목표들과 합성하여 최종 안전성 목표의 달성 여부를 분석한다.

3.2.2 CRSA1: 최상위 사건(top-event) 결정

결함 트리를 이용한 안전성 분석에서 맨 먼저 수행해야 할 일은 최상위사건을 철저하게 찾아내는 것이다. 최상위사건이란 발생하면 계통 기능상실이나 인명피해를

유발할 수 있는 모든 잠재적인 위험요소를 말한다. 이제까지는 소프트웨어 FTA를 수행할 대상인 최상위 사건을 결정하기 위해, 엔지니어의 경험에 의한 주관적 판단에 따라 HRTS 계통의 예비 위해도 분석 (PHA: Preliminary Hazard Analysis)을 수행하였다. PHA의 결과는 계통 위험요소(top-events)들의 분류된 목록이며, 각각의 최상위 사건에 대해 소프트웨어 FTA를 수행하여 가능성 있는 원인을 찾아간다.

CRSA에서는 소프트웨어 FTA의 최상위 사건을 결정하기 위해 QFM2에서 작성한 CFRL 요구사항 명세로부터 안전목표 트리를 작성한다. 이로부터 소프트웨어로 인한 계통 위험요소의 초기 목록(initial hazard list)을 파악하여 분류한다. 모든 안전 계통은 만족해야 할 최종 안전성 목표가 있다. 예를 들어, 원자력 발전소 자동정지계통의 최종 안전성 목표는 노심을 보호하여 방사능으로부터 대중의 안전을 지키는 것이다. 증기발생기 저수위 트립 제어기의 목적은 원자로의 핵반응으로 열 출력이 생산될 때, 증기발생기는 적절한 열 제거 원 역할을 수행하는 것이다. 이는 그림 6 CFRL 요구명세의 Gf에 표현되어 있다. 최종 안전성 목표 Gf의 논리적 역(negation)은 계통 위험 최상위 사건이 된다. 최종 안전성 목표 (final safety goal)를 루트로 시작하여 세부 안전성 목표들을 안전목표 트리 형태로 작성한다. 그림 6의 Gf에서 목표기반으로 구체화된 그림 7의 Gf로부터 그림 10처럼 안전목표 트리를 작성한다.

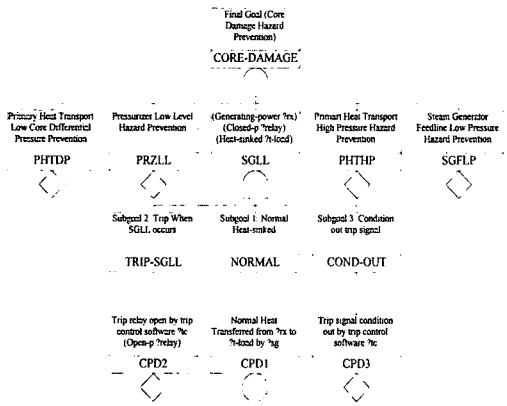


그림 10 안전목표 트리

본 논문에서는 그림 10에서 원자로심 보호를 위한 하위 목표들 중 증기발생기 저수위로 인한 위험을 방지해야 하는 목표 SGLL-HP에 대한 소프트웨어 FTA의 최상위 사건들을 찾아내고 CRSA를 적용하는 방법을 설명한다. SGLL-HP의 하위목표에는 SUBGOAL1, 2, 3이 있으며, 이들의 역을 취하면 해당 기능 동작의 최상위사건이 된다. 이 중 SUBGOAL1과 관련된 요소는 증기발생기 및 원자로 동작의 상태변화로서 제어기 CCC 내부 소프트웨어가 직접 제어할 수 없는 것이며 계통 또는 하드웨어 안전성 분석 대상이다. 그러나 SUBGOAL2와 SUBGOAL3에서 CPD2와 CPD3는 제어기 CCC의 소프트웨어에 의해 동작이 결정됨을 알 수 있다. 따라서 원전 자동정지계통 소프트웨어 FTA를 위한 최상위 사건 은 다음 2가지로 결정된다.

- 최상위 사건1: ¬SUBGOAL2 /* Trip relay fail to open in low-SG-level */
- 최상위 사건2: ¬SUBGOAL3 /* Fail to condition out trip signal in low-power */

소프트웨어 FTA는 소프트웨어의 논리적 오류로 인한 계통의 물리적 위험을 분석하는 것이 목적이기 때문에 계통과 하드웨어는 완벽하다고 가정한다. 안전목표 트리는 각각의 소프트웨어 최상위 사건들에 대해 작성된 결함 트리들을 합성(compose)할 때 지침으로 사용된다.

3.2.3 CRSA2: 결함트리 작성

CRSA1에서 결정된 위험(top-event)의 원인을 역추적하기 위해 결함 트리를 작성할 때는, HRTS의 물리적 동작을 정성적으로 모델링한 기정사실 명세에 나타난 다음과 같은 인과관계 정보를 사용함으로써 분석자의 물리적 계통 동작 이해능력 의존 문제를 해결할 수 있다.

- 표 1의 동작상태 궤적에 나타난 HRTS 동작의 정성적 상태 변화에 대한 인과관계정보
- 그림 4와 그림 5의 단위 모델들에 나타난 논리식으로 표현된 조건과 결과 형태의 구체적인 인과관계 정보

이제까지 모든 소프트웨어 FTA 기법에서 제어기 소프트웨어 명세나 이를 구현한 프로그램의 논리적 오류로 인한 물리적 위험 유발 여부 분석을 위한 인과관계 정보는, 전적으로 분석자가 이해하는 계통의 물리적 동작에 대한 주관적 지식에만 의존해 왔었다. CRSA에서는 FTA 기법을 사용하여 요구사항(Sp)에 따라 작성된 제어기(C) 명세의 논리적 오류로 인한 물리적 위험 유발 여부를 판별하기 위해, HRTS 전체(P∧C) 동작의 시뮬레이션으로 생산한 상태 인과관계 정보를 사용함으로써, 제어기(C) 명세의 논리적 오류를 제어대상 동작과 연계하여 찾아낸다. CRSA에서는 CML로 작성된 제어대상(P)의 물리적 현상 모델링도 오류를 가질 수 있으나, 일반적으로 소프트웨어 엔지니어에게 제어대상의 물

리적 현상은 주어지는 기정 사실이기 때문에 완벽하다고 가정한다.

그러나, QFM2에서 CFRL을 사용하여 요구사항(Sp)을 명세할 때, 원자력 발전소의 원자로 열 출력과 증기 발생기 열 제거원 동작을 정확히 이해하지 못하였거나, 계통 안전 전문가와의 의사전달 오류 등으로 인해 그림 6, 그림 7, 그림 8의 명세에서 위험요소가 내포될 수 있다. 사고의 원인을 추적하기 위해 기정사실 명세에서 제공된 인과관계 정보를 사용하여 그림 11과 같이 결함 트리를 작성한다. 결함 트리 작성을 위한 체계적인 CRSA2 절차와 이 예제에 대한 단계별 작성과정은 다음과 같다.

① CRSA1에서 결정된 최상위사건은 방어해야 할 위험특성(hazardous property)으로서 특정상태를 나타낸다. 최상위사건에 해당되는 상태를 HRTS 동작상태 궤적에서 찾는다. 예를 들어, 자동정지계통 소프트웨어의 FTA를 위한 첫번째 최상위사건으로, Trip relay fail to open in low-SG-level가 주어지면 표 1 동작상태 궤적에서 상태 S15가 제대로 수행되지 않았다는 것을 알 수 있다.

② 동작상태 궤적의 특정 상태를 발생시키는데 작용한 단위 모델을 직전 상태에서 찾음으로써 그 원인을 추적한다. 표 1 의 상태 S14에서 OP 단위 모델임을 알 수 있다.

③ 해당 단위 모델 조건 논리식의 역을 취해 결함 트리를 구체화한다. 예를 들어, 그림 4의 이산적인(discrete) 동작인 Relay-opening(OP) 동작 발생을 실패하게 한 원인은 "¬((Trip-relay ?t) ∧ (Closed p ?t) ∧ (Signal-on (Sig-terminal ?t)))이 된다. 이는 결함 트리에서 각 세부 조건의 역에 대한 OR 게이트로 표현된다.

④ 구체화된 결함 트리의 event들 중 제어기 소프트웨어로 인한 원인은 2)와 3)의 방법으로 계속 구체화하고, 소프트웨어로 인한 원인이 아닌 것은 기본 사건으로 처리하여 구체화를 중단한다. 이중 트립 릴레이의 존재유무와 상태는 소프트웨어로 인한 원인이 아니므로 구체화를 중단하고, (Signal on (Sig-terminal ?t))는 ②와 ③에 따라 계속 구체화한다. ②에 의해 상태궤적에서 TN 단위 모델의 오류로 인해 이 사건이 발생함을 알 수 있다. ③에 의해 그림 5에 있는TN 단위 모델 조건부의 역을 취해 결함 트리를 구체화한다.

⑤ 제어기 소프트웨어 동작을 표현하는 단위 모델의 조건 논리식으로 결함 트리가 그려질 때까지 결함 트리 작성을 계속한다. 주로 이 단계에서 소프트웨어 요구사항(Sp)과 제어기 명세(C)의 논리적 오류로 인한 HRTS 동작의 물리적 위험 원인이 발견될 수 있다. ④번째 단계에서 추적된 원인인 TN 단위 모델은 제어기 소프트웨어 동작상태를 나타냄을 알 수 있으며, 이 단위 모델 조건논리식의 역을 취하여 해당 오류의 원인을 구체화한다. 즉, Signal on 동작 발생을 실패하게 한 원인은 ((Reactor ? r) ∧ (Trip-controller ?tc) ∧ (Signal (Signal-terminal ?tc)) = off ∧ (CAvgPower ?r) >= 10 %FP ∧ (Level ?s) =< LSP)이 된다

⑥ 특정 물리적 상태의 원인 추적을 위해 상태궤적의 초기 상태에 도달할 때까지 결함 트리를 작성한다. 요구사항(Sp)과 제어기 명세(C)에서의 모순 발견으로 일차적인 위험원인을 찾게 되면, 해당 상태의 역을 취해 명세의 잘못된 부분을 변경한다. 변경한 상태를 시작점으로 또 다른 위험원인 추적을 계속한다.

이 절차에 따라 첫번째 최상위사건에 대한 결함 트리를 그림 11과 같이 구체화할 수 있으며, 같은 방법으로 두번째 최상위사건에 대한 결함 트리도 체계적으로 작성할 수 있다.

결함 트리 작성의 객관적 지침으로 사용되는 상태궤적(state trajectory), 단위 모델의 조건논리식, 상태변수의 인과순서 등은 HRTS 통합모델(P∧C)의 물리적 현상에 대한 인과정보를 표현하며, 이들은 기존 결함 트리 작성과정에서 물리적 현상에 대한 분석자의 주관적 이해를 대신한다. 따라서, 결함 트리 작성 시 HRTS의 물리적 현상에 대한 객관적 인과정보를 사용함으로써 체계적인 결함 트리 작성이 가능하도록 하였다. 이와 같이 작성되는 결함 트리의 상세함의 정도는 QFM에서 제공되는 인과정보에 따라 결정된다. 즉, QFM에서 CML을 사용하여 합성적으로 명세하기 때문에 CRSA도 이에 상응하는 정도의 상세함을 가지고 합성적으로 수행 가능하다.

특히, 여기서 상태궤적의 상태는 기존의 Petri Net이나 상태표(Statechart)를 이용하여 표현하는 소프트웨어의 이산 상태와는 다르다. 연속동작하는 제어대상 계통(P)과 이산적인 제어기(C)를 통합한 기정사실 명세의 시뮬레이션에 의해 생산되는 상태궤적은 HRTS 동작을 주요상태 변환 점(landmark) 개념에 따라 정성적으로 상태 변화를 나타내고 있다. 물론 QFM3에서 언급한대로, 이 상태궤적은 HRTS가 가질 수 있는 모든 상태를 표현하고 있는 것은 아니다.

그러나 최소한 요구사항(Sp)으로부터 정해지는 최상위 사건(top-event) 상태가 포함될 때까지 HRTS 통합

모델(P∧C)에 대한 정성 시뮬레이션을 수행함으로써, 최상위 사건에 대한 원인추적 과정에서 분석자의 주관적 지식을 대신할 수 있는 객관적 지침으로서의 정보가 상태궤적으로부터 제공된다. CRSA는 CFRL로 표현된 요구사항(Sp)과 제어기(C) 명세의 안전성 분석을 위한 FTA 기법으로서, 물리적 현상과 상충되어 위험을 초래할 수 있는, 요구사항(Sp)과 제어기(C) 명세의 논리적 오류를 찾기 위한 객관적 지침으로 이 상태궤적을 사용한다.

또한 HRTS 동작을 정성적 상태 변화로 추상화하였기 때문에 정확한 정량적 타이밍에 대한 FTA는 불가능하다. 그러나 상태의 인과순서에 따른 시간적 선후관계의 오류로 인한 위험을 분석함으로써 기존 기법의 복잡도 문제를 해결하였다. 따라서 CRSA는 HRTS 소프트웨어 요구사항의 초기 안전성 분석에 적합한 정성모델 기반 FTA 기법이라고 할 수 있다.

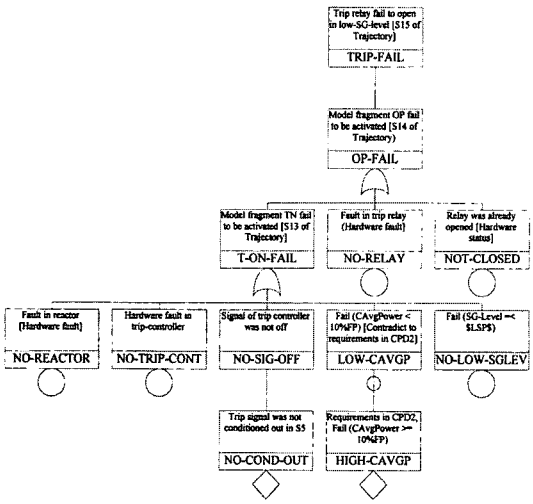


그림 11 Top-Event1에 대한 CRSA 결함 트리 작성 방법

3.2.4 CRSA3: 결함 트리 합성

각 최상위 사건에 대해 작성한 소프트웨어 FTA 결과를 CRSA 1에서 작성한 안전목표 트리를 상향식으로 추적하면서 소프트웨어 부분의 종합 FTA 결과를 합성한다. 즉, 그림 10의 안전목표 트리의 최종목표에서부터 소프트웨어 최상위 사건이 식별되는 부분까지의 트리 부분에 대한 논리적 역을 취함으로써 계통 최상위 사건(CORE-DAMAGE)의 원인추적을 위해 합성해야 하는 결함 트리를 그림 12에서와 같이 생산해 낼 수 있다. 그림 11에서 작성한 소프트웨어 결함 트리를 그림 12 결함 트리의 소프트웨어 최상위 사건 부분과 대치함으로써 소프트웨어 결함 트리의 합성을 완료한다.

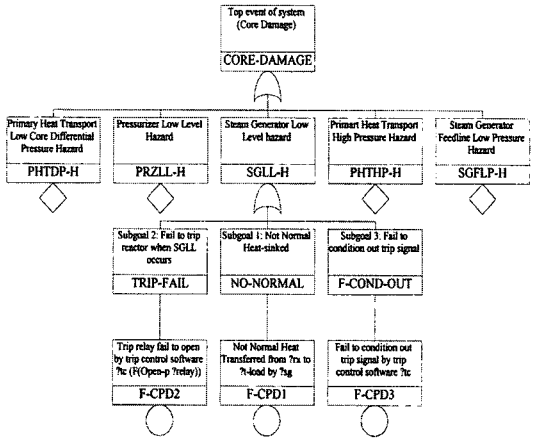


그림 12 결함 트리 합성

4. 결 론

QFM에서는 인공지능 분야에서 연구된 정성추론 이론을 HRTS 요구사항 정형명세에 도입함으로써 작성자와 분석자의 인지적 부담을 줄이고자 하였다. CML을 사용하는 QFM에서는, 연속시간과 이산시간 속성을 복합적으로 가지는 HRTS 동작의 물리적 현상을 주요상태 변환 점(landmark)에 대한 분야지식을 바탕으로 직접 물리적 단순화를 추구하기 때문에, HRTS와 같이 물리적 법칙의 지배를 받는 공학장치의 동작을 정성적 이지만 정확히 모델링할 수 있었다. 또 요구되는 기능 및 안전요건을 CFRL을 사용하여 인과관계에 따라 목표기반으로 명세하고, CML로 표현된 HRTS의 동작특성을 DME (Device Modeling Environment)를 이용해 시뮬레이션 함으로써 계통 상태의 원인결과 정보를 도출할 수 있었다.

CRSA에서는 고전적인 결함 트리 분석기법(FTA)을 소프트웨어 요구분석 단계에 적용하였다. CRSA는 QFM에서 생산된 원인결과 정보를 사용하여 결함 트리(fault tree)를 작성하기 때문에 이전의 소프트웨어 FTA 기법들이 가지는 분석자의 주관과 계통 이해능력에 의존하는 단점을 보완하였다. 또한 QFM의 결과로 생산된 원인결과 정보의 활용은 소프트웨어의 논리적 결함이 계통의 물리적 안전에 미치는 영향을 추적할 수 있도록 하며 계통 안전해석과 소프트웨어 안전성 분석

을 연결시켜 주는 장점이 있다.

현재의 DME 시뮬레이션을 통한 부분검증을 보완하여 정성차원에서 완전한 수학적 검증이 가능하도록 하기 위해, 이 논문에서 제안한 QHA 개념을 새로운 정형기법이론으로 정립할 계획이다. 또 이와 같은 정성적 정형기법은 최근 활발히 연구되고 있는 모델 검사(Model Checking) 기법[13]에 의한 검증 과정에서 상태집합(state space)의 크기를 줄여 보다 효과적인 검증을 가능하게 할 것이다. 또한 소프트웨어 개발공정 중 요구분석 단계 안전성 분석 기법인 CRSA가 설계 및 구현단계 안전성 분석기법과 연계될 수 있는 체계에 대한 연구가 계속되어야 한다. 이를 위해 인지계통공학에서 제시된 수단-목표/전체-부분(means-ends whole-part) 개념[14]을 적용한 목표기반 명세와 안전성 분석 체계에 대해 연구하고 있다. 마지막으로 가장 중요한 것은 QFM과 CRSA를 원자력 발전소 보호계통 개발과 같은 대규모 실제 문제에 적용하여 그 실용성을 증명하는 것이다.

참 고 문 헌

[1] B. Falkenhainer, A. Farquhar, D. Bobrow, R. Fikes, K. Forbus, T. Gruber, Y. Iwasaki, and B. Kuipers, CML: A Compositional Modeling Language. KSL in SRI Technical Report (KSL-94-16), 1994.

[2] Y. Iwasaki, M. Vescovi, R. Fikes and B. Chandrasekaran, A Causal Functional Representation Language with Behavior-Based Semantics, Applied Artificial Intelligence, vol. 9(1), Jan. 1995.

[3] Y. Iwasaki and C. M. Low, Model generation and simulation of device behavior with continuous and discrete change, Intelligent Systems Engineering, vol. 1(2), 1993.

[4] J. S. Ostroff, Temporal Logic for Real-Time Systems, p.209, Research Studies Press, 1989.

[5] B. Kuipers, Qualitative Reasoning: Modeling and Simulation with Incomplete Knowledge, p.418, MIT Press, 1994.

[6] R. Alur, C. Courcoubetis, T.A. Henzinger, and P.-H. Ho, Hybrid automata: an algorithmic approach to the specification and verification of hybrid systems, Hybrid Systems Workshop, Lecture notes in computer science, vol. 736, Springer-Verlag, pp. 209-229, 1993.

[7] A. Puri and P. Varaiya, Verification of Hybrid Systems using Abstractions, Hybrid Systems Workshop II, Lecture notes in computer science, vol. 999, Antsaklis, P., Kohn, W., Nerode, A., and Sastry, S.(Eds.), Springer-Verlag, pp. 359-369, 1995.

[8] U.S. Nuclear Regulatory Commission, Fault Tree Handbook, NUREG-0492, Jan. 1981.

[9] P. Fenelon and J. A. McDermid, An Integrated Tool Set for Software Safety Anlysis, J. Systems Software, vol. 21, pp. 279-290, 1993.

[10] S. Subramanian, R. V. Vishnuvajjala, R. Mojdebakhsh, W.T. Tsai, and L. Elliott, A Framework for Designing Safe Software Systems, COMPSAC95, pp.409-414, 1995.

[11] K. M. Hansen, A. P. Ravn, and V. Stavridou, From Safety Analysis to Software Requirements, IEEE Trans. on Software Engineering, vol. 24, no. 7, pp. 573-584, 1998.

[12] S. Liu, J. A. McDermid, Model-Oriented Approach to Safety Analysis Using Fault Trees and a Support System, J. Systems Software, vol. 35, pp. 151-164, 1996.

[13] G. Leeb and N. Lynch, Proving Safety Properties of the Steam Boiler Controller: Formal methods for industrial applications: A case study, In J.-R. Abrial, et al., Formal methods for industrial applications: Specifying and Programming the steam boiler control, vol. 1165, LNCS, Springer-Verlag, 1996.

[14] J. Rasmussen, A. M. Pejtersen, and L. P. Goodstein, Cognitive Systems Engineering, p.378, John Wiley & Sons, Inc. 1994.

이 장 수

1983년 경북대학교 전자공학 학사. 1986년 한국과학기술원 전산학과 석사. 1991년 정보처리기술사. 1994년 ~ 현재 한국과학기술원 박사과정. 1986년 ~ 현재 한국원자력연구소 책임연구원. 관심분야는 소프트웨어 안전성분석, 실시간 소프트웨어, 정형기법

차 성 덕

1983년 University of California at Irvine 전산학 학사. 1986년 University of California at Irvine 전산학 석사. 1991년 University of California at Irvine 전산학 박사. 1990년 ~ 1991년 Hughes Aircraft Co. 연구원. 1991년 ~ 1994년 The Aerospace Corp. 연구원. 1994년 9월 ~ 현재 한국과학기술원 전산학과 조교수