KOSHA GUIDE
X - 70 - 2016

운전원 행동분석(OAT)에 관한 기술지침

2016. 12

한국산업안전보건공단

안전보건기술지침의 개요

○ 작성자 : 충북대학교 안전공학과 임현교

○ 제·개정 경과

- 2016년 11월 리스크관리분야 제정위원회 심의(제정)

○ 관련규격 및 자료

- Hall, R.E., Fragola, J., Wreathall, J., NUREG/CR·3010, Post Event Human Decision Errors: Operator Action Tree /Time Reliability Correlation, USNRC, Washington, D.C., USA, 1982.
- IAEA-TECDOC-499, Models and Data Requirements for Human Reliability Analysis, Vienna, Austria, 1989.

○ 기술지침의 적용 및 문의

- 이 기술지침에 대한 의견 또는 문의는 한국산업안전보건공단 홈페이지(www.kosha.or.kr)의 안전보건기술지침 소관 분야별 문의처 안내를 참고하시기 바랍니다.
- 동 지침 내에서 인용된 관련규격 및 자료, 법규 등에 관하여 최근 개정본이 있을 경우에는 해당 개정본의 내용을 참고하시기 바랍니다.

공표일자 : 2016년 12월 19일
제 정 자 : 한국산업안전보건공단 이사장

KOSHA GUIDE
X - 70 - 2016

운전원 행동분석(OAT)에 관한 기술지침

1. 목 적

이 지침은 제어실 운전원을 대상으로 사고를 유발할 수 있는 직무 연쇄를 도출하고, 인지에러확률을 추정하는 운전원행동분석 (Operator Action Tree; OAT 또는 Operator Action Event Tree; OAET) 기법에 관한 기술적 사항을 정함을 목적으로 한다.

2. 적용범위

이 지침은 화학플랜트, 가스기지, 발전소, 기타 대형 제조사업장 등 제어실 운전원의 휴먼에러가 시스템의 사고발생에 중대한 영향을 미치는 감시 및 대응작업에 적용한다.

3. 용어의 정의

(1) 이 지침에서 사용되는 용어의 정의는 다음과 같다.

(가) “인간-기계 시스템(man-machine system)”이라 함은 인간과 도구, 기계, 설비 등으로 이루어진 모든 시스템을 말한다.

(나) “휴먼에러(Human error)”라 함은 인간이 수행하는 일련의 행동이나 행동군 중에서 수용 한계를 벗어난 행동, 즉 시스템의 정상적 기능을 위하여 정의된 인간의 행동 한계를 넘은, 감내할 수 없는 행동을 말한다.

주) 휴먼에러는 인지기능에 따라 다음 세 가지로 나뉜다.

① “행동 에러(slip)”란 자신이 의도한 대로 동작이나 행위가 이루어지지 않아 발생한 휴먼에러를 말한다.

② “기억검색 에러(lapse)”란 자신의 기억 속에서 특정 정보를 끄집어내지 못하여 발생한 휴먼에러를 말한다.

③ “의사결정 에러(mistake)”란 상황에 맞는 판단을 하지 못하여 발생한 휴먼에러를 말하다.

(다) “실행에러(commission error)”라 함은 인간이 업무를 수행하는 도중, 업무를 수행하기는 했으나 정해진 바에 따라 올바로 수행하지 못하여 발생한 휴먼에러를 말한다.

(라) “생략에러(omission error)”라 함은 인간이 업무를 수행하는 도중, 정해진 바에 따라 수행하여야 하는 행위를 수행하지 않아 발생한 휴먼에러를 말한다.

(마) “휴먼에러확률(Human error probability, HEP)”이라 함은 주어진 직무나 행동이 수행되었을 때 휴먼에러가 발생할 확률을 말한다. 동의어 human failure probability.

(바) “기본휴먼에러확률(Basic human error probability, BHEP)”이라 함은 독립된 직무를 수행할 때의 휴먼에러확률, 즉 선행직무의 영향을 받지 않을 경우의 휴먼에러확률을 말한다.

(사) “인간행동의 성공확률(Human success probability, HSP)”이라 함은 휴먼에러확률의 보수, 즉 1 - HEP를 말한다.

(아) “인간신뢰도(Human reliability)”라 함은 신뢰할 수 있거나 사용할 수 있는 시스템에 대하여 인간의 행동이 성공적으로 이루어질 확률을 말한다. 바꾸어 말하자면, 시스템의 신뢰도나 가용도를 훼손할만한 외적인 직무나 행동이 실행되지 않을 뿐만 아니라, 요구되는 시간 내에 시스템이 요구하는 인간행동, 직무, 또는 작업이 성공적으로 완수될 확률을 말한다.

(자) “인간신뢰도분석(Human reliability analysis, HRA)”이라 함은 인간신뢰도가 추정되는 방법을 말한다.

(차) “직무(Task)”라 함은 시스템의 목적이나 기능을 달성하는 데 기여하는 행동의 단위를 말한다.

(카) “개시사상(Initiating event)”이라 함은 사고연쇄의 발단이 되는 사상을 말한다.

(타) “의존(Dependence)”이라 함은 어떤 행동의 실패 (또는 성공) 확률이 다른 행동에서 발생한 실패 (또는 성공) 여부에 따라 달라지는 상황을 말한다. 두 행동은 동일인에 의하여 수행될 수도 있고, 다른 사람에 의하여 수행될 수도 있다.
주) 일반적으로 수학에서는 ‘종속’이라는 용어를, 확률통계학에서는 ‘의존’이라는 용어를 사용하는데, 의미상의 차이는 없다. 본 지침에서는 확률론적 이론에 따라 ‘의존’이라고 쓰기로 한다.

(파) “사상수목(또는 사상수, Event tree)”이라 함은 시스템 운전 중 수행되는 직무들을 나뭇가지 형태로 표현한 것을 말한다. 이 표현 안에서 사상들은 나뭇가지로 표현되고, 사상 연쇄는 시간에 따라 진행되는 것을 나타낸다 (KOSHA Guide P-87-2012 사건수 분석기법에 대한 기술지침 참조).

(2) 기타 이 지침에서 사용하는 용어의 정의는 특별한 규정이 있는 경우를 제외하고는 산업안전보건법, 같은법 시행령, 같은법 시행규칙 및 산업안전보건기준에 관한 규칙에서 정하는 바에 의한다.

4. 기법의 개요

4.1 개발의 배경

(1) 이 기법은 지나치게 사소한 작업요소들을 강조하는 THERP(Technique for Human Error Rate Prediction) 기법의 문제점을 극복하기 위하여, 1982년 John Wreathall 등에 의하여 개발되었다.

(2) 이 기법은 특정 개시사상(initiating event)에 대응하는 운전원의 행동을 체계적으로 구성하는 논리적인 기법으로, 이상 사태가 발생하였을 때 운전원이 반응하는 데 있어서 특히 중요한 직무들을 확인하는 데 유용하다.

4.2 기법의 특성

(1) 이 기법은 사고가 개시된 이후 원자력발전소 운전원의 인지, 진단 및 의사결정 에러에 초점을 맞추어져 있다.

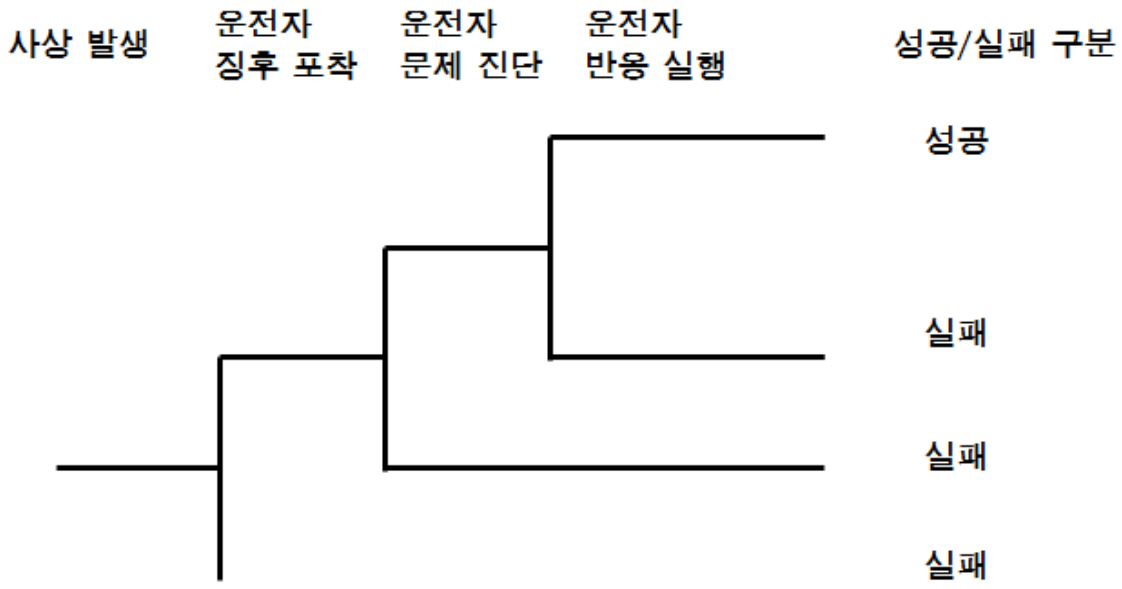
(2) 이 기법에서 이용되는 OAT(Operator Action Tree)는, 특정한 공정상의 사상을 당면하였을 때 운전팀이 수행할 것이라고 예상되는 다양한 의사결정과 행동의 연속을 표현한, 나무처럼 생긴 다이어그램이다.

(3) OAT 기법은 어떤 사상에 대한 인간의 반응이 <그림 1>에서 보는 바와 같이 다음 세 가지 단계로 설명될 수 있다고 하는 전제에 기반을 두고 있다. 즉, 휴먼 에러는 다음 세 가지 중 하나의 형태를 갖는다.

(가) 사상을 알아차리는 단계.
사고가 발생했다고 인지하는 단계에서의 에러. 인지에러.

(나) 사상을 진단하고 생각하는 단계
사건의 본질을 진단하고, 대응 조치를 확인하는 데 있어서의 에러. 진단에러.

(다) 사상에 반응하는 단계.
시기적절하게 필요한 대응 조치를 실행하는 데 있어서의 에러. 반응에러.



<그림 1> 기본적인 운전원 행동 수목의 예시 (NUREG/CR-3010)

주) 이 <그림 1> 하단에 '운전자 징후포착' 실패 이후에 가로선이 없는 것은, 운전자가 징후 포착에 실패했더라도, 그 이후에 여러 가지 후속조치가 있을 수 있음을 나타내기 위한 원저자(NUREG/CR-3010)의 의도를 나타낸다.

(4) 이 기법은 상황에 따라 크게 달라지는 행동형성요인 하에서의 개인행동을 설명하기보다, 일반화된 상황에 대응하는 운전원 집단의 통계적인 행동특성을 설명하는 것을 목적으로 한다.

(5) 이 기법은 특히 인지에러(cognitive error)에 중점을 두고 휴먼에러확률을 추정한다. 이런 에러들은, 관련 신호가 확인된 순간부터 성공적인 회복을 위하여 행동이 취해져야 할 시점까지라는 시간 간격의 함수로서 표현된다.

(6) 분석 결과로 얻어지는 휴먼에러확률(HEP)은 이후 사상수목분석(event tree analysis; ETA)이나 결함수목분석(fault tree analysis; FTA)에 이용된다 (KOSHA Guide P-84-2012 결함수분석, KOSHA Guide P-87-2012 사건수 분석기법에 대한 기술지침 참조).

5. 분석절차

5.1 기본흐름

OATS의 기본흐름은 다섯 단계로 구성된다. 각 단계에서의 상세한 분석 내용은 다음과 같다.

(1) 시스템의 안전확보를 위하여 분석 대상이 되는 사고 발생과 시스템의 대응 방법을 확인한다.
시스템에 이상이 발생하였을 때, 시스템을 안전하게 유지하기 위해서는 시스템의 어떤 기능을 어떻게 조작하여 대응하여야 하는가를 파악한다.

(2) 운전원에게 요구되는 대응 직무를 일련의 시나리오로 표현하여 사상수목(event tree)을 구성한다 (KOSHA Guide P-87-2012 사건수 분석기법에 대한 기술지침 참조).

(3) 운전원이 해당 직무를 수행함에 있어서 요구되는 경보 및 정보, 그리고 적절한 조치를 하는 데 쓸 수 있는 가용 시간 등을 나타내는 표시장치를 확인한다.

(4) 확률론적 안전성 평가를 위하여 사상수목(event tree)이나 결함수목(fault tree)에 휴먼에러를 표현한다.

(5) 휴먼에러확률을 추정한다.
<그림 2>의 가용시간-에러 확률 그래프를 이용하여 OAT의 휴먼에러확률을 결정한다.

최종적으로 추정된 휴먼에러확률은 이후 추가적인 분석에 활용될 수 있다.

5.2 휴먼에러확률의 추정

(1) 진단에 활용가능한 시간이 에러 확률을 결정짓는 결정적 요인이다. 즉, 짧은 시간이 주어진다면, 긴 시간이 주어졌을 때보다 상황을 올바로 진단하는 데 실패하기 쉬워진다. 그러므로, 휴먼에러확률의 추정은 의사결정을 하는 데 활용할 수 있는 시간과 밀접한 관계가 있다.

(2) 진단에 활용할 수 있는 시간(Thinking-Time)은 비정상적인 상황을 처음 인지하였을 때부터 선택된 반응을 개시할 때까지로 한정된다.
그러므로, 이 간격은 다음과 같이 표현될 수 있다.

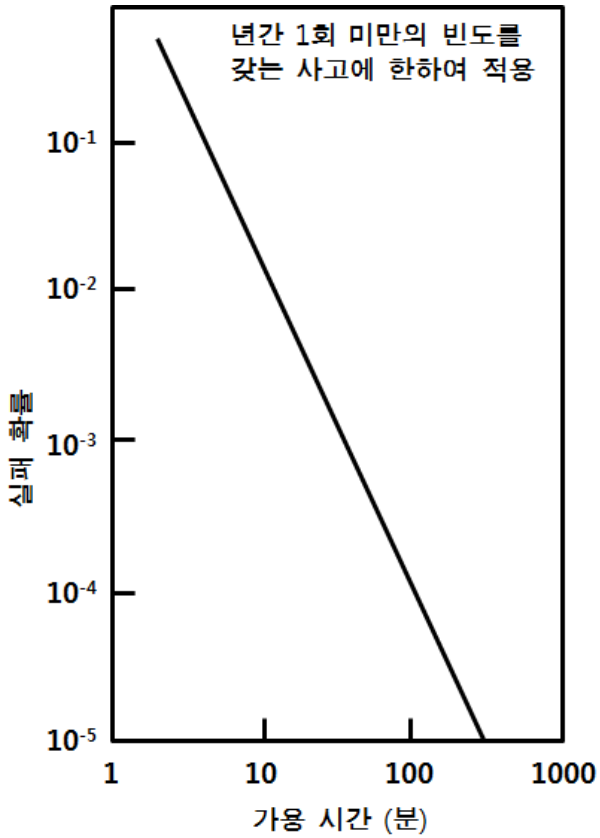
$$t_T = t_O - t_I - t_A$$

여기에서,
t_T : 운전원이 행동을 개시할 때까지 사용할 수 있는 시간
t_O : 사건 개시로부터 행동이 종료될 때까지의 시간
t_I : 사건 개시로부터 적절한 조짐이나 또는 신호가 감지될 때까지 경과된 시간
t_A : 결정된 계획을 실행하는 데까지 걸리는 시간.

즉, 운전원이 상황을 판단하고 의사결정을 하는 데 쓸 수 있는 시간 중, 사건 개시로부터 대응 행동의 종료시까지의 시간에서 신호가 감지될 때까지의 경과시간과, 운전원이 대응 행동을 하는 데 걸리는 동작시간(movement time)을 뺀 시간이라는 의미이다.

(3) 일단 활용할 수 있는 시간이 설정되면, <그림 2>과 같은 가용시간-에러 확률 그래프를 이용하여 에러 확률을 추정한다. 이 그림은 대수(log)-대수(log) 그래프로서, 에러 확률과 가용시간과의 관계를 입증하기 위하여 공학심리학자와 시스템분석가들에 의하여 개발되었는데, 1년에 1회 미만의 사고에만 적용될 수 있다.

그림에서 가로축은 운전원이 상황을 판단하고 의사결정을 하는 데 활용할 수 있는 시간을 나타내며, 세로축은 주어진 시간 동안에 올바른 판단을 내리지 못할 휴먼에러확률을 나타낸다.



<그림 2> 가용시간에 따른 휴먼에러확률 (NUREG/CR-3010)

6. 장·단점

6.1 장점

(1) 적용하기에 신속하고, 상대적으로 편리한 분석적 기법이다.

(2) 교육이 거의 필요 없을 만큼 상대적으로 쉬운 기법이다.

(3) 사상수목분석(Event Tree Analysis; ETA)과의 차이가 거의 없고 호환성이 커서 확률론적 안전성평가(Probabilistic Safety Assessment)나 인간신뢰도분석(HRA)에 널리 활용되어 왔다.

(4) OAT를 시각적으로 훑어봄으로써, 개시 사상에 반응하는 데 있어서 중대한 직무요소를 확인할 수 있다.

(5) 시스템의 초기 설계단계에서 다중 반응 대안 등 문제가 될 수 있는 직무스텝들이나, 치명적인 결과를 초래할 수 있는 휴먼에러의 잠재성이나 휴먼에러를 초래할 수 있는 직무스텝들을 강조하는 데 활용될 수 있다.

(6) 적절히 활용되면 시스템 운전 중에 발생할 수 있는 어떤 불상사든지 설명할 수 있다.

6.2 단점

(1) 복잡한 대규모 시스템에서는 수목이 엄청나게 대형화되고 복잡해진다.

(2) 적용하는 데 많은 시간이 소요된다.

(3) 결과상에 직무 스텝들이 설명되지 않는다.

(4) 잘못된 의도나 진단 에러(diagnosis error)를 확인하는 데에는 만족할 만한 기법이 아니다.

(5) 생략 에러를 나타내는 데 최적이지만 중요한 실행 에러 즉, 실행될 수 있는 대안 행동은 만족스럽게 포함되기 곤란하다.

(6) 모델링 과정에 사용되는 데이터가 완전하고 정확하다는 것을 보장하는 지원 수단이 없다. 그러므로, 최종적인 OAT의 정확성은 분석자의 경험에 좌우된다 (이것은 모든 인간신뢰성분석 기법에 공통되는 지적이다).

(7) 휴먼에러의 저감방법이나 근본원인을 발견하는 방법 등, 사고예방을 위한 대응 조치는 제시하지 않는다.

7. 적용상의 주의사항

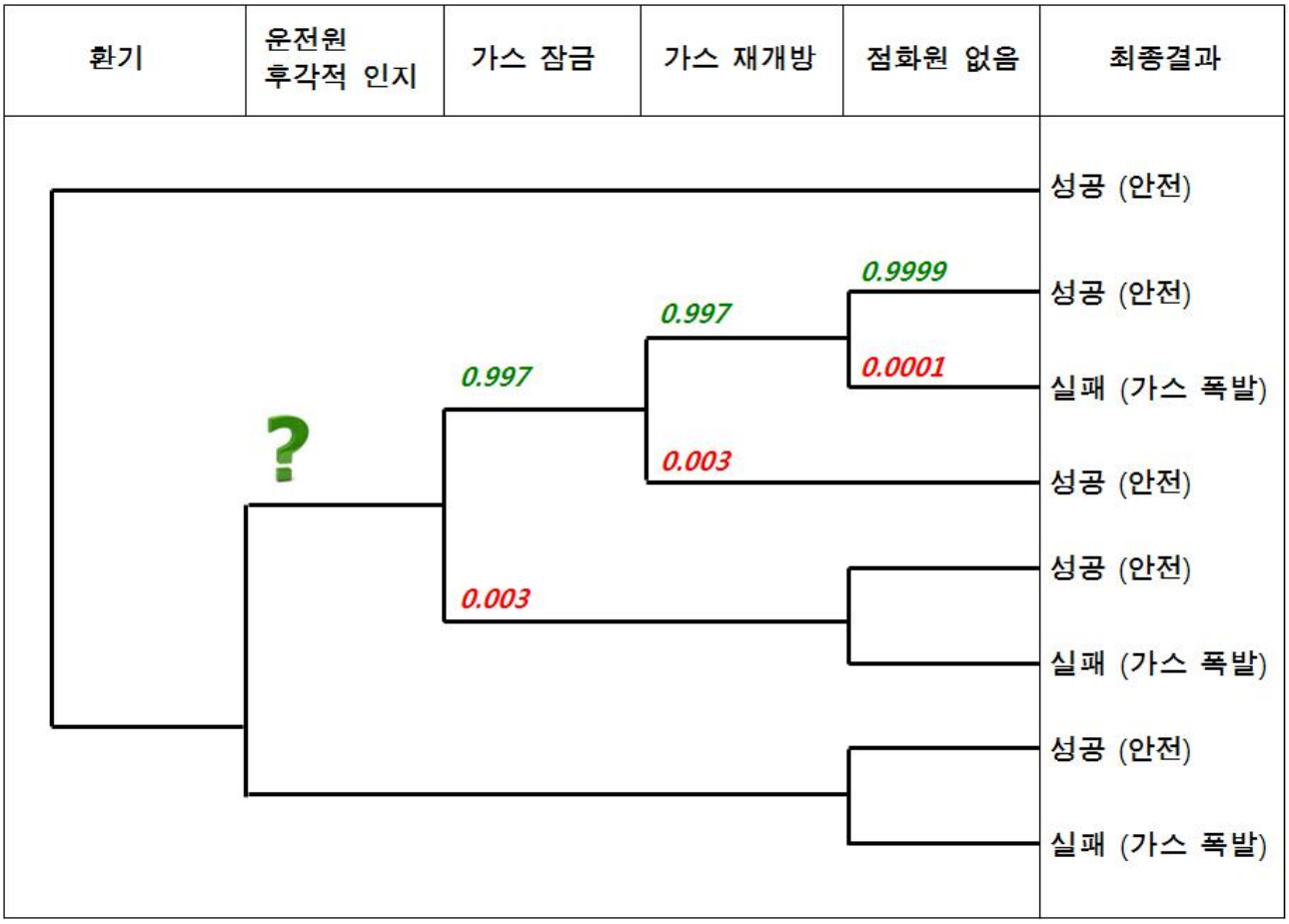
(1) 직무를 지나치게 세분하면, 상대적으로 다루기 어렵게 되기 때문에 수목구조를 통하여 사건 전개의 주요 흐름을 간파하는 것이 어려울 수 있다.

(2) 각 직무는 수목 구조 안에서 하나의 노드(node)로 표현되며, 각 직무의 결과는 노드로부터 벋어 나온 가지를 따라 '성공' 또는 '실패' 경로로 표현된다. 이런 식의 직무 표현은 대안 행동(실행 에러)이 어떻게 다른 중대한 상황을 일으킬 수 있는가는 설명하지 않는다. 그런 문제들을 극복하기 위해서는 각각의 실행 에러를 모델화하기 위하여 개별적인 OAT가 구성되어야 한다.

(3) OAT 기법이 인지에러의 확률을 예측할 수는 있다. 그러나, 어떤 예측값에 대하여 불확실성이 매우 높으며, 경험이나 스트레스가 진단이나 의사결정에 미치는 영향 같은 행동형성요인들의 잠재적 대규모 영향은 설명하지 못한다. 그래서 개발자들은 이 기법을 생략 에러(omission error)와 선별 분석(screening analysis)에 한하여 사용할 것을 권하고 있다.

<부록> OAT 분석 사례

그림 A.1은 로(furnace)에서 가스를 방출하는 데 따르는 사상들에 대한 사상수 분석(event tree analysis)을 나타낸다. 이 예에서는 가스 누출이 개시 사상이고, 폭발이 최종 위험요인이다.



<그림 A.1> 로(furnace)에서 방출되는 가스에 관한 사상수 분석의 예

그림 A.1에서 배기가 불충분하여, 운전원이 후각을 통해 탐지한 다음, "가스를 잠그다(Gas Turned Off)"라는 행동을 10분 이내에 수행하여야 할 때, 다른 요인들은 하드웨어의 고장률이나 통계적 데이터를 활용할 수 있으나, 운전원의 인지 에러확률은 쉽게 구할 수 없다.

이 때 OAT를 아용하면, <그림 2>로부터 $F_{10}=10^{-2}$이므로 운전원의 후각적 인지 성공확률은 $P_{10}=1-F_{10}=1-10^{-2}=0.99$라는 결과를 얻을 수 있다.

이 값을 그림에 대입하여 사상수 분석을 진행하면 (다른 직무의 휴먼에러확률은 NUREG/CR-1278 참조, 점화원 유무확률은 임의), 운전원의 후각적 인지, 가스 잠금 및 재개방, 점화원 없음의 과정을 거쳐 성공적으로 작업이 수행될 확률은 다음과 같다.

$$0.99 \times 0.997 \times 0.997 \times 0.9999 = 0.9840$$

만약 허용된 시간이 100분이라면 $F_{100} = 10^{-4}$이고 성공확률은 $P_{100} = 1 - F_{100}$ $P_{100} = 1 - F_{100} = 1 - 10^{-4} = 0.9999$가 된다. 따라서, 성공적인 작업수행확률은 다음과 같다

$$0.9999 \times 0.997 \times 0.997 \times 0.9999 = 0.9938$$

이 결과는 다른 직무들에 대한 신뢰도 및 고장확률과 함께 확률론적 안전성평가(PSA)에 활용된다.