J. Korea Saf. Manag. Sci. Vol. 17 No. 1 March 2015
http://dx.doi.org/10.12812/ksms.2015.17.1.93

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

안전중시 시스템에서 DSM 기반 인터페이스 설계를 통한 시스템 오류 감축에 관한 연구

정 호 전* · 이 재 천*
*아주대학교 시스템공학과

On Reducing Systemic Failure of Safety-Critical Systems by DSM-based Systematic Design of Interfaces

Ho-Jeon Jung* · Jae-Chon Lee*
*Dept. of Systems Engineering, Ajou University

Abstract

The demand from customers on better products and systems seems to be ever increasing. To meet the demand, the systems are becoming more and more complicated in terms of both scale and functionality, thereby requiring enormous effort in the development. One bright spot of this trend is that such effort has been the driving forces of the remarkable advancement in modern systems development. On the other hand, safety issues appear to be critical in many large-scale systems such as transportation and weapon systems including high-speed trains, airplanes, ships, missiles/rockets launchers, and so on. Such systems turn out to be prone to a variety of faults and thus the resultant failure can cause disastrous accidents. For the reason, they can be referred to as safety-critical systems. The systems failure can be attributed to either random or systemic factors (or sometimes both). The objective of this paper is on how to reduce potential systemic failure in safety critical systems. To do so, a proper system design is pursued to minimize the risk of systemic failure. A focus is placed on the fact that complex systems have a lot of complicated interfaces among the system elements. To effectively handle the sources of hazards at the complicated interfaces and resultant failure, a method is developed by utilizing a design structure matrix. As a case study, the developed method is applied in the design of train control systems.

Keywords : Safety, Systemic Failure, DSM, Hazard Analysis, Systems Engineering

1. 서론

현대의 안전중시 시스템들은 과거와 비교해서 급격한 운영성능의 발전을 가져 왔고, 동시에 기능적으로도 매우 복잡해지게 되었다. 특히 이런 안전중시 시스템들은 사고나 고장이 인명 및 재산피해로 직결되기 때문에 체계적인 안전관리가 필요하다[1]. 이에 따라 국방, 철도, 항공, 해양, 원자력 등의 안전이 중시되는 산업분야에서는 안전과 관련한 표준규격을 제정하고 이를 준수하도록 권장하고 있다. 또한 현대의 시스템에서 전기

†이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2012R1A1A2009193)
†Corresponding Author : Prof. Jae-Chon Lee, Dept. of Systems Engineering, Ajou University, Wonchon-dong, Youngtong-gu, Suwon, 443-749, Tel: 031-219-3941, E-mail: jaelee@ajou.ac.kr
Received January 20, 2015; Revision Received March 13, 2015; Accepted March 16, 2015.

전자 및 소프트웨어의 비중이 높아지면서 전기전자 기능안전성 규격(IEC 61508)이 제정되어 현대시스템의 안전에 관한 규격을 제시하고 있다. 이를 바탕으로 하여 안전이 매우 중요시 되는 각 산업분야의 특성에 맞게 개선하여 자동차, 원자력, 의료기기 등의 산업분야에서 기능안전성에 관한 표준이 제정되어 이에 따른 시스템의 개발을 권고 하고 있다. 이와 같이 안전은 여러 산업분야에서 시스템의 개발에 있어서 반드시 확보해야 할 필수 요소가 되었으며, 이를 위한 투자가 활발히 이뤄지고 있다.

이처럼 중요시되고 있는 안전의 확보를 위해서는 발생 가능한 고장을 설계초기에 미리 식별하고 분석하여 대응하는 것이 중요하다. 안전관련 표준규격에서는 안전 확보를 위한 절차를 제시하고 있으며, 가장 핵심적인 단계로 위험원 분석 및 위험평가단계를 제시하고 있다. 또한 위험원 분석 및 위험평가를 설계의 초기 단계에 수행할 것을 권장하고 있다[2].

이런 분석과정을 통해 시스템에서 발생 가능한 고장을 식별하게 되는데 고장은 두 가지 유형으로 나뉜다. 첫째는 Random Failure로써 제품의 사용기한이 오래되어, 또는 외부의 충격에 의한 하드웨어 상의 고장을 일컫는다. 두 번째 유형은 Systemic Failure로써 시스템의 설계과정에서 발생 가능한 위험원에 의한 고장을 일컫는다. Random Failure의 경우 장치 및 부품 수준에서의 고장과 연관이 있고 Systemic Failure의 경우 시스템수준에서 식별해야 할 고장으로써 시스템을 구성하는 여러 구성요소들 간의 인터페이스 등의 영향을 받는 고장이다. 따라서 최신의 시스템일수록 복잡성이 증가하고 대형화 되고 있으므로 Systemic Failure의 식별 및 개선이 매우 중요해지고 있다.

M. Gentil 등(2008)에서는 시스템의 고장유형으로써 Random Failure와 Systemic Failure의 정의와 유발원인에 대해 정의 하고 있다. 여기서 Systemic Failure는 복잡성이 증가하고 있는 현대의 시스템에서 필수적으로 분석되고 감축되어야 할 고장유형으로 정의하고 있다. 그리고 Systemic Failure의 대표적인 위험원으로써 인터페이스의 복잡성을 제시하고 있다.

Y.M. Chen 등(2010)에서는 시스템의 개념설계 단계에서 기능식별 및 분석결과를 활용하여 위험원 분석을 수행하는 방법에 대해 제안하고 있다. 이것은 기능안전의 측면으로 고장분석이 이뤄지고 있는 최근의 위험원 분석에 대한 접근방법에 유용한 방법이라 할 수 있다.

위와 같은 선행연구 결과의 분석을 통해 현대의 복잡성이 증대되었고, 인터페이스가 매우 복잡한 시스템에 대해서는 Systemic failure의 분석이 매우 중요하며, 이는 개념설계 결과를 바탕으로 한 위험원 분석을 통해 식별이 가능하다는 것을 확인 할 수 있다. 그러나 근본적인 Systemic failure의 감축을 위한 접근 방법은 부족하다. 이를 위해 본 연구에서는 Systemic failure의 감축 방법으로써 근본적인 유발요인인 인터페이스의 통합을 통한 인터페이스의 최소화에 대해 연구하였고, 이때 DSM 기법을 활용 하였다. 이를 통해 시스템을 구성하고 있는 인터페이스를 최소화하여 Systemic failure의 감축을 달성할 수 있다.

본 논문의 구성은 다음과 같다. 서론에서는 사회 및 연구의 연구동향과 필요성을 제시하였고, 2장에서는 관련 선행연구 및 연구 목표를 기술하여 문제정의를 했다. 3장에서는 DSM 기반의 인터페이스 분석을 통한 Systemic Failure의 감축 방안에 대해서 제시한다. 4장에서는 3장의 활동을 바탕으로 철도시스템의 제어기능에 대해 Systemic Failure를 분석한 사례를 제시하였다. 5장에서는 본 논문의 결과를 정리 및 요약 하였다.

2. 문제 정의

2.1 현대의 시스템에서의 Systemic Failure 감축의 중요성

현대의 시스템은 더욱 복잡성이 증가하고 있고 구성요소들 간의 인터페이스도 더욱 많이 이뤄지고 있다. 따라서 구성 요소들 간에 인터페이스에서 발생 가능한 위험분석이 필요하다. 이에 따라 단일 부품 장치에 대한 고장만이 아닌 부품들이 모여서 이뤄진 컴포넌트, 또는 더 상위수준인 시스템 수준에서의 위험분석이 필요하다[5]. 이는 고장 유형 중 Systemic Failure와 연관이 있다.

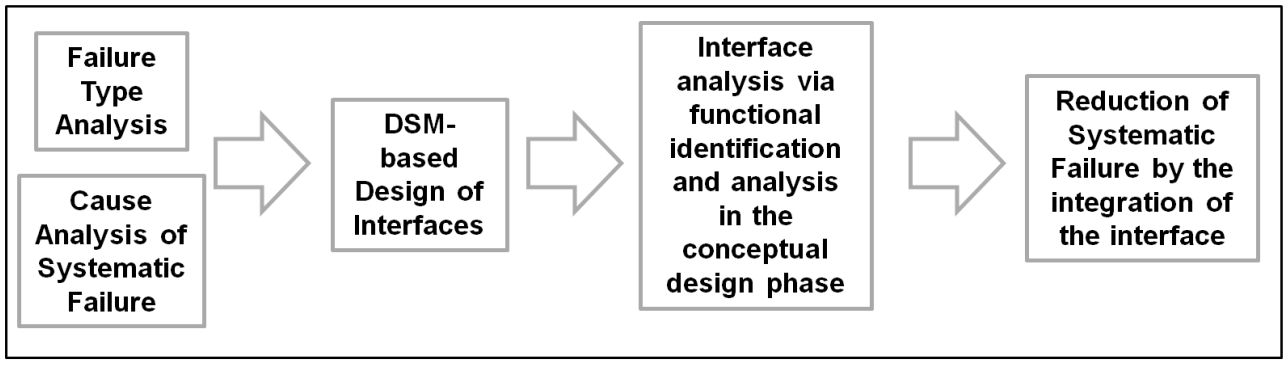
즉 Systemic Failure는 복잡성이 증가하며, 무수한 인터페이스가 이뤄지는 현대의 시스템에서 반드시 분석되고 관리과 이뤄져야 하는 고장 유형이라 할 수 있다.

이러한 Systemic failure의 감축을 위해서는 기능안전 표준에서 제시하고 있는 안전 수명주기를 바탕으로 하여 시스템의 개념설계 단계에서 위험분석을 통해 고장의 분석이 이뤄져야 한다[6]. 또한 개념설계를 통해 기능식별 및 기능분석을 수행함으로써 시스템의 인터페이스를 분석 할 수 있으며 이것을 최소화함으로써 Systemic failure의 유발 원인을 최소화 할 수 있다.

2.2 DSM 기반 인터페이스 통합의 유용성

DSM(Design Structure Matrix)은 복잡한 시스템을 명확하고 간결하게 표현하며, 또한 시스템요소(예를

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)



[Figure 1] Concept model for current research.

들어 하부시스템 및 모듈) 간의 상호작용 또는 상호의 존성과 인터페이스를 식별하는 방법을 제공한다[7]. 다양한 응용 분야에서 시스템 모델을 나타내고 분석하기 위한 방법으로 사용된다.

DSM은 효과적인 아키텍처의 설계, 최적의 아키텍처의 설계를 위해 적용되는 기법들 중의 하나이다.

DSM 기법에서 구성 요소간의 인터페이스를 분석하는 방법 중 하나가 Clustering 기법이다.

Clustering 기법은 그룹 간에 서로 배타적인 또는 그룹 간 상관관계를 최소로 하는 DSM 요소들의 그룹을 찾는 프로세스라 정의 된다. Clustering의 목표는 하나의 Cluster와 최소한의 인터페이스를 가지도록 하는 것이다. 즉 모듈화 개념과 유사하다 할 수 있다. 서로 상관관계가 높은 요소들을 하나의 그룹으로 묶어 나가되 그룹 간의 상관관계가 최소가 되도록 하는 것이다. 이를 통해 시스템을 구성하는 구성요소들 간의 인터페이스를 최소화 할 수 있다.

따라서 Clustering 분석을 수행함으로써 구성품들간 상관관계가 높은 요소들을 하나로 묶으면서 이러한 그룹들 간의 상관관계가 최소가 되도록 함으로써 인터페이스를 최소화 할 수 있다.

시스템을 개발하기 위해서는 우선적으로 사용자의 요구사항을 수집하고 이렇게 수집된 요구사항을 분석하여 논리적 아키텍처를 개발한다. 또한 이를 통해 사용자의 요구사항에 따른 시스템의 기능들을 파악 할 수 있다. 그 후 파악된 기능을 바탕으로 기능을 요소로 하는 DSM을 구성하고 각 기능들 간의 서로 영향을 주고받는 상호작용을 파악하여 DSM을 표현한다. 이를 바탕으로 Clustering을 수행하면 서로 밀접한 상호작용을 가지고 있는 기능들끼리 묶이게 된다. 이 결과를 바탕으로 인터페이스를 최소화 시킬 수 있으며, 이는 Systemic Failure의 유발원인인 인터페이스를 최소화 함으로써 Systemic Failure의 감축을 도모 할 수 있다.

2.3. 연구 목표 및 범위

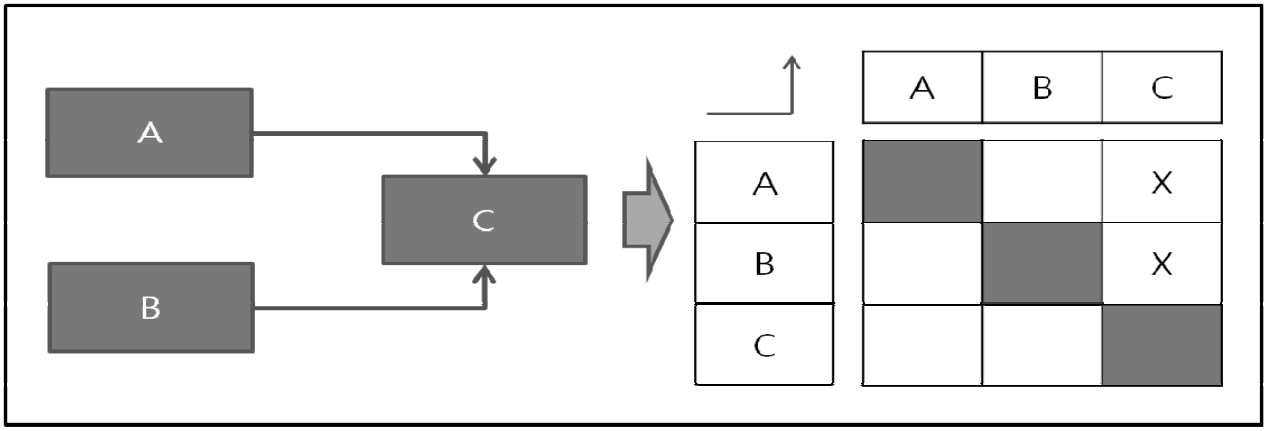
상위 선행연구 분석을 통해 현대의 시스템의 안전 확보를 위해선 Systemic Failure의 분석 및 감축이 필요하다는 것을 인지하였다. 또한 현재의 고장 및 위험 분석 활동이 부품 및 장치 수준에서 Random Failure의 분석에 집중 되어 있다는 것을 확인했다. 이러한 관점은 복잡성 및 구성요소간의 인터페이스가 증가하고 있는 현대의 시스템에는 부적절함을 알 수 있었다. 따라서 Systemic Failure를 식별하고 감축하는 것에 대한 접근 방법이 필요하다.

따라서 [Figure 1]과 같이 먼저 고장 유형의 분석 및 Systemic Failure의 원인에 대한 분석을 하고 Systemic Failure의 유발 원인인 인터페이스의 최소화를 위해 DSM 기법을 활용하는 것을 목표라 한다. 이를 위해 개념설계 단계에서 기능식별과 분석을 통한 인터페이스의 분석 방법에 대한 연구가 필요하며 최종적으로 개념설계 단계에서의 인터페이스 분석결과와 DSM 기법을 통한 인터페이스의 최소화를 수행하여 인터페이스의 통합을 통한 Systemic failure의 감축을 도모하는 것이 목표이다.

3. DSM 기반의 인터페이스 분석을 통한 Systemic Failure의 감축 방법

3.1. 개념설계 단계에서의 기능분석을 통한 인터페이스 식별

개념설계 단계에서 기능식별 및 분석을 통한 인터페이스의 식별 방법을 제안하기 위해 개념설계 단계에서의 설계활동을 분석했다.



[Figure 2] Relationship between a digraph and corresponding binary matrix.

시스템의 개념설계는 요구사항의 분석, 기능분석, 통합 세 가지 단계로 이루어져 있다.

첫 번째 요구사항 분석 단계에서는 사용자의 needs로부터 시스템의 구현에 필요한 요구사항을 도출한다. 이때 도출된 요구사항들은 기능분석의 근거가 되며, 향후 시스템의 통합단계에서 시험요구사항으로도 이용된다. 따라서 개발의 시작점으로써 요구사항의 분석은 매우 중요하다.

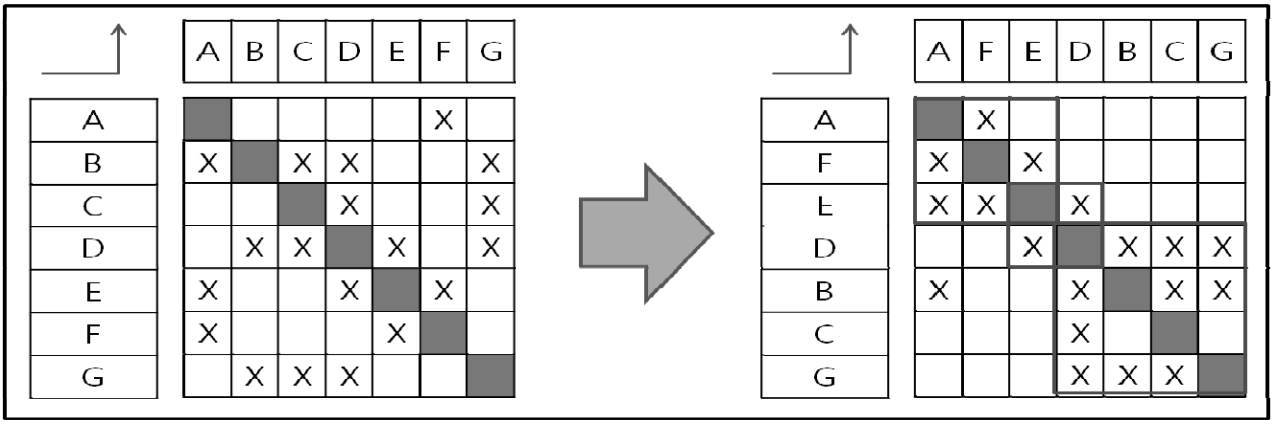
요구사항 분석결과 도출된 요구사항을 바탕으로 요구사항을 시스템에 구현하기 위해 필요한 기능을 식별 및 거동분석을 하는 기능분석단계가 수행된다. 도출된 요구사항을 할당받아 필요한 기능을 식별한다. 기능도 최상의 수준의 기능으로부터 하위 수준의 기능까지 구조적으로 식별한다. 또한 거동분석을 통해 식별된 기능들 간의 순서와 기능의 입출력 데이터와 데이터의 교환을 분석하여 인터페이스를 식별 할 수 있다.

이 두 가지 단계가 개념설계 단계에서의 핵심 활동이라 할 수 있으며, 이 두 단계를 통해 시스템을 구성하는 기능을 식별하고 기능들 간의 인터페이스를 식별 할 수 있다.

이때 거동분석을 하는데 에는 여러 가지 모델링 기법이 활용되는데 본 연구에서는 EFFBD(Enhanced Functional Flow Diagram)을 활용하여 거동 분석을 수행하였다.

3.2. DSM 기반의 인터페이스 통합 방법

DSM은 행과 열의 수가 같은 정사각 매트릭스로써 시스템 요소간의 관계 파악을 가능하게 한다. 시스템 구성요소간의 상호작용, 즉 인터페이스가 매트릭스에 표시되기 때문에 요소들의 거동과 값을 대규모로 파악할 수 있고, 이러한 이유로 인해 최근 DSM은 한층 유용하고, 중요해졌다.



[Figure 3] Clustering and resultant matrix.

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

DSM 방법론은 시스템 모델링을 그래픽적으로 표현하면서부터 시작되었다. DSM 표현방식의 특징은 상관관계의 정도와 방향을 동시에 표기할 수 있다는 것이다.

예를 들어, [Figure 2]와 같이 시스템이 요소 A, B, C로 이루어져 있고 세 요소 간에 정보 교환 및 물질 교환과 같은 상관관계가 존재한다고 가정하면, DSM은 3 × 3 매트릭스를 생성하고 매트릭스 안에 요소 간의 관계를 표현한다. 요소의 명칭은 매트릭스 가장자리 즉, 맨 좌측과 맨 위쪽에 기록된다. 요소 간의 관계 표시는 관계가 있는 경우 X, 없는 경우에는 빈 칸으로 표시한다.

기본적으로 관계의 표시를 'X'로 하는 매트릭스를 binary matrix라 하고, 관계의 정도를 숫자로 표현하여 가중치를 부여한 매트릭스를 numerical matrix라 한다.

[Figure 2]은 위에서 가정한 요소 A, B, C의 상관관계를 diagraph와 DSM으로 표현한 것이다.

이렇게 표현한 매트릭스를 기반으로 하여 DSM 기법에선 분석단계를 거치게 되며 이때 사용되는 기법이 clustering이다.

Clustering의 목표는 구성요소간의 하위집합을 발견하는 것이다. [Figure 3]과 같이 매트릭스가 변하면서 생긴 하위 집합을 모듈 또는 클러스터라 부른다.

매트릭스가 [Figure 3]에서 오른쪽과 같은 형태를 갖기 위해서는 행과 열의 재배열을 통해서 위쪽 삼각형 형태 또는 아래쪽 삼각형 형태로 만들어야 한다. 이러한 활동을 partitioning 또는 sequencing이라 부른다.

Partitioning 결과를 바탕으로 클러스터를 식별하여 클러스터들 사이의 상호작용, 즉 인터페이스를 최소화 시킨다.

이러한 목표를 가지고 clustering을 수행하는 절차는 다음과 같다.

(1) Binary Matrix 작성

(2) 모든 Component(구성품)들에게 input(입력) 데이터를 받지 않는 열을 매트릭스의 왼쪽으로 재배열 시킨다. 동시에 같은 행을 매트릭스의 위쪽으로 재배열 시킨다. 재배열 된 행과 열은 다음 단계에서는 제외시킨다.

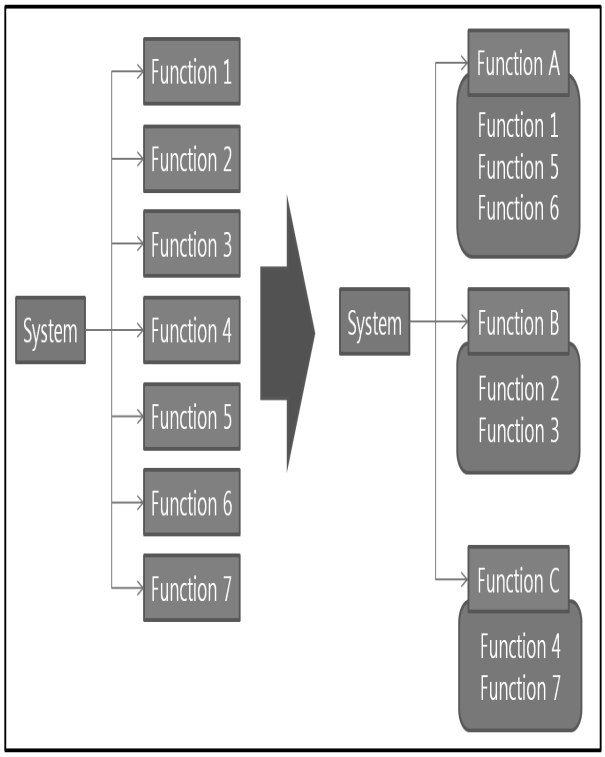
(3) 모든 Component들에게 output(출력) 데이터를 보내지 않는 행을 매트릭스의 아래쪽으로 재배열 시킨다. 동시에 같은 열을 매트릭스의 오른쪽으로 재배열 시킨다. 재배열 된 행과 열은 다음 단계에서 제외시킨다.

(4) 행과 열의 재배열이 끝나면 루프를 가지는 Component를 임의로 식별하여 (2)를 다시 수행한다.

(5) 위쪽 삼각형 형태(upper triangular form)으로 매트릭스가 완성되면 clustering을 마친다.

위와 같은 과정을 거쳐 [Figure 3]의 오른쪽 매트릭스의 결과를 얻는 것이 DSM이 최종 결과물이라 할 수 있다. 이 결과의 의미는 [Figure 3]의 왼쪽 매트릭스 X마크의 개수가 구성요소들 사이의 인터페이스 개수라 할 수 있다. 이를 clustering을 통해 밀접한 상호관계를 가지는 구성요소들을 통합하게 되면 [Figure 3]와 같이 클러스터들 사이의 인터페이스 2개와 클러스터외의 인터페이스 1개로 인터페이스가 최소화 되는 것을 확인할 수 있다. 클러스터 내부의 인터페이스는 기능의 통합, 물리적 구성품의 통합 등을 통해 구현할 수 있다.

이와 같이 DSM을 통해 시스템의 구성요소간에 인터페이스를 분석하고 이를 분석과정을 통해 최소화 할 수 있다.



[Figure 4] Concept of interface integration.

3.3. 인터페이스 통합을 통한 Systemic Failure의 감축

서론에서 고장의 유형에 대해서 분석한 결과에 따라 Systemic failure의 주요 유발원인은 인터페이스의 복잡성이다. 따라서 Systemic failure의 감축을 위해서는 시스템의 인터페이스를 줄이는 것이 가장 근본적인 해결방법이라 할 수 있다.

3.2절에서와 같이 본 연구에서는 인터페이스를 줄이는 방법으로써 DSM 기법을 활용하였다. 이를 통한 인터페이스 통합의 개념은 [Figure 4]와 같다. [Figure 4]의 왼쪽 그림이 DSM 적용 이전의 시스템

을 구성하는 Function의 모습을 나타낸 것이다. 여기에 DSM 기법을 적용하면 [Figure 4]의 오른쪽 그림과 같은 형태가 된다. Function A,B,C 라는 기존의 Function이 통합된 새로운 기능을 도출 할 수 가 있게 된다. 이때 통합된 기능은 clustering을 통해 생성된 클러스터이다. 이를 통해 기존의 7개의 기능 사이에 존재하던 인터페이스들이 3개의 기능들 사이의 인터페이스로 절대적인 개수가 줄어들게 된다. 이에 따라 Systemic failure의 위험원인 인터페이스가 줄어들어 결과적으로 Systemic failure가 감축 될 수 있다.

즉, 3장의 연구 결과를 통해 시스템의 설계 결과를 바탕으로 인터페이스를 식별하고 여기에 DSM 기법을 활용하여 인터페이스를 최소화 하며, 그 결과 Systemic failure의 유발 원인인 인터페이스가 줄어듦으로써 Systemic failure가 감축되는 효과를 얻을 수 있다.

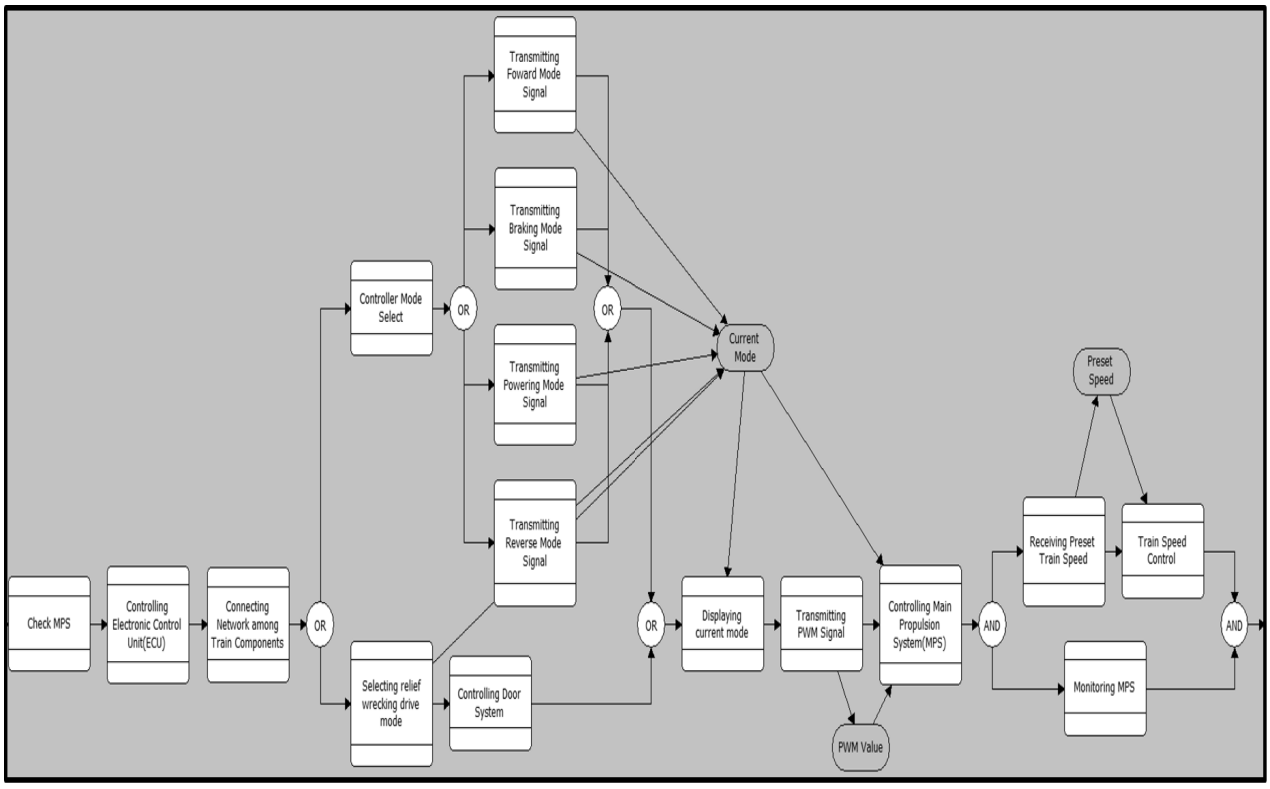
4. DSM 기반의 철도시스템 Systemic Failure 분석

3장에서 제시한 DSM기반의 인터페이스 통합 기법을 바탕으로 철도시스템의 제어기능에 대해 연구 결과를 적용하였다. 철도시스템의 제어 부분에 대한 기능 식별 및 거동 분석을 수행하여 인터페이스를 식별하고 이 결과를 기반으로 DSM 기법을 적용하여 인터페이스의 통합을 수행하였다. 그 결과를 1,2,3절에 제시하였다.

4.1. 철도시스템 제어 기능 분석

철도시스템은 철도차량, 철도 인프라, 신호 및 제어 시스템 등을 포함하는 복합 시스템이라 할 수 있다.

철도 시스템에서 철도 신호 및 제어시스템은 철도차량을 운행하는 과정에서 인명 사상 및 시설물 파손 등의 사고가 발생하는 것을 방지하는 시스템이라 할 수 있다. 철도 제어 시스템을 구축, 운용하기 위해서는 철도운행과정에서 발생할 수 있는 위험원 식별, 위험대책 설계 및 안전성 확인, 검증과 같은 위험원 분석 활동이 반드시 필요하다. 이에 더하여 철도 제어시스템에서 소프트웨어, 유, 무선통신기술등의 비중이 증가함으로써 위험원 분석을 포함하는 안전성의 확보가 더욱 중요 해졌다.



[Figure 5] Transforming the result of functional analysis into a behavior model for the train control system.

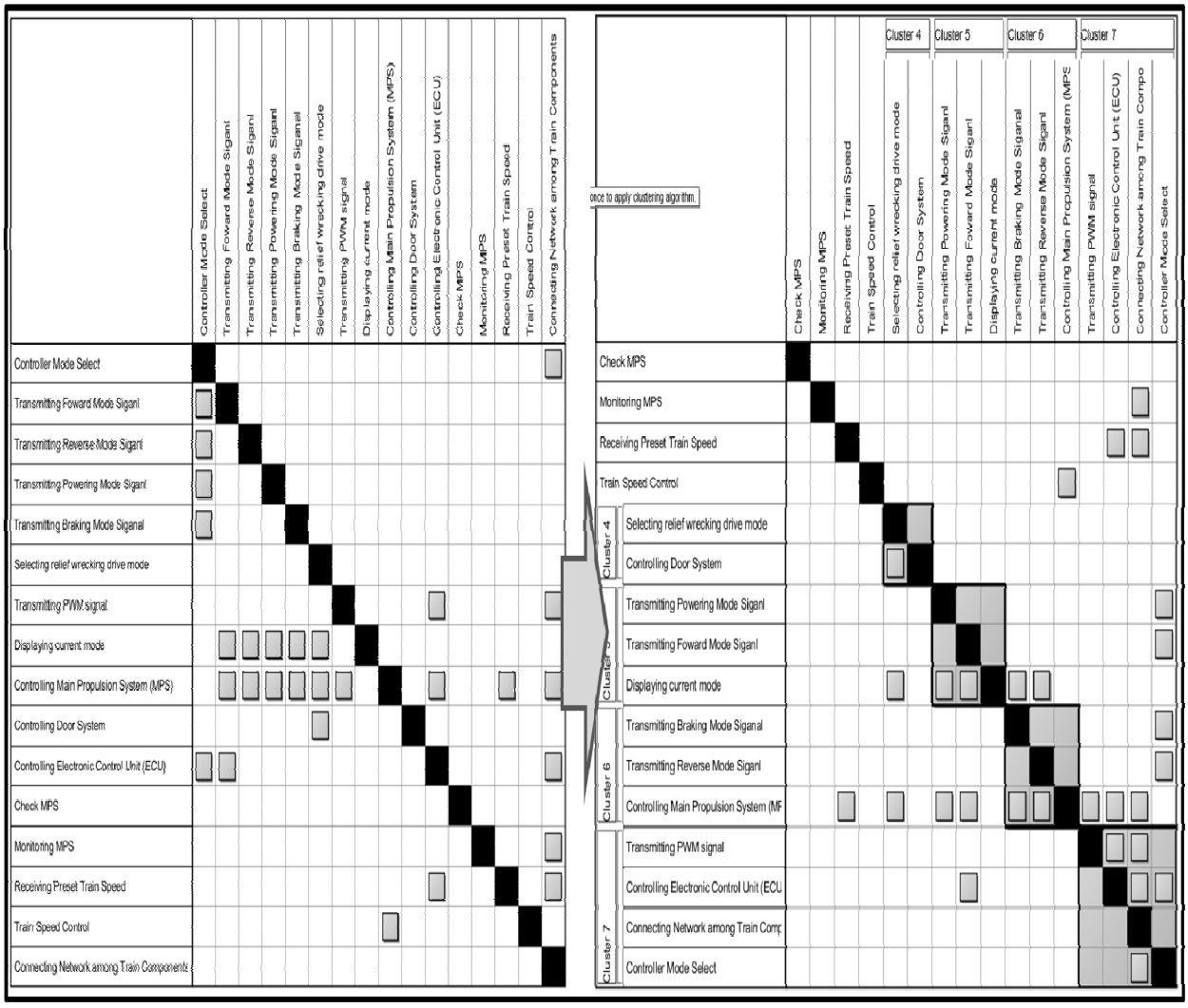
ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

이에 따라 철도 선진국에서는 IEC 61508 기능안전 표준을 바탕으로 하여 철도분야에 적용한 IEC 62278, 62279, EN 50126, 50128, 50129 등의 철도 및 철도 신호, 제어시스템에 대한 기능안전표준을 제정하여 철도 제어 시스템에 대한 정의 및 안전성을 확보하기 위한 안전관리 활동에 대해 정의 하고 있다.

철도 제어시스템은 철도차량의 운영을 위한 다양한 기능으로 구성되어 있으며, 배터리 제어, 속도 제어, 통신 제어 등의 기능이 포함되어 있다. 다양한 차량 제어부로 구성이 되어있다. [Figure 5]는 식별한 차량 제어시스템에 대한 기능들 중 차량의 제어 초기에 필요한 기능들과 기능들 간의 순서, 데이터 교환 등을 EFFBD를 활용하여 분석한 결과이다.

4.2. DSM을 통한 철도시스템 제어 기능 인터페이스 통합

4.1절의 철도시스템 제어기능 분석결과를 바탕으로 DSM기법을 적용하여 인터페이스의 통합을 수행하였다. [Figure 6]의 왼쪽 그림은 4.1절의 기능분석 결과를 바탕으로 매트릭스를 작성한 것이다. 왼쪽과 상단에 기입된 기능들이 식별된 기능들이며, 매트릭스의 마크가 있는 부분은 기능들 간의 식별된 인터페이스를 표시한 것이다. 이를 통해 철도의 제어시스템을 구성하는 기능과 기능들 간의 인터페이스를 매트릭스를 통해 확인할 수 있다.



<Figure 6> Applying DSM technique to the train control system.

[Figure 6]의 오른쪽 그림은 왼쪽의 매트릭스에 대해 clustering을 수행한 결과이다. 매트릭스 상에서 확인 할 수 있듯이, 기존의 기능들의 일부를 통합하여 추가적으로 4개의 클러스터를 식별하였다.

클러스터의 내부 인터페이스는 클러스터를 구성하는 기능의 통합 또는 기능을 수행하게 될 물리적 구성품의 통합을 통해 제거 할 수 있다.

이를 통해 기존의 29개의 인터페이스를 17개로 줄일 수가 있었다. 이것은 Systemic failure의 가장 대표적인 유발요인인 인터페이스의 최소화가 이뤄진 것을 의미하며 이것은 Systemic failure의 감축으로 이어진다.

5. 결 론

오늘날 점차 대형화 복잡화 되어가고 있는 시스템들은 더욱 커진 사고 및 고장에 대한 위험을 내재하게 된다. 또한 철도와 같은 대형 복합 시스템에서 발생하는 사고 및 고장은 바로 큰 재산피해나 인명피해와 직결 될 수 있다. 따라서 체계적인 안전관리의 필요성이 점차 커지고 있다.

이때 발생 가능한 고장의 유형에는 random failure와 Systemic failure가 있는데 시스템의 설계과정에서 발생 가능한 Systemic failure의 분석과 감축은 현대 시스템에선 매우 중요해지고 있다.

따라서 본 논문에서는 Systemic failure의 감축 방법으로써 DSM 기법을 활용한 인터페이스의 통합방법을 활용하였다. Systemic failure의 가장 큰 유발요인은 인터페이스의 복잡성이다. 따라서 가장 근본적인 Systemic failure의 감축 방법은 인터페이스를 최소화하는 것이다.

이를 위해 먼저 시스템 개념설계 단계의 기능분석 단계에서 기능을 식별하고 거동분석을 통해 기능간의 인터페이스를 분석했다. 기능 분석 결과를 바탕으로 DSM 기법을 적용하여 식별한 기능들간의 인터페이스를 최소화 하는 과정을 수행하였다. 이를 통해 기능의 통합, 기능을 수행하게 되는 물리적 구성품의 통합이 가능하게 되고 이것은 절대적인 인터페이스 숫자의 감소를 가능하게 한다. 그리고 이러한 인터페이스의 감소는 Systemic failure의 감축으로 이어진다. 위와 같은 과정을 대표적인 안전중시 시스템인 철도시스템에 적용하여 검증을 수행하였다.

본 논문에서의 연구결과와 적용사례를 통해 DSM 기반의 인터페이스 통합을 통한 Systemic failure의 감축을 달성할 수 있다는 것을 보여줬다. 향후에는 더욱 다양한 인터페이스 타입에 대한 DSM 적용 방안과 개념설계 단계에서 인터페이스가 최소화된 기능적, 물리적 아키텍처를 생성하는 방안에 대한 연구를 수행 할 필요가 있다.

6. References

[1] Road vehicles -- Functional safety --, International Organization for Standardization Standard, ISO 26262, 2011.

[2] C. A. Ericson, Hazard Analysis Techniques for System Safety. Hoboken, NJ: WILEY, 2005.

[3] Functional safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission Standard, IEC 61508, 2010.

[4] M. Gentile and E. Summers, "Random, systematic, and common cause failure: how do you manage them?," Process Safety Progress, vol. 25, no. 4, pp. 331-338, Dec. 30, 2006.

[5] Y.M. Chen, K.S. Fan, and L.S. Chen, "Requirements and functional analysis of a multi-hazard disaster-risk analysis system," Human and Ecological Risk Assessment, vol. 16, no. 2, pp. 413-428, Apr. 9, 2010.

[6] M. Bellotti and R. Mariani, "How future automotive functional safety requirements will impact microprocessors design," Microelectronics Reliability, vol. 50, no. 9-11, pp. 1320-1326, Sep. 30, 2010.

[7] Steven D. Eppinger and T.R. Browning, Design Structure Matrix Methods and Applications. The MIT Press, May 25, 2012.

ISSN 1229-6783(Print)
ISSN 2288-1484(Online)

저 자 소 개

정 호 전

현 아주대학교 시스템공학과 박사과정. 관심분야는 ,시스템 공학, 모델기반 시스템 공학, 시스템 안전(System Safety), 기능안전(Functional Safety), 시스템 안전관리체계(Safety Management System), 위험원 분석 및 식별, Modeling & Simulation 등.

주소 : 경기도 수원시 영통구 원천동 산5번지 아주대학교 성호관 244호

이 재 천

현 아주대학교 시스템공학과 정교수. 서울대학교 전자공학과에서 공학사, KAIST 전기 및 전자공학과에서 공학석사 및 박사 학위를 취득. 미국 MIT (Massachusetts Institute of Technology)에서 Post-Doc을 수행하였으며, 미국 Univ. of California (Santa Barbara)에서 초빙연구원, 캐나다 Univ. of Victoria (BC)에서 방문교수, KIST에서 책임연구원 재직. 이 후 미국 Stanford Univ. 방문교수 역임. 현재 연구 및 교육 관심분야는 시스템공학(SE), 모델기반 시스템공학 (MBSE), 시스템 안전(Systems Safety), 시스템 시험평가(Systems T&E) 및 다양한 산업 및 공공 분야에서의 SE 응용 등.

주소 : 경기도 수원시 영통구 원천동 산5번지 아주대학교 서관 309호