2001 추계학술발표회 논문집
한국원자력학회

유한상태기계 기반의 소프트웨어요구명세 표현 방법

A Method of SRS Representation based on the Finite State Machine

서용석, 장귀숙, 서상문, 금종용, 이종복
한국원자력연구소

요 약

임의의 시스템으로부터 유한개의 상태와 상태간의 천이가 도출된다면 그 시스템은 유한상태기계로 표현될 수 있으며 이는 자연어로 표현되는 것보다 그 시스템의 행위가 일관되게 해석될 수 있다. 본 논문은 SMART 정보처리계통의 경보표시를 위한 소프트웨어요구명세를 유한상태기계의 표현규칙을 근간으로 작성하였다. 이는 소프트웨어 개발자에게 자연어로 작성된 명세보다 명확하게 소프트웨어요구명세 내용을 이해시킬 수 있었다. 경보표시요건이 확장되어도 유한상태기계의 표현규칙이 유용함에 대해 추가적인 연구가 필요하다.

Abstract

If a finite number of states and transitions between the states are figured out from a system, the system can be represented with the finite state machine so that its behavior can be interpreted more consistently than the representation with natural language. The software requirement specification for alarm display of the information processing system for SMART represented with the finite state machine is presented in this paper. The specification was easily understood by a software programmer than that of natural language. Even if the requirements of the alarm display are extended more, to show that the representation method of software requirement specification is still useful is remained in further study.

1. 서론

일체형원자로형(type)인 SMART의 MMIS(Man-Machine Interface System)에 적용되는 소프트웨어 수명주기(SDLC)에서 소프트웨어요구명세서(SRS) 작성은 필수적인 과정이다[1]. 소프트웨어요구명세서는 계통 설계자와 소프트웨어 개발자의 의사소통 수단으로써 가장 우선적으로 참조되는 문서이다. 소프트웨어 개발자는 소프트웨어요구명세서를 기반으로 하여 소프트웨어 구조를 설정하고 모듈을 프로그래밍 한다. 그러므로 계통 설계자는 자신의 계통에서 요구하는 소프트웨어 개발 요구사항을 분석하여 소프트웨어 개발자가 이해할 수 있는 형태와 내용으로 소프트웨어요구명세서를 작성하여야 한다. 소프트웨어요구명세서를 통해 생산하려는 최종 결과물인 소프트웨어에 대한 계통 설계자의 요구사항과 이에 대한 소프트웨어 개발자의 개발관점에서의 이해관계를 일치시킴으로써 계통 설계자의 만족도 기준에 부합하는 소프트웨어가 최종적으로 산출되고 인수될 수 있게 한다[2].

소프트웨어요구명세서는 자연어(natural language), 정형언어(formal language), 의사어(pseudo code), 알고리즘(algorithm), 다이어그램(diagram) 등의 여러 형태로 작성될 수 있는데 어느 형태를 사용할 것인가에 대해서는 요건 및 시스템의 복잡도에 따라 적절한 평가가 이루어진 후 명세기법을 선정하여야 할 것이다.

자연어로 작성된 소프트웨어요구명세는 제 삼자로부터 해석의 일관성을 유지할 수 없는 것은 사실이다. 수학적 증명이 가능케 하려는 정형언어는 구문과 의미의 전달이 아직까지 일반화되어 있지 못하여 사용자에게 친숙하지 못하다. 의사어 또는 알고리즘은 계통 설계자보다는 소프트웨어 개발자에게 친숙하므로 소프트웨어설계명세를 작성하는데 유용하다. 명세를 다이어그램 형태로 작성하는 방법이 사용자에게 친숙하며 CASE(Computer Aided Software Engineering) 도구 역시 다이어그램 형태의 표현을 가능케 하는 도구이다. 본 논문은 소프트웨어요구명세를 다이어그램 형태로 작성하는 방법으로써 유한상태기계의 개념을 사용한다. 이는 명세의 내용이 프로그래머에게 규칙적으로 해석되게 하고 일관되게 알고리즘으로 변환이 가능하도록 하기 위함이다. 본 논문은 2장에서 유한상태기계 개념을 검토하며, 3장에서 유한상태기계 개념을 바탕으로 상태천이도와 상태천이테이블을 이용하여 소프트웨어요구명세를 작성하며, 4장에서 작성된 결과를 검토하며, 5장에서 결론을 맺는다.

2. 유한상태기계

2.1 정의

본 논문에서 제시하는 소프트웨어요구명세 표기법은 결정론적 유한상태기계(또는 유한오토마타라고 한다.)를 따른다. 결정론적 유한상태기계인 DFSM(Deterministic Finite State Machine)은 다음과 같이 5개의(quintuple) 요소로 정의된다[3]:

DFSM = (Q, Σ, δ, q_0, F)

Q : 유한개의 내부 상태 집합을 의미한다. 상태천이도에서 원(circle)으로 표시된다.

Σ : 유한개의 입력을 의미한다. 즉, 입력되는 사건을 의미한다.

δ : Q × Σ → Q 즉, 천이함수를 의미한다. 상태천이도에서 아크(arc)로 표시된다.

q_0 : $q_0 \in Q$ 즉, 초기 상태를 의미한다.

F : F ⊆ Q 즉, 최종 상태 집합을 의미한다.

DFSM 정의를 다이어그램(diagram)으로 도식하면 상태천이도(예, 그림 1)가 되며 테이블로 표현하면 상태천이테이블(예, 표 1)이 된다. 본 논문은 상태천이도와 상태천이테이블을 이용하여 소프트웨어요구명세를 작성하는 방법을 제시한다. DFSM에서 결정론적을 만족하는 전제조건은 모든 상태는 적어도 하나 이상의 천이가 발생되도록 아크(arc)가 연결되어야 하며 각 상태는 하나의 입력에 대해 하나의 천이만이 발생되도록 유일한 천이조건이 설정되어야 한다. 상대적으로 비결정론적 유한상태기계는 천이가 없는 상태를 허용하거나, 동일한 조건으로 서로 다른 상태로 천이를 허용하거나, 최초 입력이 null 또는 empty인 경우에도 천이가 이루어지도록 한다. 응용 범위에 따라 비결정론적 유한상태기계가 더 유용할 수 있으나 이에 대한 상세한 언급은 본 논문에서 제외한다.

2.2 의미

컴퓨팅 시스템의 계산은 새로운 입력에 의해 상태가 천이되는 과정의 연속이라 할 수 있다. 이러한 천이과정을 다이어그램 형태로 표현하려는 표기법들로써 페트리넷(Petri net), 스테이트챠트(Statecharts), 마코프연쇄(Markov chain), 객체지향설계기법의 UML(Unified Modeling Language)의 use case, 구조적설계기법의 DFD(Data Flow Diagram) 등을 들 수 있으며 이들의 표기법은 DFSM을 확장한 상태천이도와 유사하나 의미(semantics)에서 차이를 보여준다. 본 논문에서 제시하는 소프트웨어요구명세 표현방법은 근본적으로 DFSM의 상태천이도의 의미를 따른다. 본 논문의 상태천이도에는 토큰(token)이 표시된다. 시스템이 기동되어 정지될 때까지 항상 하나의 토큰이 임의의 상태에 존재한다. 토큰이 상태 사이를 이동하는 천이규칙(fire rule)은 다음과 같다:

가) 시스템이 기동되어 최초의 입력이 발생하면 토큰을 초기상태에 부여한다.

나) 다음에 입력되는 사건부터는 사건이 발생할 때마다 아래의 다)와 라)를 무한히 반복한다.

다) 천이 조건을 만족하면 다음 상태로 토큰이 이동된다.

라) 그렇지 않으면 현재 상태에서 토큰이 머무른다.

위 천이규칙에는 시간제약(timing constraint)이 없다. 즉, 주기적이든 비주기적이든 사건이 입력되면 즉시 천이 조건을 검사하여 만족되면 즉시 토큰이 이동된다.

2.3 상태천이도 도식 절차

상태천이도 도식을 위해서는 상태정의구역(state domain) 즉, 유한한 상태의 분류가 관건이다. 이것은

그 시스템의 행위(behavior)에 대한 시나리오를 전개하면서 상태를 반복적으로 추출과 정제(refining)해 나가는 방법을 통해 이루어진다. 본 논문의 소프트웨어요구명세의 상태천이도 도식은 먼저 가) 상태정의 구역으로부터 개별적 상태를 분류하고, 2) 상태천이도에 입력되는 사건을 분류하고, 3) 천이조건을 분류한 후, 각각의 상태를 아크로 연결하는 과정을 통해 이루어진다. 상태천이도가 도식되면 각각의 아크를 명확히 설명하는 즉, 천이조건을 설명하는 상태천이테이블을 작성한다.

3. 소프트웨어요구명세 작성

본 논문은 SMART 정보처리계통의 경보표시를 예로 선정하여 소프트웨어요구명세를 작성한다. 디지틀 시스템으로 설계되는 정보처리계통의 경보기능은 불필요한 경보를 감축하는 경보처리기능과 경보의 위급성별로 구분하여 표시하는 경보표시기능으로 구분된다. 본 논문은 경보표시기능에 대한 소프트웨어 요구명세를 작성하며 경보처리기능은 추후 요건을 확정하여 작성할 것이다.

3.1 요건도출

과학기술부령 원자로시설 등의 기술기준에 관한 규칙 제38조에서 언급하고 있는 “방사선량률이 현저하게 상승한 때에 이들을 검출하여 자동적으로 경보하는 장치를 설치하여야 한다.”로부터 SMART 주제어실에 설치되는 정보처리계통에게도 경보를 발생하는 임무를 부여함으로써 정보처리계통의 경보표시에 대한 상위요건을 설정한다. SMART MMIS 설계개념[4]으로부터 “경보표시는 VDU(Visual Display Unit) 장치를 통해 경보를 우선순위로 구분하여 표시함으로써 위급한 경보를 운전원이 즉시 인지하도록 한다.”를 정보처리계통의 경보표시기능에 대한 요건으로써 설정한다. 정보처리계통에서 표시하는 미믹(mimic) 그래픽개체의 경보표시에 대한 상세설계요건을 다음과 같이 요약하였다.

가) 운선순위 1 경보(이하 P1이라 한다.)는 입력공정값이 P1 설정치를 벗어나면 이를 운전원이 5분 이내에 인지하여 적절한 조치를 취하도록 발생하며 경보표시는 주홍색으로 초당 3회 균등점멸한다.

나) 운선순위 2 경보(이하 P2라 한다.)는 입력공정값이 P2 설정치를 벗어나면 이를 운전원이 15분 이내에 인지하여 적절한 조치를 취하도록 발생하며 경보표시는 황갈색으로 초당 3회 균등점멸한다.

다) 운선순위 3 경보(이하 P3라 한다.)는 입력공정값 상태가 bad-data 또는 out-of-range이면 운전원이를 인지하도록 발생하며 경보표시는 흰색으로 초당 3회 균등점멸한다.

라) 운전원이 점멸되고 있는 경보의 점멸을 멈추게 하는 행위를 경보 인지행위(acknowledgement, 이하 ACK라 한다.)라 정의하며 이를 ACK된 경보상태라 한다. ACK된 경보상태는 점멸을 멈추고 경보색을 표시한다. 운전원이 ACK하지 않은 점멸 경보는 입력값이 정상상태로 회복되어도 계속 경보색으로 점멸을 유지한다.

마) 운전원이 ACK한 경보가 정상상태로 회복되었을 때 이를 운전원이 인지하도록 하는 개념을 링백

(ringback)이라 정의하며 이를 해제된(clear, 이하 CLR이라 한다.) 경보상태라 한다. CLR된 경보상태를 운전원이 리셑(reset, 이하 RST라 한다.)행위를 하면 그 경보는 정상상태를 표시한다. CLR된 경보상태는 초당 1회 경보색을 점멸한다.

바) 우선순위가 낮은 경보상태에서 우선순위가 높은 경보가 발생하면 우선순위가 높은 경보표시를 할 수 있으나 우선순위가 높은 경보상태에서는 반드시 그 경보에 대해 운전원이 ACK행위를 한 후 우선순위가 낮은 경보표시를 할 수 있다.

사) ACK된 경보상태에서 새로운 입력값에 의해 CLR된 경보상태 또는 우선순위가 더 낮은 ACK 안된 경보상태를 표시할 수 있다.

아) CLR된 경보상태에서 운전원의 RST행위에 의해 정상상태 또는 우선순위가 더 낮은 ACK된 경보상태를 표시할 수 있다.

자) 운전원이 ACK버튼을 누른 순간에 입력값이 정상이 되었다 하여도 우선 ACK된 경보상태를 표시하고 다음 처리시간에 CLR된 경보상태를 표시한다.

3.2 상태천이도 도식

상태천이도 도식을 위해서는 자연어로 기술된 요건으로부터 상태를 분류하는 것이 핵심적인 기술이다. 위 3.1절의 경보표시 상세설계요건으로부터 상태정의구역, 사건, 천이조건, 행위를 다음과 같이 도출할 수 있다:

가) 상태정의구역 : 정상상태, P1, P2, P3, ACK된 경보상태, CLR된 경보상태

나) 사건 : 입력공정값 또는 상태, 운전원 행위

다) 천이조건 : 설정치 비교, bad-data 또는 out-of-range, ACK 또는 RST 운전원 행위

라) 행위 : 색깔 표시와 점멸여부

이와 같이 도출된 정보를 바탕으로 그림 1과 같이 상태천이도를 도식하였다. 그림 1의 상태천이도는 3.3절의 상태천이테이블을 통해 이해될 수 있다.

3.3 상태천이테이블 작성

그림 1의 상태천이도에서 아크(즉, 천이)부분을 구체적으로 설명한 것이 표 1의 상태천이테이블이다. 표1에서 From은 현재 상태이며 To는 천이될 수 있는 다음 상태를 의미한다. 표1은 From상태에서 To 상태로 전이될 수 있는 조건을 모두 표시하였다. C는 입력공정값 또는 입력공정값의 상태를 의미한다. C가 정상범위 내라는 것은 가장 우선순위가 낮은 경보설정치를 범하지 않는 범위에 C가 속해있다는 의미이다. X는 천이가 발생되지 않음을 의미한다. 각각의 상태에서 경보표시행위는 3.1절의 상세설계요건으로부터 쉽게 알 수 있다. 예를 들어, P1 경보상태에 대한 경보표시행위는 초당 3회 주홍색을 점멸하며 P1-ACK 경보표시는 주홍색을 표시하며, P1-CLR 경보표시는 초당 1회 주홍색을 점멸한다. 정상상태

표시는 미믹의 성격에 따라 다를 수 있으며 이는 화면표시요건에서 취급하는 내용이므로 본 논문에서 언급하지 않는다.

3.4 데이터베이스

정보처리계통에서 경보표시를 해야하는 모든 변수는 데이터베이스에 등록되어야 한다. 표2는 데이터베이스 필드의 예를 보여준다. 표2에서 ringback은 링백개념 적용여부를 나타낸다.

표 2 : 데이터베이스 필드 예

변수이름	ringback	P1저설정치	P2저설정치	P2고설정치	P1고설정치

데이터베이스에 작성된 내용에 따라 상태천이도의 적용범위가 달라질 수 있다. 예를 들어, ringback 필드 값이 0이고 P2 경보상태만 표시하는 변수에 대해서는 그림 2와 같이 간단한 상태천이가 발생할 것이다. 그림 2는 그림 1의 부분집합이 된다.

4. 검토

자연어로 작성된 상세설계요건을 상태천이도와 상태천이테이블로 표현함으로써 상세설계요건에 대한 해석이 유일(unique)하게 되었음을 알 수 있다. 이것은 상태의 수를 제한했고 천이조건을 명확히 했기 때문에 가능하다. 프로그래머는 알고리즘을 작성하기 위해서 자연어를 어떤 식으로든 해석해야만 할 것이다. 그 해석을 도와주는 역할을 CASE 도구가 담당하는데 대부분의 CASE 도구가 상태천이 중심으로 표현하도록 도와준다. 따라서 본 논문에서 제시하는 표현방법이 근본적으로 CASE 도구가 지원하는 표현방법을 벗어나지 않는다. 프로그래머에게 자연어로된 3.1절의 상세설계요건과 3.2절의 상태천이도 및 3.3절의 상태천이테이블을 함께 설명하였을 때 상호이해가 쉽게 도달할 수 있었다. DFSM을 적용하는데 있어서의 제한조건은 컴퓨팅 시스템으로 구현하고자 하는 대상을 유한개의 상태로 분류할 수 있는가 하는 것이다. 실세계에서 일어나는 모든 행위와 변화를 상태천이도로 표현할 수는 없겠으나 SMART MMIS 컴퓨팅 시스템에서 구현하고자 하는 요건은 유한개의 상태로 분류가 가능할 것이다.

본 논문에서 예제로 삼은 정보처리계통 경보표시요건이 확장되었을 경우에도 상태천이도 및 상태천이테이블로 표현이 가능한 가를 고려할 필요가 있다. 경보표시요건의 확장 예로써, 경보 cut-out, time-delay, variable setpoint, 평균편차, 고유함수 등을 들 수 있는데 이들 가운데 천이조건에 반영이 가능한 요건도 있고 경보표시 이전에 경보처리 부분에서 처리하도록 하여야 하는 요건도 있다. 추후, 이들 요건을 반영하기 위한 상태천이도 및 상태테이블 작성방법을 확장할 것이다.

상태천이테이블을 작성하면서 기능시험에서 확인하여야 할 항목들이 자연스럽게 도출됨을 알 수 있었다. 상태천이테이블을 통해 천이가 일어나야 하는 조건과 천이가 일어나지 말아야 하는 조건을 시험항

목(test case)으로 작성할 수 있을 것이다.

본 논문은 제한된 요건으로 비롯해 기본적인 상태천이도와 상태천이테이블을 작성하였다. 복잡한 요건에 DFSM을 적용하는 것은 한계가 있을 것이며 따라서 확장된 모델이 필요할 것이다. 또한 본 논문에서는 CASE 도구를 사용하지 않았으나 소프트웨어요구명세 작성에 CASE 도구를 사용하는 것이 효율적일 수도 있다. 상용 CASE 도구는 자체적으로 풍부한 기능과 의미를 제공하려 하고 또한 높은 제품가격 때문에 사용자가 쉽게 접근할 수 없는 단점과 어려움이 있다. 그러나 수작업으로 상태천이도와 상태천이테이블을 작성하는 것은 한계가 있으므로 CASE 도구를 이용한 표현방법을 고려할 필요가 있다.

5. 결론

본 논문은 SMART 정보처리계통의 경보표시를 위한 상세설계요건으로부터 소프트웨어요구명세를 유한상태기계의 표현규칙을 근간으로 작성하였다. 이는 자연어로된 상세설계요건과 함께 상태천이도 및 상태천이테이블을 프로그래머에게 설명하였을 때 상호이해가 쉽게 도달되었음을 알 수 있었다. 본 논문에서 제시한 상태천이도 및 상태천이테이블을 이용하여 소프트웨어요구명세 작성방법을 정보처리계통 전체에 적용가능한 가에 대해 추후 연구할 것이다. 이를 통해 확장된 요건에 유한상태기계의 표현규칙 적용 가능성이 검토될 것이다.

Acknowledgement

본 연구는 과학기술부의 원자력연구개발사업 일환으로 수행되었음.

[참고문헌]

1. 서용석 외, "SMART MMIS 설계에 적용을 위한 소프트웨어 개발 개념", 2000춘계원자력학회 학술발표회, 2000. 5.
2. IEEE 830, "IEEE Recommended Practice for Software Requirements Specifications", 1998.
3. Peter Linz, "An Introduction to Formal Languages and Automata", D.C. Heath and Company, 1990.
4. KAERI/RR-1901/98, “일체형원자로 MMIS설계기술개발”, 한국원자력연구소, 1999. 3.

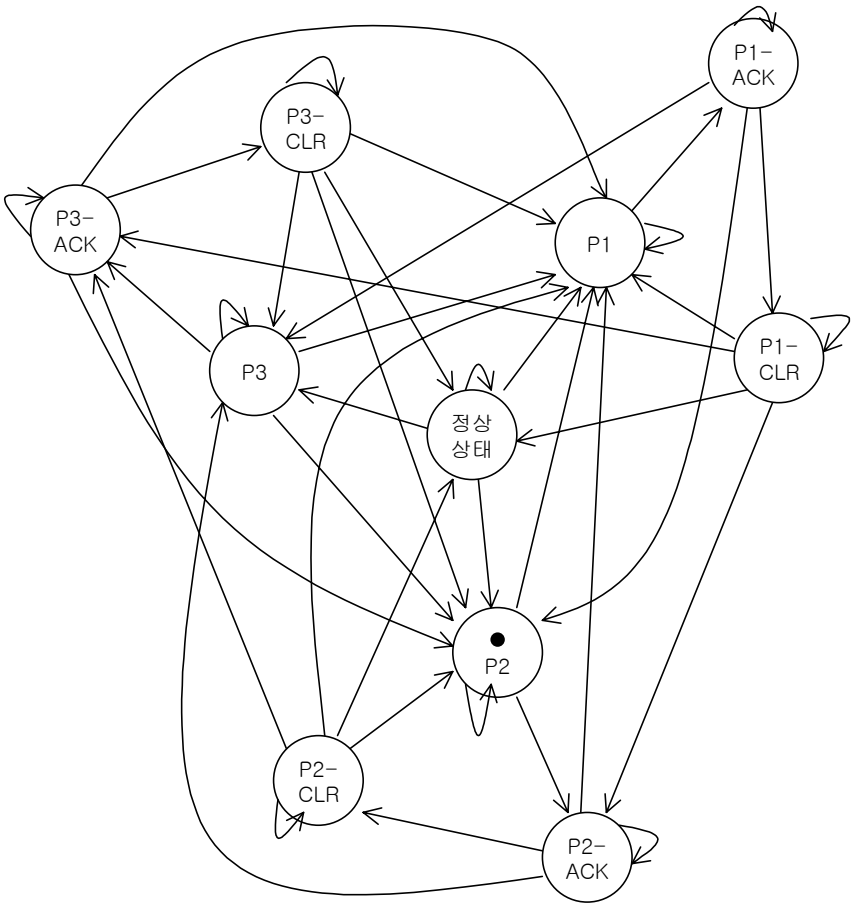

그림 1 : 상태천이도 예 1

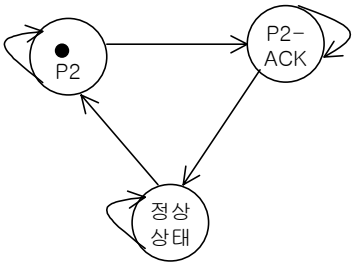

그림 2 : 상태천이도 예 2

표 1 : 상태천이테이블

To / From	정상상태	P3	P3-ACK	P3-CLR	P2	P2-ACK	P2-CLR	P1	P1-ACK	P1-CLR
정상상태	C가 정상범위 내임	C가 bad-data 또는 out-of-range	X	X	C<=P2저설정치 또는 C>=P2고설정치	X	X	C<=P1저설정치 또는 C>=P1고설정치	X	X
P3	X	C가 bad-data 또는 out-of-range	운전원이 ACK 함	X	C<=P2저설정치 또는 C>=P2고설정치	X	X	C<=P1저설정치 또는 C>=P1고설정치	X	X
P3-ACK	X	X	C가 bad-data 또는 out-of-range	C가 정상범위 내임	C<=P2저설정치 또는 C>=P2고설정치	X	X	C<=P1저설정치 또는 C>=P1고설정치	X	X
P3-CLR	운전원이 RST 함	C가 bad-data 또는 out-of-range	X	C가 정상범위 내임	C<=P2저설정치 또는 C>=P2고설정치	X	X	C<=P1저설정치 또는 C>=P1고설정치	X	X
P2	X	X	X	X	C<=P2저설정치 또는 C>=P2고설정치	운전원이 ACK 함	X	C<=P1저설정치 또는 C>=P1고설정치	X	X
P2-ACK	X	C가 bad-data 또는 out-of-range	X	X	X	C<=P2저설정치 또는 C>=P2고설정치	C가 정상범위 내임	C<=P1저설정치 또는 C>=P1고설정치	X	X
P2-CLR	운전원이 RST 함	X	C가 bad-data 또는 out-of-range	X	C<=P2저설정치 또는 C>=P2고설정치	X	C가 정상범위 내임	C<=P1저설정치 또는 C>=P1고설정치	X	X
P1	X	X	X	X	X	X	X	C<=P1저설정치 또는 C>=P1고설정치	운전원이 ACK 함	X
P1-ACK	X	C가 bad-data 또는 out-of-range	X	X	C<=P2저설정치 또는 C>=P2고설정치	X	X	X	C<=P1저설정치 또는 C>=P1고설정치	C가 정상범위 내임
P1-CLR	운전원이 RST 함	X	C가 bad-data 또는 out-of-range	X	X	C<=P2저설정치 또는 C>=P2고설정치	X	C<=P1저설정치 또는 C>=P1고설정치	X	C가 정상범위 내임