Building **Robust** Systems

Razvan Tataroiu

Coliberator Summit 2025

Personal Background

- Engineering – Teaching – Research
  - Embedded Systems
    - wireless sensor networks & IoT
    - scientific & test equipment
  - Data Acquisition & Control
    - analog & digital electronics
    - distributed systems
    - firmware & application software
  - Automated Test Stands
  - Industrial Safety

Topics

- Software
- Hardware

- Standards
- Risks

- Reliability, Resilience, Robustness

Personal
Stories
&
Opinions

Tools

Building Hardware

- PCB Design Software
- Prototyping Solutions
- Smart Parts

PCB Design

- KiCad
  - competent, professional-grade software
  - modern GUI
  - integrated Python console
  - free software, GPL version 3 or later
  - free component library, CC-BY-SA 4.0
  - human-readable files

Prototyping

- Hand-built PCBs
- Cheap, Quick PCB Manufacturing
- Dev Boards
- Modules
  - standardized interfaces?

Smart Parts

- Modern parts can be powerful tools
  - feature-rich, programmable devices
  - highly integrated
    - many design problems already solved (almost)
    - reduced development time
- Necessary Software Tools
  - effective software dev tools
  - useful software components

Traps

- Errata
- Overly optimistic expectations
- Increasing degree of complexity

Mitigation

- Trusted parts & software libraries
- Abstraction & Agility
- Standardized platforms

Story Time...

- 2021-2023 chip shortage
- Microcontrollers
  - ATmega – gone
  - STM32 – gone
  - PIC32MM anyone?
- LM317 adjustable voltage regulator
  - “jellybean” part, ~50 year old design
  - built by many mfgs, usually > 100k in stock

Weak link

- Fragile foundation of modern technology
- Semiconductor manufacturing
  - very specialized operation
  - long lead times
  - relatively few competitors
  - manufacturers will discontinue parts

Mitigation ?

- Standardization
  - some simple parts are “second-sourced”
    - opamps, voltage regs, logic gates, ancient 8051 MCUs
  - design workflow, esp. for digital ICs
- FPGAs
  - programmable at the circuit level
  - hardware description languages
  - few manufacturers
  - efforts to develop free tools

Mitigation ?

- Move most functionality into software
- Make the software modular
  - engineer the software core to be
    as hardware-agnostic as possible
- Leverage software platforms
  - that support a wide variety of hardware
- Avoid wastage
  - development effort / hardware resources

Industrial Standards

Industrial Standards

- Safety of operators
- Safety of bystanders
- Safety of service technicians
- Safety of property
- Safety of the environment
- Interoperability, Reliability, Repairability

Safety

- Risk assesment
- Risk reduction
  - Intrinsically-safe design
  - **Reliable** safeguards
  - Organizational measures
- Examples
  - ISO 12100, ISO 13849, IEC 60204, IEC 61010

Reliable Hardware

- built out of reliable components
- redundant configurations
  - two sensors reading the same thing
    - software checks for coincidence
  - two switches in series
    - in case one fails short-circuit
    - with monitoring
  - two CPUs

Reliable Software

- kernel code written by
  2 people for the 2 CPUs
- user code written in
  Limited Variability Languages
  - actually drawn as diagrams
  - limited functionality
- documented verification procedures, tests

Noteworthy Aspects

- Industrial Standards Require Documentation
  - schematic diagrams
  - parts lists
  - description of functionality
    - business customers also require these
    - documents are usually non-public
- Consumers don’t usually demand schematics

Clouds

IoT

Scenario

- “Smart Home”
  - Ambient sensors
  - Lighting control
  - HVAC control
  - fridge camera
  - front door camera / intercom

Cloud-Based Solution

- User Advantages
  - ease of deployment
  - low maintenance
- Vendor Advantages
  - move functionality into the cloud
    - ease of development
    - centralized maintenance
  - recurring subscription revenue

Cloud-Based Solution

- User Risks
  - recurring subscription fee
  - leaks of personal data
    - “TV watches you”
  - discontinuation of cloud service
    - e.g. IoT solution vendor discontinues support or ceases operation entirely

Mitigation

- Standardized IoT-specific Protocols
- Separate Device, Cloud and App Vendors
- Run your own private “cloud”

Closing Remarks

Conclusion

- Robustness is a matter
  - engineering
  - risk management
  - awareness
  - foresight
  - policy

Thank you!

Building Robust Systems

Razvan Tataroiu

Coliberator Summit 2025