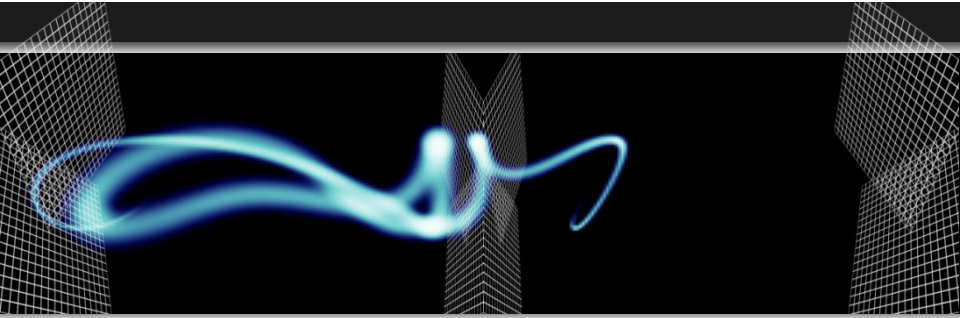


소프트웨어 무결점 연구센터 5th 워크샵



QNX RTOS기반 비행제어S/W
및 고장사례 분석

2011 년 1월 6일 - 9일
한용수

서울대학교 비행역학 및 제어연구실



Flight Dynamics and Control Lab
Seoul National University, Republic of Korea



I. 연구 배경

II. QNX 기반 비행제어 프로그램 구성

III. 항공분야 코드오류 고장사례 분석

IV. 결과 및 향후 과제

◆ 연구배경

● 무인항공기(UAV)

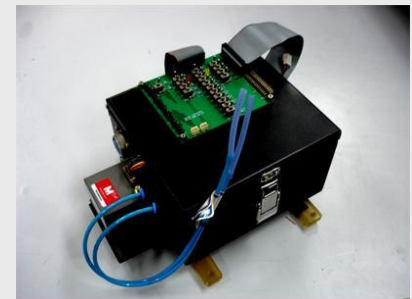
- 높은 활용도와 가능성
- 다양한 임무 수행 능력
 - 영상을 이용한 실시간 감시 및 정찰, 적의 방공망 체계 무력화 등의 임무
- 자동화, 실시간 처리 -> **고성능의 비행제어컴퓨터가 필요**

● DSP(TMS320LF2407A)

- 기존의 비행제어컴퓨터
- 데이터 처리속도, 저장공간, 실시간 처리능력 한계

● PC/104(ATH660-128)

- 새롭게 구성한 비행제어컴퓨터
- 데이터 처리속도, 저장공간 증가
- RTOS(Real Time Operation System)을 통한 실시간 처리능력 향상

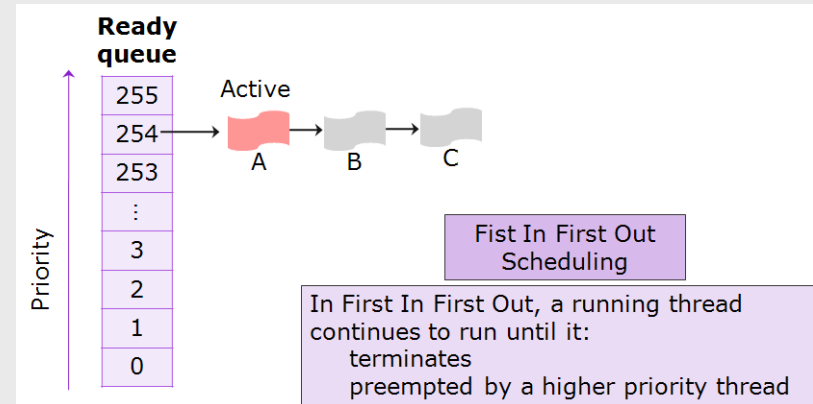


QNX 기반 비행제어 프로그램 구성

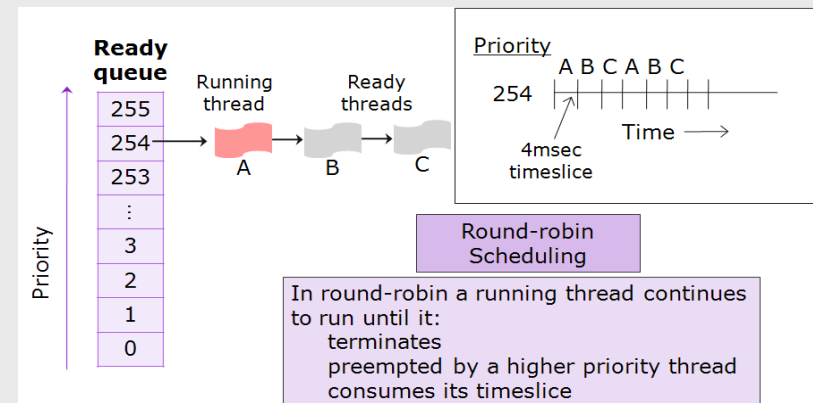
◆ QNX

- 철저한 우선순위(Priority) 기반의 선점형(Pre-emptable) Thread 지원
- Thread Scheduling
 - FIFO scheduling
 - 자기 자신이 스스로 블록하거나, 높은 우선순위 thread가 준비상태가 될 때까지 실행
 - Round-Robin scheduling
 - 동일한 우선순위를 가지는 thread들이 시분할 간격 단위로 번갈아 가며 실행
- 새롭게 구성한 비행제어 프로그램에서는 Hardware Thread와 Software Thread를 나누어 RR scheduling 방법을 사용

<FIFO>

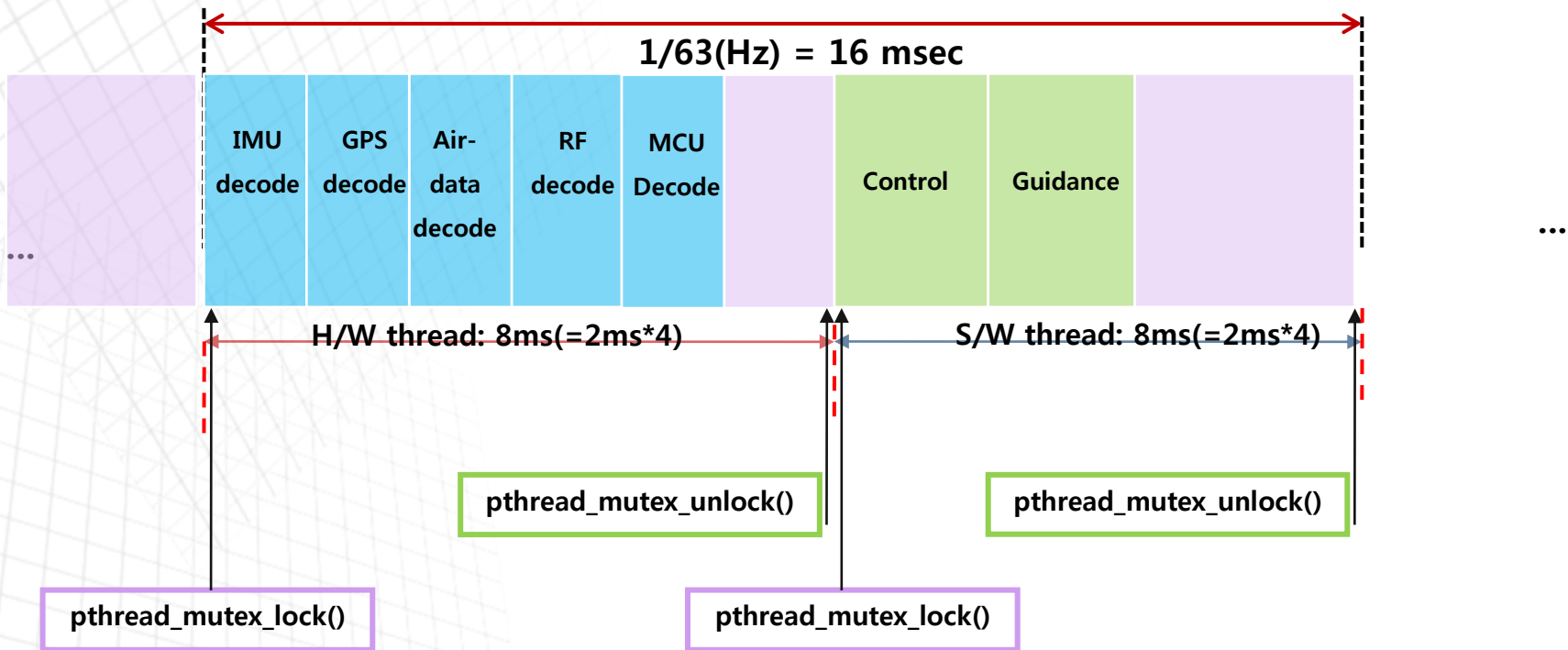


<Round Robin>



Thread scheduling 개념도

◆ QNX용 FCC(Flight Control Computer) 구성 현황



고장사례 분석

항공분야에서의 코드오류로 인한 고장사례 - 우주탐사

◆ 우주발사체

- The Ariane 5 Bug(June 4, 1995)
 - 'Operand Error'
 - 발사 후에 로켓 폭발
 - 발사체 항법 및 제어 시스템 분석 부족으로 인한 사고
 - \$7.5 billion
- The NASA English/Metric System Bug(September 23, 1999)
 - The Mars Climate Orbiter
 - Unit Confusion: English system unit <-> Metric system unit, 개발팀간 서로 다른 unit사용
 - 화성 표면 40m상공에서 엔진 shut-off -> 추락
 - \$125 million
- Mars Global Surveyor (MGS) Spacecraft(November 2, 2006)
 - Mis-sent command(하드웨어 구속조건을 초과한 입력)에 의한 배터리 손실
 - 전력저하로 임무 조기중단



항공분야에서의 코드오류로 인한 고장사례 - 민간/군사

◆ 민간 항공

- The Air Traffic Control System Bug(September 14, 2004)
 - countdown timer 수가 4 billion milliseconds(46.3 days)를 초과
 - System runs out
 - 이후 30일 동안 manually reboot

◆ 군사 항공

- The Patriot Missile(February 21, 1991)
 - Clock drift로 인해 missile 위치 오차 600m
 - 군인 28명 사망
- F-22 Raptor(1992, 2007)
 - Pilot-Induced Oscillation
 - Multiple computer crashes coincident
- Smart ship USS Yorktown(1997)
 - Divided by zero



항공분야에서의 고장사례 분석

◆ 고장분류 1

- Operand error, unit system error, divide by zero, etc

◆ 고장분류 2

- Countdown timer, clock drift
- **장시간의 시뮬레이션을 통해 검출 가능**
- HILS(Hardware In the Loop Simulation)을 통한 검증

결과 및 향후 과제

◆ 결과

- QNX RTOS 기반의 비행제어프로그램 구성
 - Round-Robin scheduling 기법을 이용한 hard real-time 구현
- 고장사례 분석

◆ 향후 과제

- 새로운 QNX 기반 비행제어 프로그램 오류 검증 필요
- 고장사례 분석을 통한 고장검증(HILS)
- **공동논문작성 및 추가 연구과제 도출 !!**