|  |
| --- |
| **학번: 201924463 성명: 문석준** |

**1. Therac 25 : 사고 개요**

1985년 캐나다의 AECL 이라는 회사는 암 종양 제거를 위한 방사선 치료기인 Therac 25 라는 제품을 판매하기 시작했다. Therac 25는 피부 근처의 종양을 제거하는 Electron 모드와 X-ray로 피부 깊숙한 곳의 종양을 제거하는 X-ray 모드의 두가지 동작 모드를 지원했다. 그런데 X-ray 모드에서 강한 방사선을 균일하고 안전하게 환자에게 쪼일 수 있는 ‘턴테이블’이라는 장치의 위치가 간혹 제 위치에 있지 않는 경우가 발생했다. 이로 인하여 환자들은 대량의 방사능을 과다 섭취하게 되었고 이로 인하여 6명의 사상자가 발생하게 되었다.

**2. Therac 25 : 사고 원인 및 재발 방지 대책**

턴테이블의 동작 상태를 저장하는 변수가 8bit라는 점이 문제가 되었다. 시스템이 준비된 상태이면 해당 변수가 0, 아닐 경우 1을 증가하는 구문이 있는데 이 구문을 256번 수행되면 256번째 수행할 때 해당 상태값은 overflow가 발생하여 0으로 변하고 턴테이블이 준비 상태여야 하지만 방사능을 발사하게 되는 사고가 발생한다. 해당 사고 재발 방지를 위해서는 상태 저장을 위해 bool 형 변수를 사용하면 overflow 가 발생하지 않아 더 안정적인 관리가 가능 할 것이다.

---------------------------------------------------------------------

**1. 미국 Hatch 원자력 발전소 비상 셧다운 : 사고 개요**

2008년 3월 7일 미국 Georgia 주 Baxley 근처에 위치한 Hatch 원자력 발전소의 Unit 2가 48시간 동안 셧다운 되는 사고가 발생하였다. Unit 2의 모든 7개 복수탈염기의 출구 밸브가 거의 동시에 잠기면서 정상적인 급수 흐름 기능을 일시적으로 상실하였다. 인명피해는 없었다.

**2. 미국 Hatch 원자력 발전소 비상 셧다운 : 사고 원인 및 재발 방지 대책**

사고 원인은 해당 발전소의 기술 운영을 담당하는 Southern Nuclear Operating Company의 한 엔지니어가 발전소의 비즈니스 네트워크 상의 컴퓨터를 업데이트하는 과정에서 발생하였다. 비즈니스 네트워크와 통제 네트워크 상에 동시에 존재하는 컴퓨터가 있었는데, 비즈니스 네트워크의 업데이트로 재부팅 되면서 통제 네트워크 상에서도 재부팅이 되는 문제가 발생하여 발전소의 안전 시스템은 이 데이터 결여를 핵 연료봉을 냉각시켜주는 냉각수 수위가 떨어진 것으로 해석하고 결과적으로 비상 셧다운을 가동시켰다. 이를 방지하기 위해서는 서로 간섭이 일어나서는 안되는 서버들 간의 네트워크 연결을 완벽히 분리시켜야 한다.