

무인 비행체 제어 SW 분석 검증

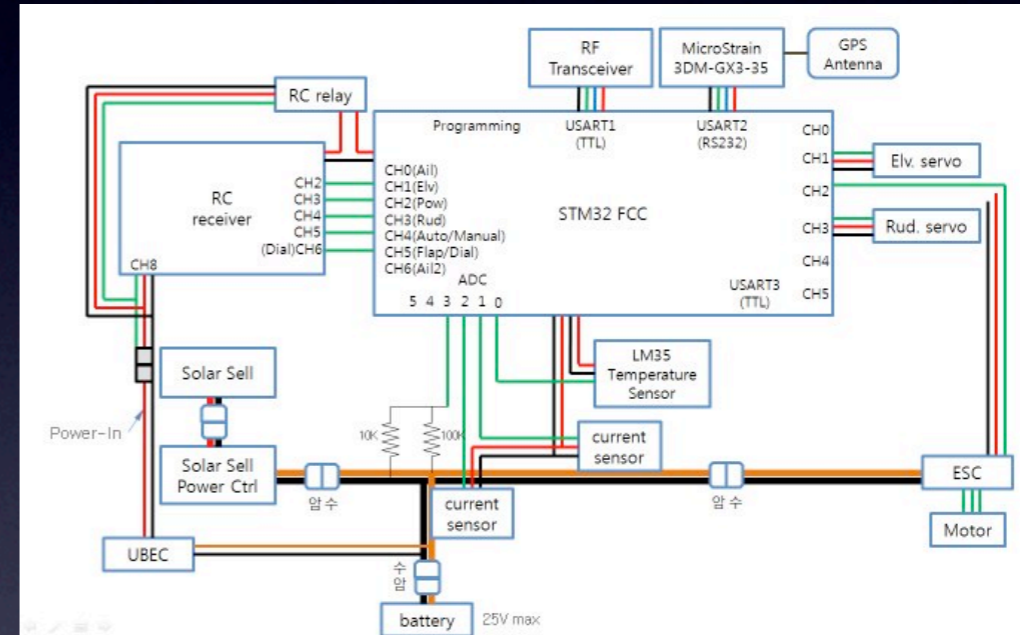
허기홍, 강동욱, 오학주
서울대학교 프로그래밍연구실

2012 ROSAEC 여름 워크샵

목표

- 대상 : 항공대학교 무인 비행체 제어 SW
- 검증요소 : 프로그램을 죽이는 안전성 오류
 - 버퍼 오버런, 0으로 나누기

프로그램 특징



- 초기화; (센서입력; 필터; 자세제어)+

*사진 출처: 항공대 박상혁 교수님 홈페이지

프로그램 특징

- 핵심 코드 (C코드 4400줄) + 라이브러리
- 동적할당, 재귀함수 없음
- 반복문
 - 전체 반복
 - 유한 반복문 : 배열 원소 접근
 - 센서 입력 대기 : `while(buffer.length < 4)`

프로그램 분석

- 요약 의미 공간

$$[[P]] \in \mathbb{C} \rightarrow \hat{S}$$

$$\hat{S} = \hat{L} \rightarrow \hat{V}$$

$$\hat{V} = \hat{Z} + 2^{\hat{L}} + \text{Array}_{\perp} + \text{Struct}_{\perp}$$

$$\hat{Z} = \{\perp\} + \{[l, u] \mid l, u \in \mathbb{Z} \cup \{-\infty, +\infty\}\}$$

프로그램 분석

- 요약 의미 : 다음 F의 최소 고정점

$$\hat{F} \in (\mathbb{C} \rightarrow \hat{\mathcal{S}}) \rightarrow (\mathbb{C} \rightarrow \hat{\mathcal{S}})$$

$$\hat{F}(\hat{X}) = \lambda c \in \mathbb{C}. \hat{f}_c \left(\bigsqcup_{c' \hookrightarrow c} \hat{X}(c') \right)$$

대상 특화

- 인터럽트를 통한 센서 입력
 - 센서값을 담는 버퍼를 특별히 처리
 - 센서값이 갖는 범위 파악해서 반영

대상 특화

- 행렬 연산 코드에 적절한 넓히기(widening) 연산

```
// 행렬 곱셈 계산
for(i = 0; i < sa; i++){
    for(j = 0; j < sb; j++){
        w = 0.0;
        for(k = 0; k < sc; k++)
            w += a[i*sa+k] * b[k*sb+j];
        c[i*sc+j] = w;
    }
}
```


결론

- 무인 비행체 SW에 특화된 분석기 제작중
 - 하드웨어 동작 처리, 똑똑한 넓히기 연산
- 자세한 이야기는 포스터 발표에서

고맙습니다