Programovací techniky a úskalí při vývoji SW v automotive oblasti

na případu Toyoty

Martin Butnikošarovski

Případ Hyundai Sonata

- Náhlé samovolné zrychlení

Případ Hyundai Sonata

- Náhlé samovolné zrychlení
- Špatný design

Případ Hyundai Sonata

- Náhlé samovolné zrychlení
- Špatný design
- Bezpečnostní pravidla

Případ Hyundai Sonata

- Náhlé samovolné zrychlení
- Špatný design
- Bezpečnostní pravidla
- Pozdní řešení

Případ Toyota

- Náhlé samovolné zrychlení

Případ Toyota

- Náhlé samovolné zrychlení
- Prokázaných 89 mrtvých

Případ Toyota

- Náhlé samovolné zrychlení
- Prokázaných 89 mrtvých
- Problém ve vývoji softwaru

Případ Toyota

- Náhlé samovolné zrychlení
- Prokázaných 89 mrtvých
- Problém ve vývoji softwaru
- Použití zpráv NASA a BARR Group

Pravidla v programování

- Firemní pravidla

Pravidla v programování

- Firemní pravidla
- Rekurze

Pravidla v programování

- Firemní pravidla
- Rekurze
- Přetypování

Pravidla v programování

- Firemní pravidla
- Rekurze
- Přetypování
- Globální proměnné

Pravidla v programování

- Firemní pravidla
- Rekurze
- Přetypování
- Globální proměnné
- MISRA

Pravidla v programování

- Firemní pravidla
- Rekurze
- Přetypování
- Globální proměnné
- MISRA
- Složitost funkcí

Řešení v Toyota

- Podle BARR group - porušeno 32% vlastních pravidel

Řešení v Toyota

- Podle BARR group - porušeno 32% vlastních pravidel
- NASA našla 7000 MISRA porušení

Řešení v Toyota

- Podle BARR group - porušeno 32% vlastních pravidel
- NASA našla 7000 MISRA porušení

  BARR group přes 80 000

Řešení v Toyota

- Více než 11 000 globálních proměnných

Řešení v Toyota

- Více než 11 000 globálních proměnných
- Komplexnost funkcí – 67 funkcí jejichž skóre vyšší než 50

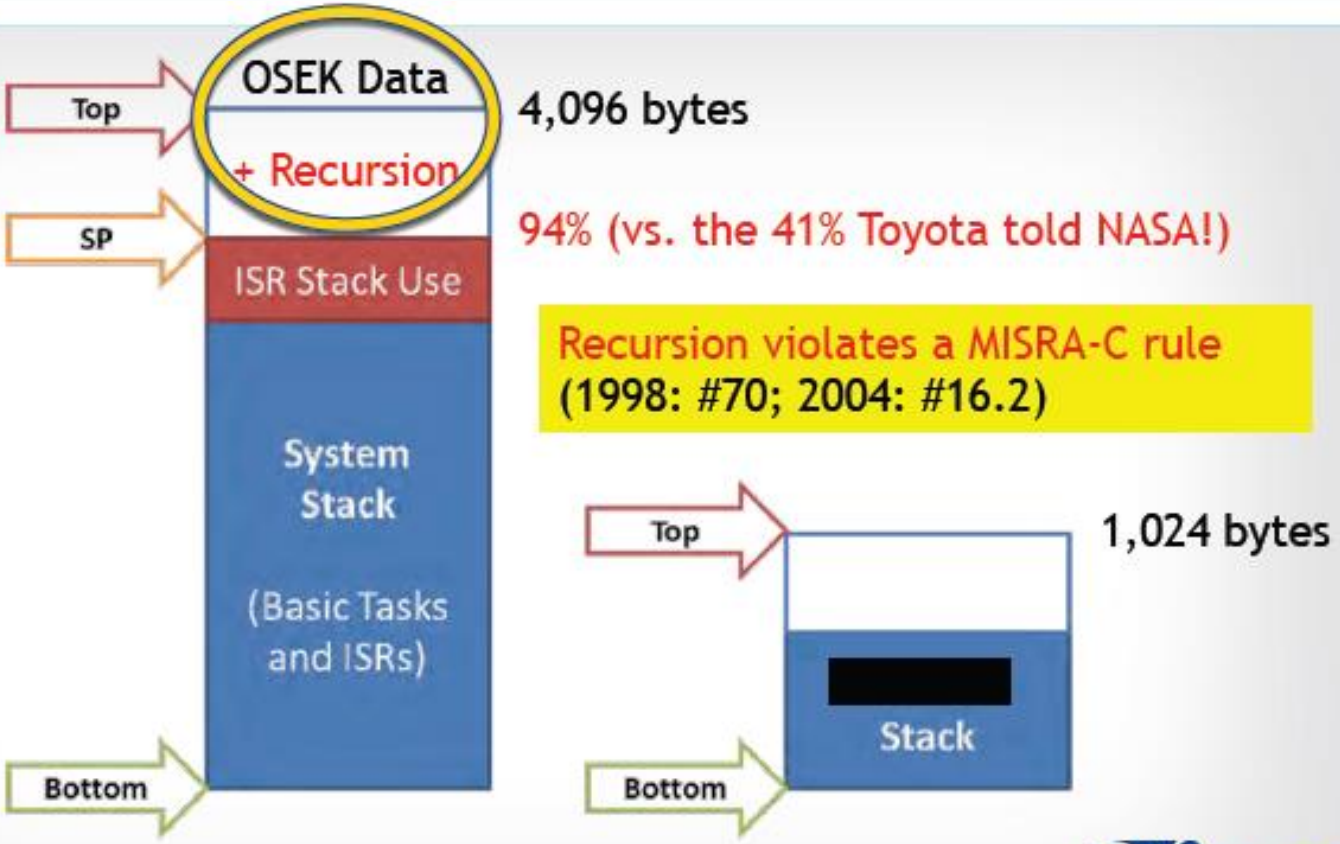
Řešení v Toyota

- Více než 11 000 globálních proměnných
- Komplexnost funkcí – 67 funkcí jejichž skóre vyšší než 50
- Funkce nastavení úhlu plynového pedálu 146 (1300 ř.)

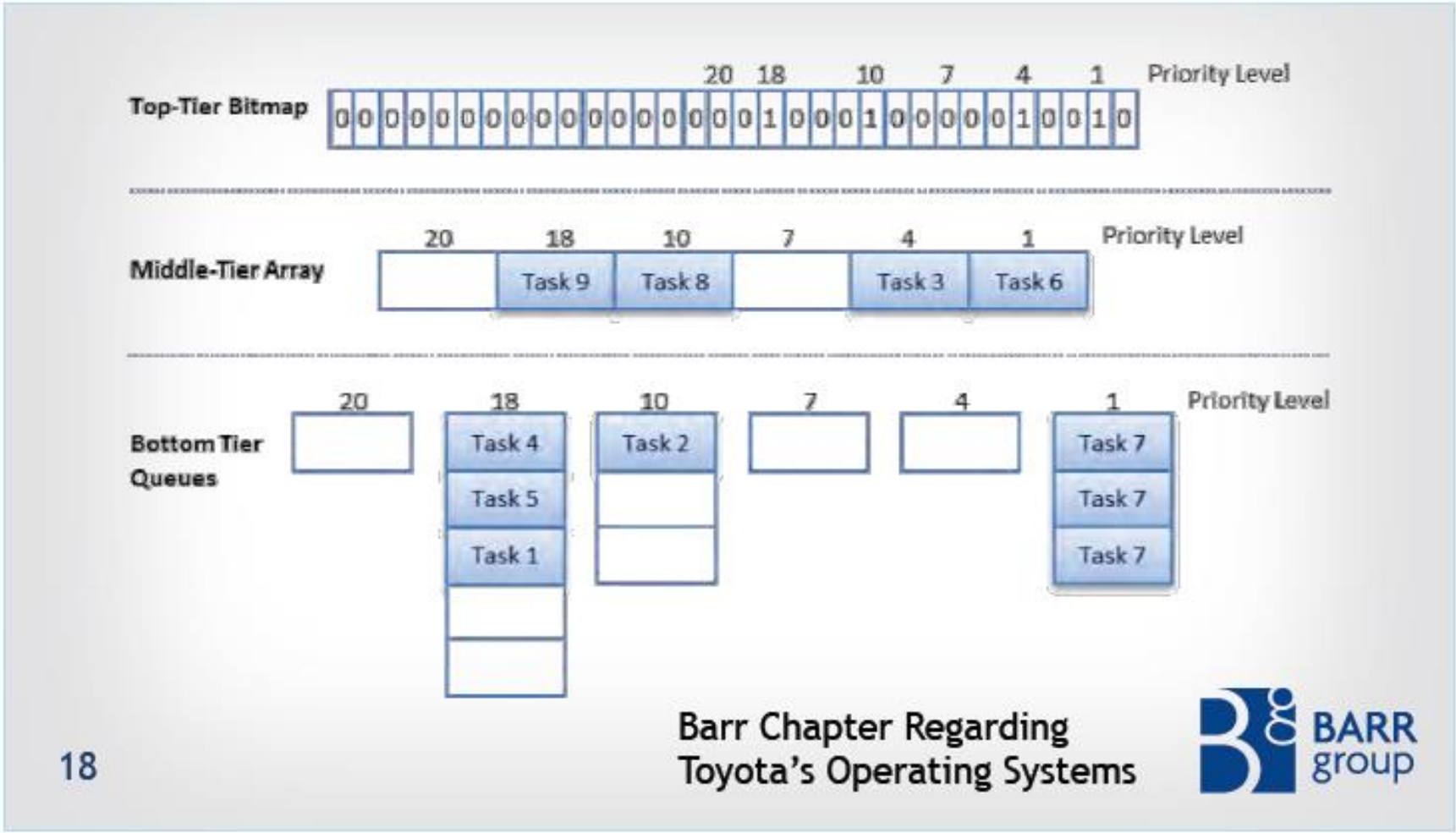
Zajištění paměti

- Parity bit
- Zrcadlení paměti
- CRC
- Test použití paměti

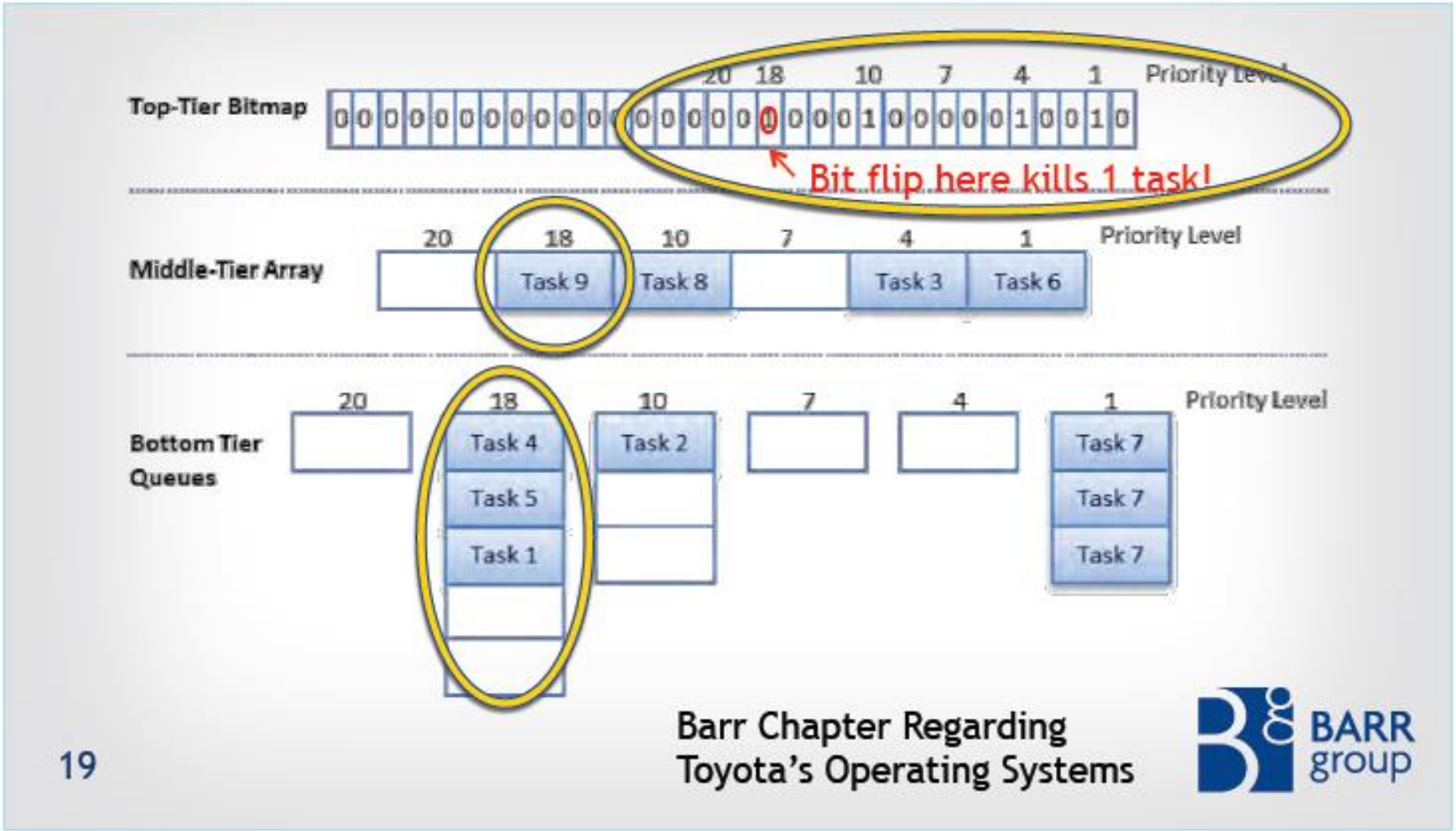
Řešení v Toyota



Řešení v Toyota



Řešení v Toyota

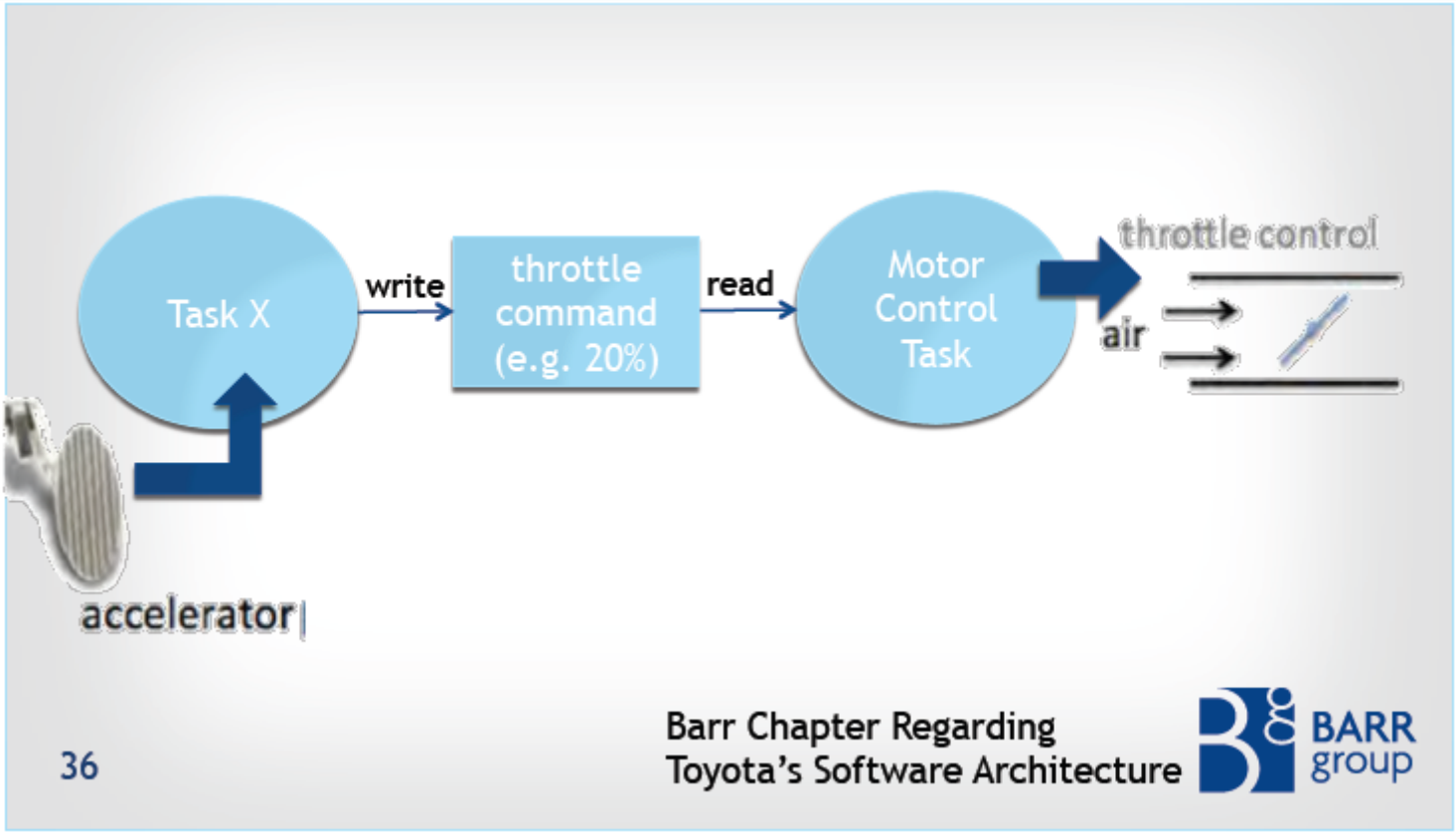


Bezpečnost softwaru

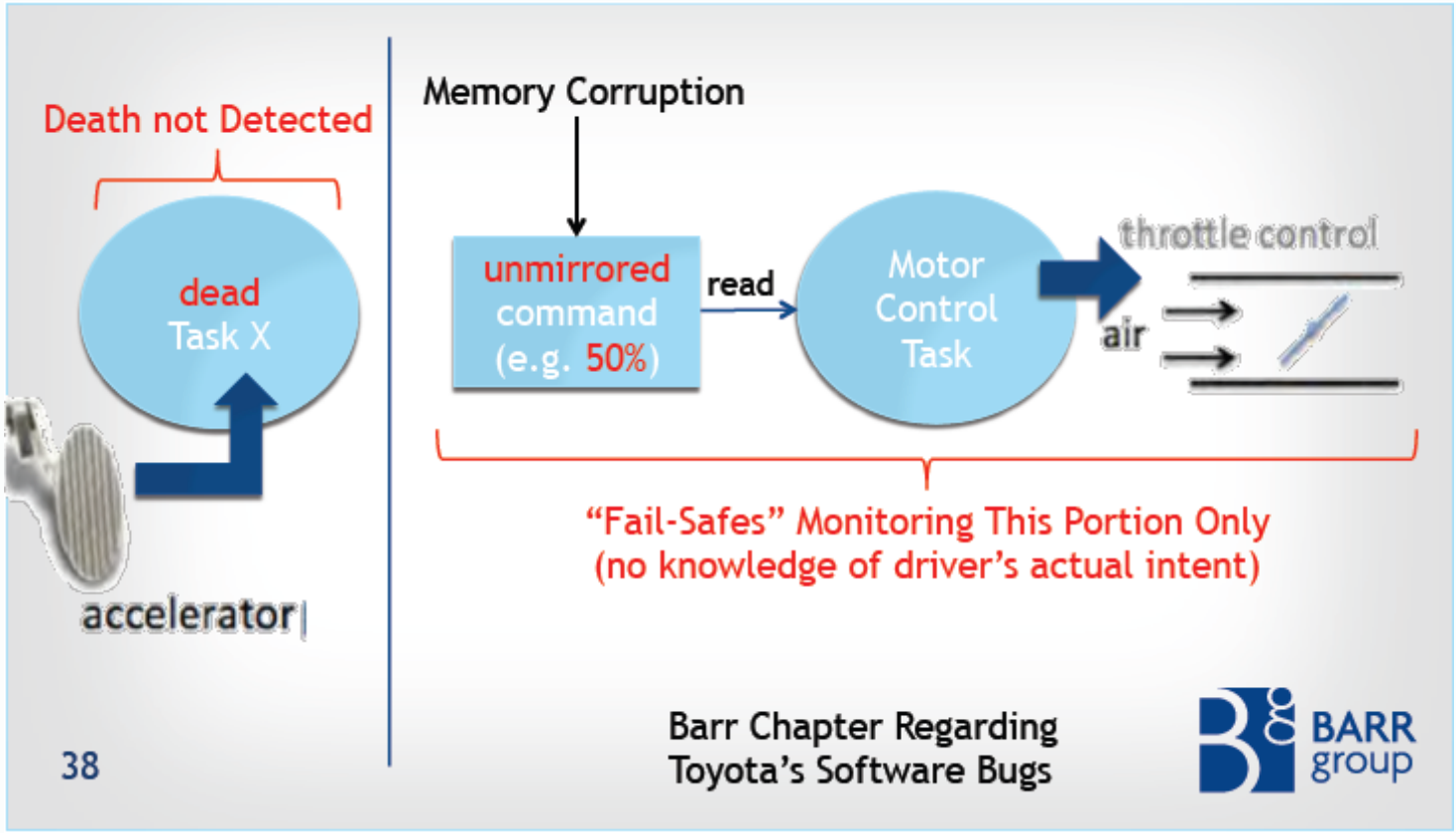
- Zdvojení kritických proměnných
- Bezpečné stavy
- Watchdog

Řešení v Toyota

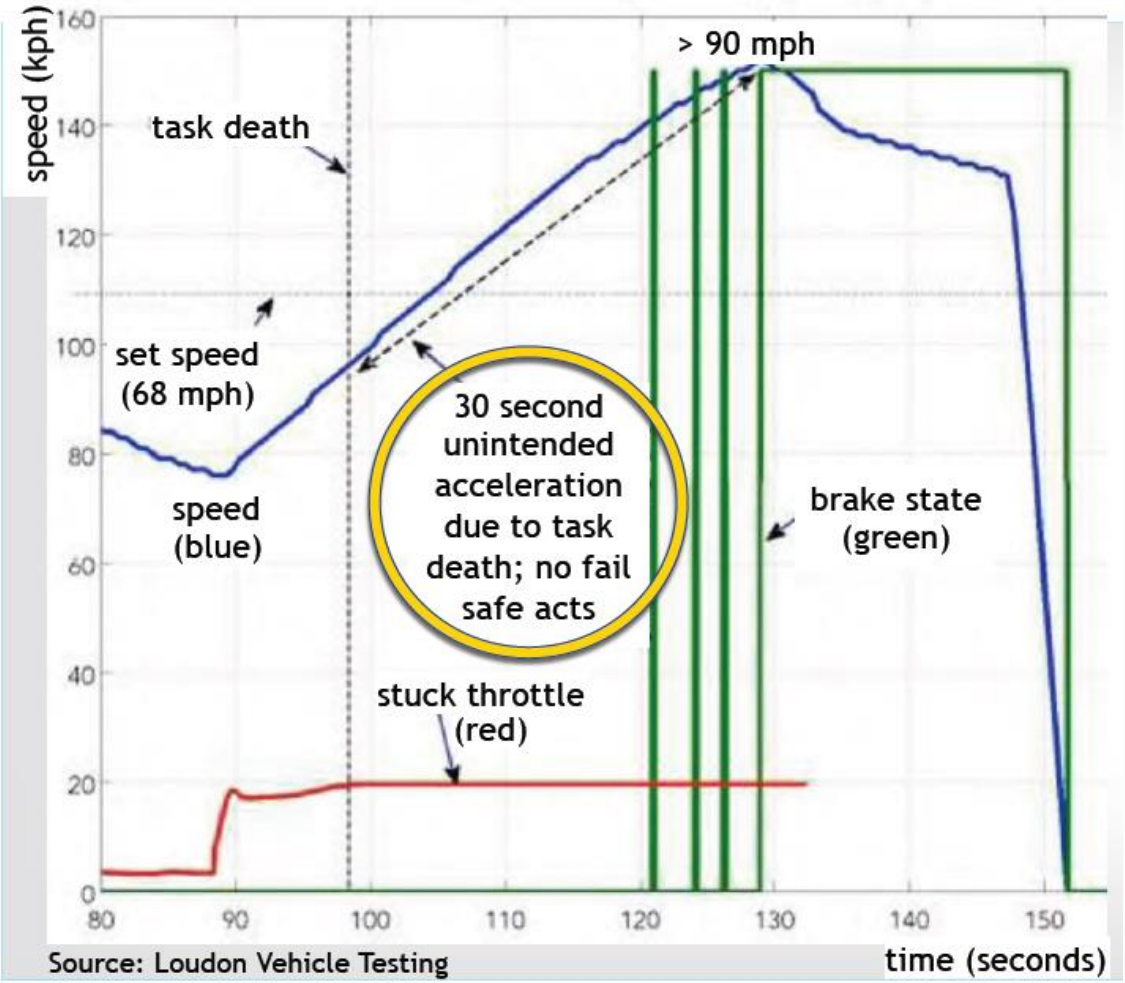
- Úhel sešlápnutí plynového pedálu



Řešení v Toyota



Řešení v Toyota



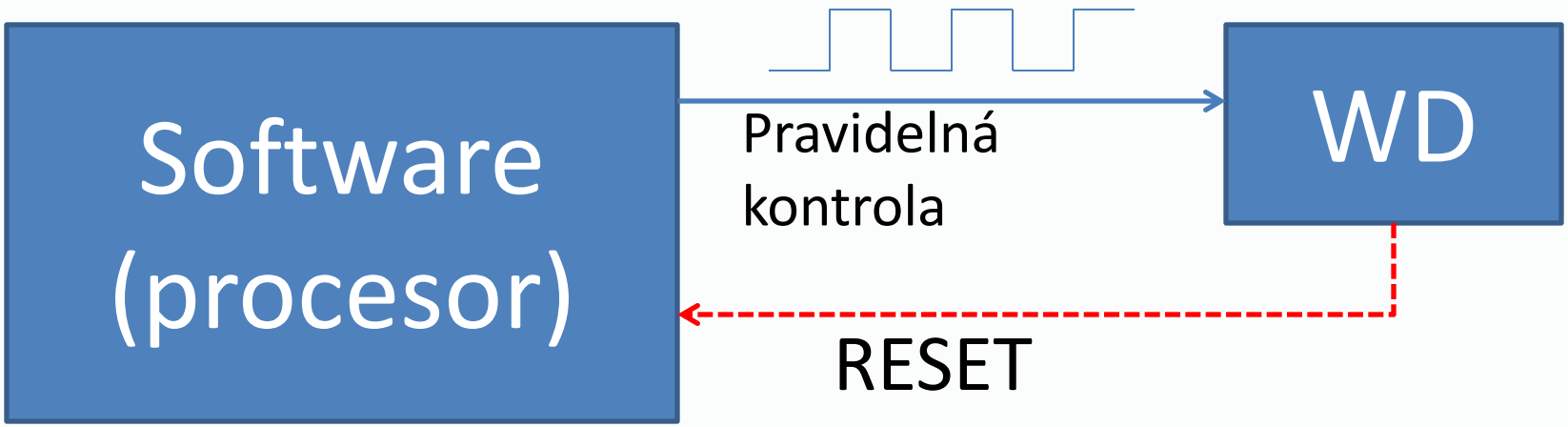
Řešení v Toyota

- Bezpečné stavy
  - Limp home modes
  - Idle mode fuel cut
  - Engine off

Řešení v Toyota

- Bezpečné stavy
  - Limp home modes
  - Idle mode fuel cut
  - Engine off
- Všechny ve stejném tasku jako ovládání pedálu

Watchdog



Řešení v Toyota

- WD volaný z HW interrupt pro aktualizaci časovače

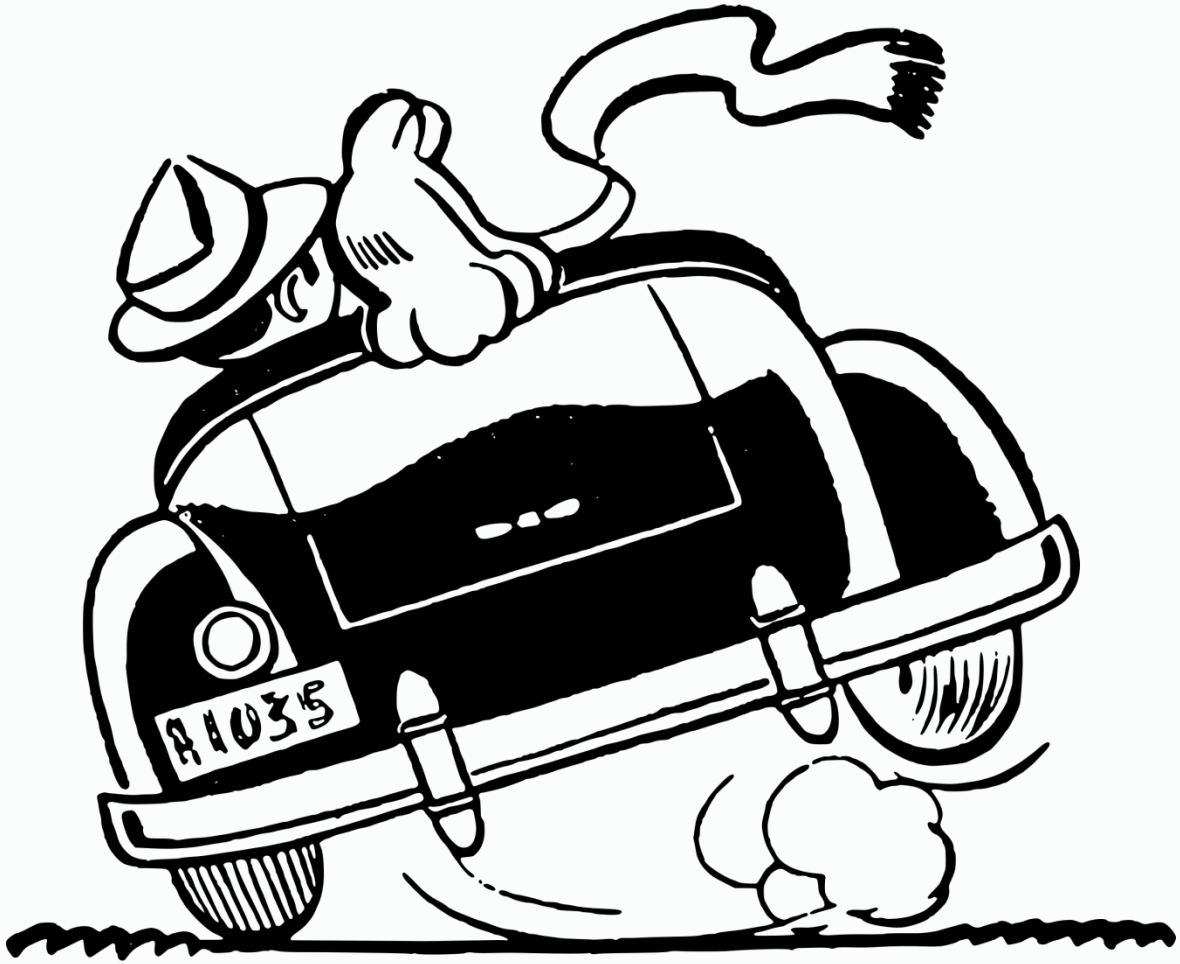
Řešení v Toyota

- WD volan[illegible] interrupt pro aktualizaci [illegible]e

Shrnutí

- Toyota porušila základní principy vývoje SW
- Odškodnění 1.2 mld. $
- 10 mil. aut

Děkuji za pozornost



Zdroje

- NASA report
  - http://www.nhtsa.gov/UA
- BARR Group report
  - http://www.safetyresearch.net/Library/BarrSlides_FINAL_SCRUBBED.pdf
- Video s Hyundai Sonata
  - https://www.youtube.com/watch?v=3bXQ5m11lw8