Аппаратное обеспечение IoT/CPS
Лекция 10

А. А. Подшивалов
apodshivalov@miem.hse.ru

Функциональная безопасность встраиваемых систем

Найдите лишнее

Критическая информационная инфраструктура

Ответственность

I. Уголовный кодекс Российской Федерации:

Статья 217.1. Нарушение требований обеспечения безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса

Статья 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Статья 283. Разглашение государственной тайны

Статья 284. Утрата документов, содержащих государственную тайну

Статья 293. Халатность

Немного определений (по ГОСТ Р 56205–2014, он же IEC/TS 62443-1-1:2009)

- Безопасность (safety) — отсутствие недопустимого риска

Немного определений (по ГОСТ Р 56205–2014, он же IEC/TS 62443-1-1:2009)

- Безопасность (safety) — отсутствие недопустимого риска
- Защита (security) — предотвращение несанкционированного или нежелательного проникновения, а также вмешательства в исправную и запланированную работу системы промышленной автоматики и контроля (одно из определений)

Немного определений (по ГОСТ Р 56205–2014, он же IEC/TS 62443-1-1:2009)

- Безопасность (safety) — отсутствие недопустимого риска
- Защита (security) — предотвращение несанкционированного или нежелательного проникновения, а также вмешательства в исправную и запланированную работу системы промышленной автоматики и контроля (одно из определений)
- Кибербезопасность (киберзащита) (cybersecurity) — действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов

Основные документы

- IEC 61508 — «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью»
  - ISO 26262 — Автомобильный транспорт
  - EN 50126, EN 50128, EN 50129 — Железнодорожный транспорт
  - IEC 62061 — Системы управления
  - IEC 62304 — Медицинские приборы
  - DO-178C — Авиационная техника

И еще немного определений (из IEC 61508)

- Риск (risk) — сочетание вероятности события причинения вреда и тяжести этого вреда
- Вред (harm) — физическое повреждение или ущерб, причиняемый здоровью людей, имуществу или окружающей среде
- Опасность (hazard) — потенциальный источник причинения вреда
- Допустимый риск (tolerable risk) — риск, который приемлем при данных обстоятельствах на основании существующих в обществе ценностей

Немного философии, или об оценке рисков

- ALARP (as low as reasonably practicable)
- GAMAB (globalement au moins aussi bon)
- MEM (minimum endogenous mortality)

Основные «документы»

- Анализ опасностей и рисков (hazard and risk analysis)
- Safety case
- Анализ отказов (failure analysis)
- План обеспечения безопасности (safety plan)
- Руководство по безопасности (safety manual)

Разработка безопасных систем

Некоторые противоречия

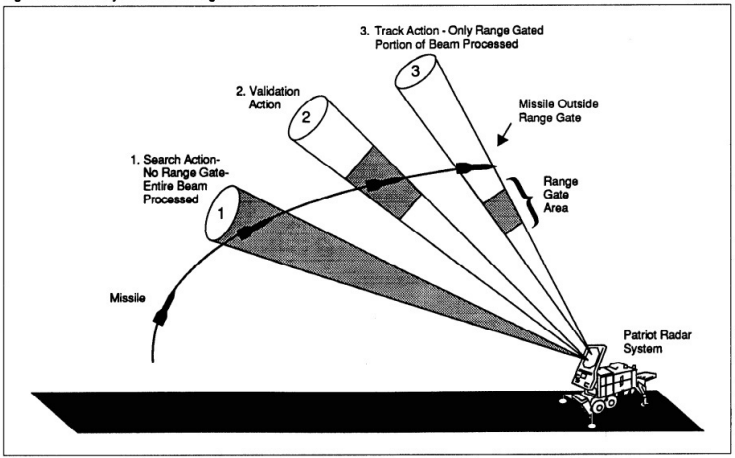
- Доступность/надежность
  - Может ли система выдать неправильный отклик, но вовремя?
- Функциональность/безопасность
  - А если ничего не делать...
- Защищенность/производительность/безопасность

Обнаружение ошибок

- Можно ли доверять внешним данным?
  - Что делать, если данные «неправдоподобны»?
- Аномалии во внутренних метриках системы
- Rejuvenation
  - Накопление ошибок
  - Patriot 25.02.1991

Patriot 25.02.1991

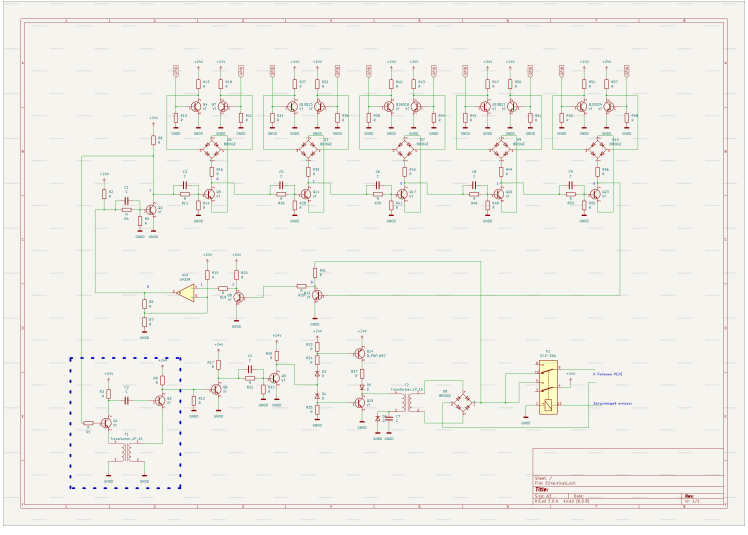
Figure 5: Incorrectly Calculated Range Gate



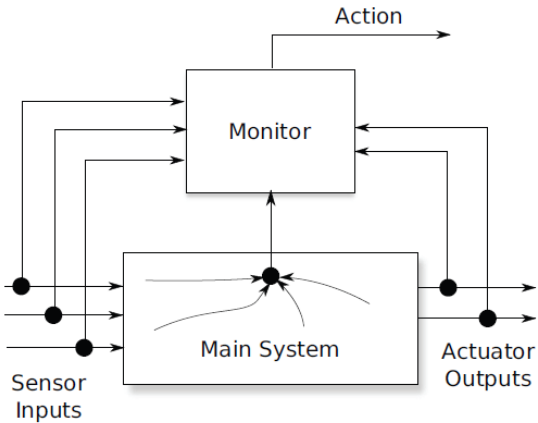
Обнаружение ошибок — что делать?

- Заведомо безопасное состояние
- Восстановление системы
- Fail-fast, crash only и тому подобные подходы — максимизация ошибки

Давайте включим реле...



Дублирование и мажорирование



- Имеет смысл, если надежность ПО намного превышает надежность аппаратной части
- Вырожденный случай 1 — два процессора разной архитектуры, две команды программистов
- Вырожденный случай 2 — watchdog

Программное обеспечение

ПО как особый компонент системы

- Сбои ПО — детерминированные или случайные?
- Верификация кода
  - Полуформальные методы — конечные автоматы, сети Петри, ...
  - Формальные методы — pre-conditions, post-conditions, инварианты

Написание кода

- Язык программирования
  - MISRA C
  - Ada
- Тестирование
- Статический анализ

SOUP

- SOUP — Software of Unknown Provenance
  - Разработка в соответствии с IEC 61508
  - PIU — proven-in-use
  - Оценка не соответствующего стандарту ПО