Software V&V for the SDLC of the HANARO Control Computer

Min Woo Lee, Yun Teak Yim, Seung Kyoo Doo, Yeong San Choi, Hyung Kyoo Kim, Sung Hyo Lee

(leemw@kaeri.re.kr)

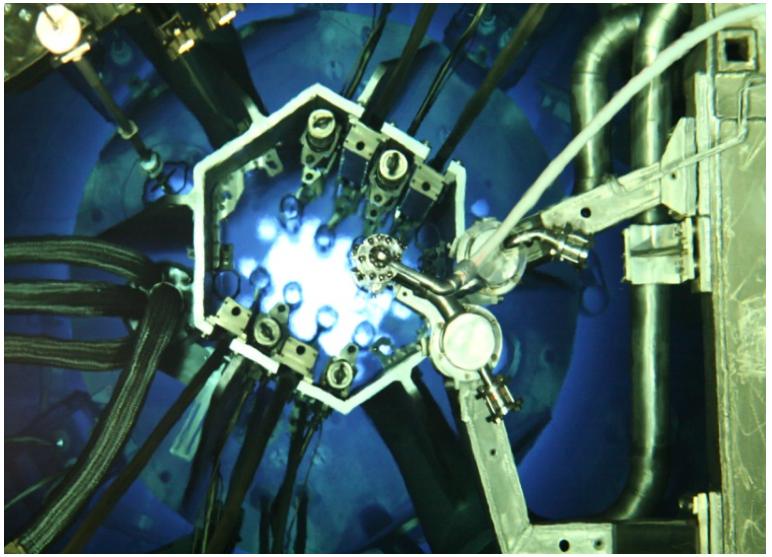
18 May. 2017

KAERI Korea Atomic Energy Research Institute

CONTENTS

Overview _ HANARO

(High-Flux Advanced Neutron Application Reactor)



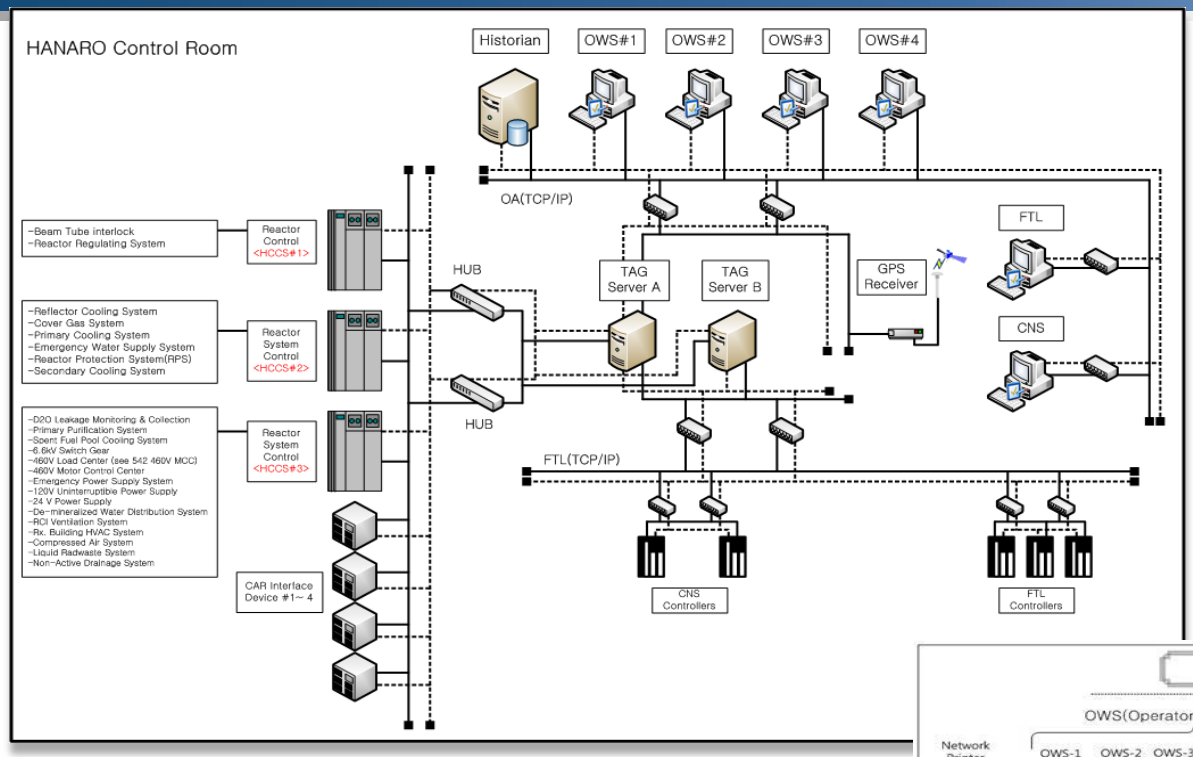
Type	Open-tank-in-pool
Thermal power	30 MWth
Coolant	Light Water
Reflector	Heavy Water
핵연료 및 농축도	U_3Si, 19.75% (금속 연료)
핵연료 피복재	알루미늄
원자로 정지 기능	제어봉, 정지봉
원자로 건물	준격납건물(Confinement)
최대 열중성자속	$5x10^{14}$ n/cm^2s
조사공	7 개의 수평공, 36 개의 수직공
운전주기	28일(연간 200일 운전)

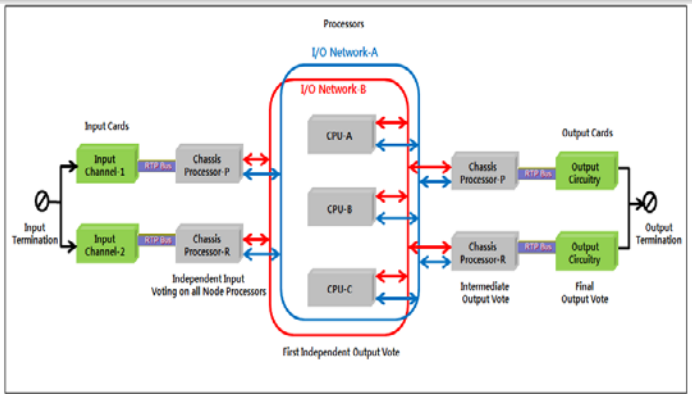
Overview _ Control Computer

- 하나로 제어컴퓨터
  - ✓ 하나로의 출력제어
  - ✓ 운전에 필요한 변수표시, 데이터 수집
  - ✓ 공정계통의 경보, 추세기록

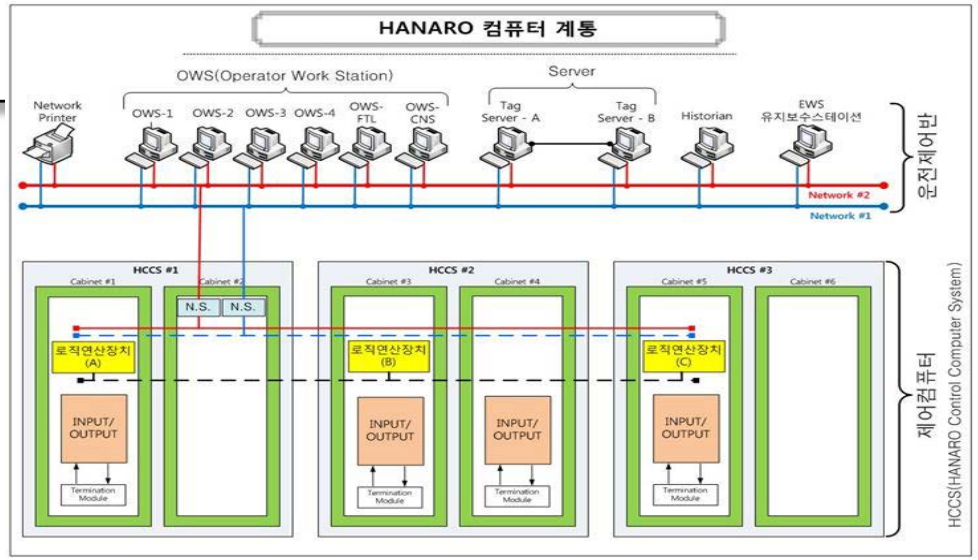
- 하나로 제어컴퓨터의 구성
  - ✓ 제어컴퓨터
    - 원자로출력제어
    - 공정 계측제어
    - 보조계통 계측제어
  - ✓ 운전 제어반
    - 원자로 및 각종 공정계통을 제어하는 인터페이스
  - ✓ 제어봉 인터페이스 장치
    - 제어봉 구동신호 발생
    - 스텝에러를 제어컴퓨터에 전달

Overview _ Configuration of Control Computer





Configuration of CPU & I/O



Overview _ Replacement of Control Computer

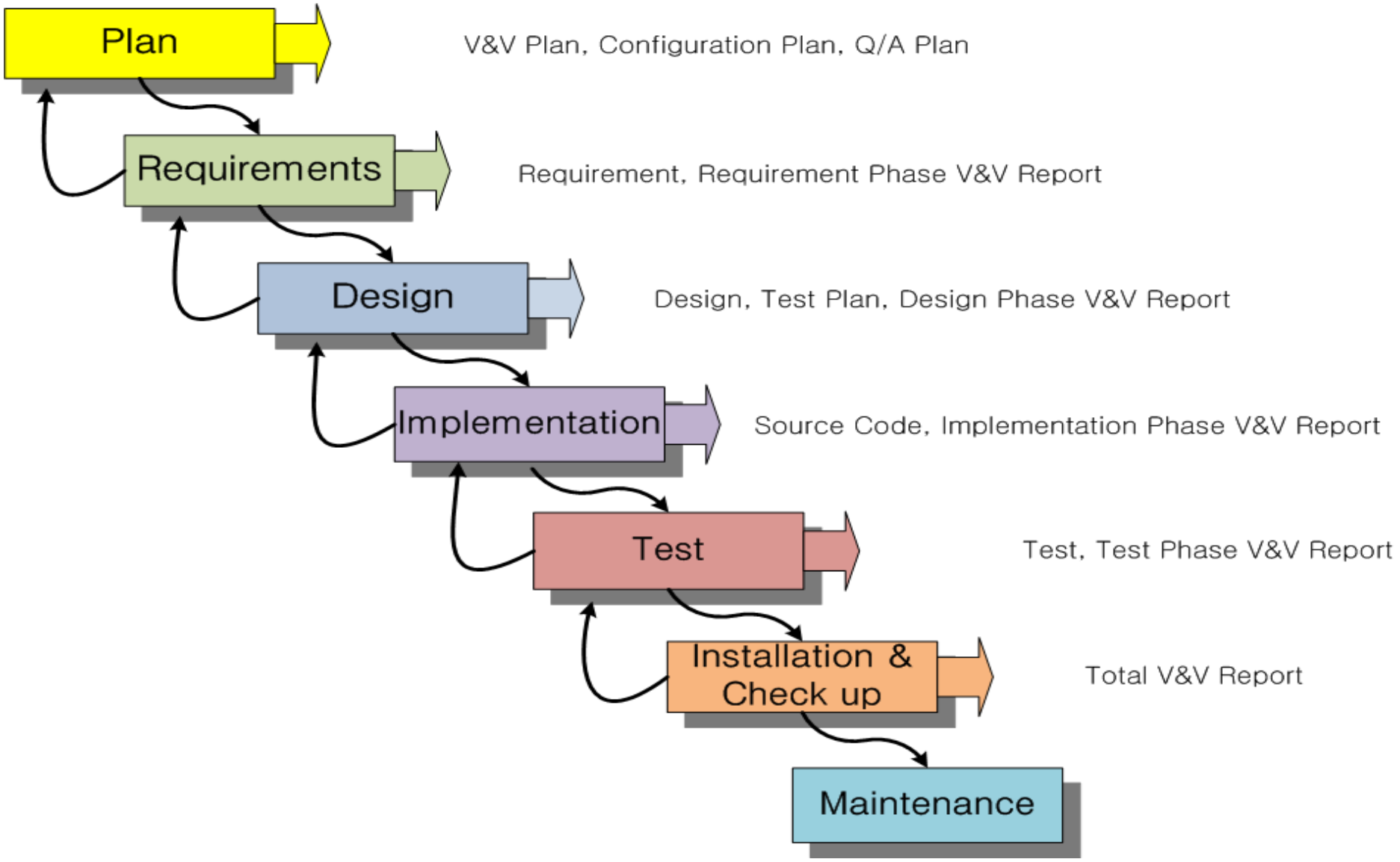
제어컴퓨터 교체 전

제어컴퓨터 교체 후

제어봉 인터페이스 장치 교체 전

제어봉 인터페이스 장치 교체 후

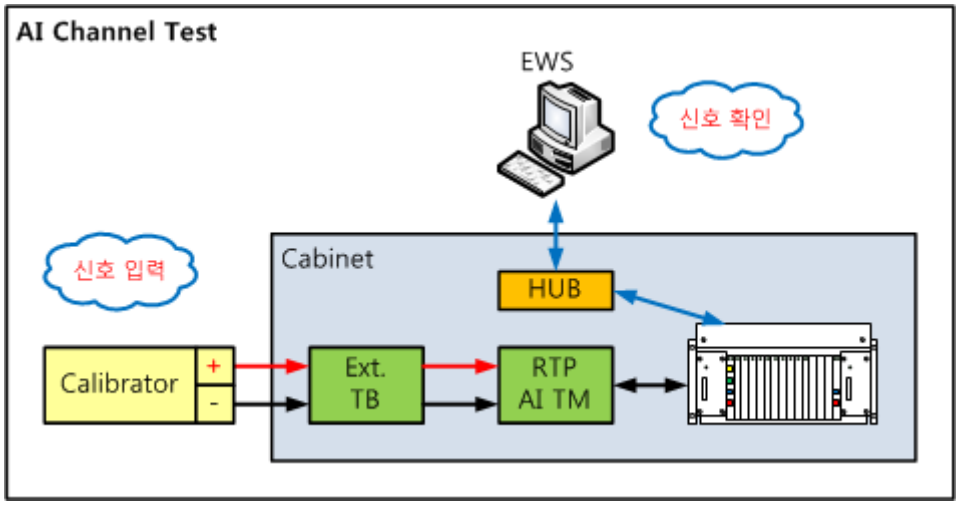
SDLC(Software Development Life Cycle)



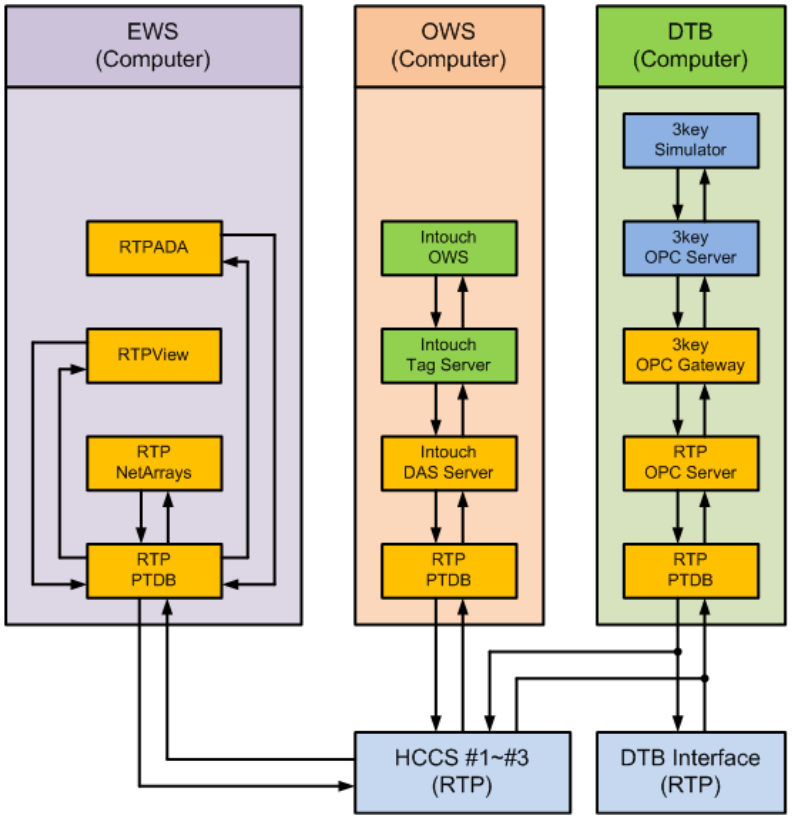
V&V(Verification & Validation)

단계	V&V 업무	입력물	출력물
요건 단계	– 소프트웨어 요건 분석 – 소프트웨어 요구사항 추적성 분석	기술시방서 SRS	요건단계 V&V Checklist 및 RTM
설계 단계	– 소프트웨어 설계 분석 – 소프트웨어 설계 추적성 분석	SDD	설계단계 V&V Checklist 및 RTM
구현 단계	– 소스코드 분석 – 소스코드 추적성 분석	Control Logic Diagram	구현단계 V&V Checklist 및 RTM
시험 단계	– 시험 절차서/보고서 V&V 분석	시험계획 및 절차서, 시험보고서	시험단계 V&V Checklist 및 RTM
설치, 점검 단계	– 최종 V&V 보고서 작성	단계별 V&V 결과	V&V 최종보고서 (SVVR)

Test for the V&V



Configuration of Unit Test



Configuration of Integration System Test

RTM(Requirement Traceability Matrix) for V&V

No.1	6.6kV Switch Gear 계통 요건	확인단계			
		요건	설계	구현	시험
1	6.6kV 스위치 기어의 정상 전압을 OWS에 표시해야 한다.	3.3.1-1	3.1-1	340-3011(CLD)	340-3011(UT)
2	6.6kV 스위치 기어의 정상 전류를 OWS에 표시해야 한다.	3.3.1-2	3.1-2	340-3011(CLD)	340-3011(UT)
3	6.6kV 스위치 기어의 대체 전압을 OWS에 표시해야 한다.	3.3.1-3	3.1-3	340-3011(CLD)	340-3011(UT)
4	6.6kV 스위치 기어의 대체 전류를 OWS에 표시해야 한다.	3.3.1-4	3.1-4	340-3011(CLD)	340-3011(UT)
5	6.6kV 스위치 기어의 버스 전압을 OWS에 표시해야 한다.	3.3.1-5	3.1-5	340-3011(CLD)	340-3011(UT)
6	4급 전원의 상태를 OWS에 표시하고, 전원을 상실하여 접점입력 CI53103이 닫힐 때, 알람을 발생해야 한다.	3.3.1-6	3.1-6	340-3012(CLD)	340-3012(UT)
7	스위치 기어의 상태를 OWS에 표시하고, 비정상 동작으로 접점입력 CI53109이 닫힐 때, 알람을 발생해야 한다.	3.3.1-7	3.1-7	340-3014(CLD)	340-3014(UT)
8	Breaker S01-02의 Trip 상태를 OWS에 표시하고, 접점입력 CI53101이 닫힐 때, 알람을 발생해야 한다.	3.3.1-8	3.1-8	340-3015(CLD)	340-3015(UT)
9	Breaker S01-05의 Trip 상태를 OWS에 표시하고, 접점입력 CI53102이 닫힐 때, 알람을 발생해야 한다.	3.3.1-9	3.1-9	340-3015(CLD)	340-3015(UT)
10	Breaker S01-10의 Trip의 상태를 OWS에 표시하고, 접점입력 CI53104이 닫힐 때, 알람을 발생해야 한다.	3.3.1-10	3.1-10	340-3015(CLD)	340-3015(UT)
11	Breaker S01-13의 Trip의 상태를 OWS에 표시하고, 접점입력 CI53110이 닫힐 때, 알람을 발생해야 한다.	3.3.1-11	3.1-11	340-3015(CLD)	340-3015(UT)
12	Breaker S01-16의 Trip의 상태를 OWS에 표시하고, 접점입력 CI53108이 닫힐 때, 알람을 발생해야 한다.	3.3.1-12	3.1-12	340-3016(CLD)	340-3016(UT)
13	Breaker S01-18의 Trip의 상태를 OWS에 표시하고, 접점입력 CI53105이 닫힐 때, 알람을 발생해야 한다.	3.3.1-13	3.1-13	340-3016(CLD)	340-3016(UT)
14	Breaker S01-19의 Trip의 상태를 OWS에 표시하고, 접점입력 CI53107이 닫힐 때, 알람을 발생해야 한다.	3.3.1-14	3.1-14	340-3016(CLD)	340-3016(UT)
15	Breaker S01-20의 Trip의 상태를 OWS에 표시하고, 접점입력 CI53106이 닫힐 때, 알람을 발생해야 한다.	3.3.1-15	3.1-15	340-3016(CLD)	340-3016(UT)
16	Breaker S01-02가 닫힐 때, 접점입력 CI53111의 닫힘을 OWS에 표시해야 한다.	3.3.1-16	3.1-16	340-3012(CLD)	340-3012(UT)
17	Breaker S01-02가 닫힐 때, 접점입력 CI53112의 닫힘을 OWS에 표시해야 한다.	3.3.1-17	3.1-17	340-3012(CLD)	340-3012(UT)
18	Breaker S01-10가 닫힐 때, 접점입력 CI53113의 닫힘을 OWS에 표시해야 한다.	3.3.1-18	3.1-18	340-3013(CLD)	340-3013(UT)
19	Breaker S01-13가 닫힐 때, 접점입력 CI53117의 닫힘을 OWS에 표시해야 한다.	3.3.1-19	3.1-19	340-3013(CLD)	340-3013(UT)
20	Breaker S01-16가 닫힐 때, 접점입력 CI53115의 닫힘을 OWS에 표시해야 한다.	3.3.1-20	3.1-20	340-3013(CLD)	340-3013(UT)
21	Breaker S01-18가 닫힐 때, 접점입력 CI53114의 닫힘을 OWS에 표시해야 한다.	3.3.1-21	3.1-21	340-3013(CLD)	340-3013(UT)
22	Breaker S01-19가 닫힐 때, 접점입력 CI53116의 닫힘을 OWS에 표시해야 한다.	3.3.1-22	3.1-22	340-3014(CLD)	340-3014(UT)
23	Breaker S01-20가 닫힐 때, 접점입력 CI53118의 닫힘을 OWS에 표시해야 한다.	3.3.1-23	3.1-23	340-3014(CLD)	340-3014(UT)

Result of V&V

단계	V&V 업무
요건 단계	– 하나로 제어컴퓨터 기술시방서와 SRS의 비교를 통하여 정확한 요건 반영과 추적이 가능함을 확인함.
설계 단계	– SRS와 SDD의 비교를 통하여 설계의 적합성과 추적이 가능함을 확인
구현 단계	- 소프트웨어 설계 분석은 SDD와 Control Logic Diagram 사이의 추적성을 평가하는 방법으로 소스코드의 완전성, 만족함을 확인하였다.
시험 단계	- 소스코드와 시험절차서 사이의 추적 성을 평가하는 방법을 기반으로 소스코드의 완전성, 소스코드와 시험절차서의 일치 성 및 성능 요건 만족을 확인하였다.
설치, 점검 단계	V&V 활동을 통하여 각 생명주기에서 수행되는 소프트웨어 개발을 확인할 수 있었으며, 소프트웨어 생명주기별 상호 추적이 가능함을 확인하였다.

Conclusion

이 논문에서는 하나로 제어컴퓨터의 생명주기에 따른 V&V에 대해 논의 되었다.

V&V는 계획단계를 포함한 총 5개의 단계로 구성하였고, 소프트웨어 검증을 위해 IEEE 1012-20004에 따라 각 단계별 RTM_(Requirement Traceability Matrix)에 근거하여 추적이 가능함을 확인하였고, 요건정의에 따라 최종 시험을 누락 없이 완료하였다.

이 V&V를 통하여 하나로 제어컴퓨터를 성공적으로 교체할 수 있었으며, 향후 하나로의 시스템 개발에 유용하게 사용하게 될 것이다.