학번: 201527137 성명: 정대현

Loss of Precision Error in Patriot Missile Defense System at Dhahran, Saudi Arabia

1) 사고 내용

1991년 2월 25일 사우디아라비아 다라한에서 사용하던 패트리어트 미사일은 이라크가 발사한 스커드 미사일 요격을 실패를 하고 해당 미사일은 미 육군 막사에 떨어져 28명 사망 98명 부상

2) 사고 원인 분석

패트리어트 시스템은 공중 요격 미사일과 적 미사일을 탐지하는 레이더로 구분됩니다. 시스템에서 레인지 게이트는 적의 미사일이 어디에 있는지 탐지하는 것으로 목표물의 속도와 레이더에서 발견된 최종 '시간'을 기반으로 목표물이 다음에 어디에 나타날 지 예측하게 됩니다. 시스템에서 속도를 십진 정수로 표현 가능한 실수 형식이지만 시간은 내부 클락에 의해서 1/10단위로 측정되고 다시 1/10을 곱하여 정수 형식으로 컴퓨터에 저장됩니다. 시간을 정수에서 실수로 전환하는 과정에서 24비트 이후 소수점 뒷부분이 잘리는 라운드 오프 에러가 발생하게 되며 시간이 지날수록 오차는 더 커지게 됩니다. 사고 당시 시스템의 시간 오차는 0.34초이며 미사일의 위치는 687미터를 더 이동하게 되여 레인지 게이트가 추적에 실패하게 됩니다.

3) 재발 방지 대책

정기적으로 재부팅을 통해 시스템 클락을 0으로 리셋할 것을 권고했으며 이후 해당 시간 오차를 버그를 수정한 소프트웨어 배포합니다.

Misplacement of a Satellite by Titan IV B-32/Centaur Launch Vehicle

1) 사고내용

1999년 4월 30일 Titan IV B-32가 Milstar 위성을 지구 동기 궤도에 올려놓기 위해서 발사하였으나, 제2차 연소 중 불완전한 동작으로 제어를 상실해서 목표 궤도 도달 실패했습니다. 1993년부터 총 4번의 발사 실패로 프로젝트는 12억 3천만 달러의 손실을 입었습니다.

2) 사고 원인 분석

해당 로켓은 2단 분리로 이루어집니다. 1단계 연소과정에서 Centaur가 분리하는데 RCS연료가 고갈될 때 개방 루프를 발사하게 되어 남은 미션에 비해 추진체를 과다하게 소모하는 문제가 있었습니다. 이는 2단계 연소단계에서 자세제어를 위한 충분한 연료를 확보하지 못했으며 자세 안정화에 실패를 했습니다. 사고 원인은 잘못된 프로그램의 방정식의 결과로 보고 있습니다. 해당 방정식에서 소프트웨어 상수 생성(위성 손실에 중요한 요소)은 이전에 아무런 문제가 없었기 때문에 위험도가 낮은 것으로 간주되었으나 실은 잠재적으로 매우 중요한 요소였습니다. 결국 해당 롤 레이트 데이터가 비행 컴퓨터에서 무시되었으며, 프로젝트 실패로 이어졌습니다.

3) 재발 방지 대책

해당 데이터의 우선순위는 이전 프로젝트에 따라 잠재적으로 결정되었으나, 해당 중요도가 어떻게 측정되었는지 아무도 몰랐습니다. 전체 프로세스에 있어 데이터가 정확하고 사용처가 적합한지 지속해서 추적해야 하며 데이터의 중요도는 암묵적이 아닌 명시적으로 평가받아야 합니다.