Panel Discussion:

Pervasive Formal Verification in Control System Design

Moderator: Lee Pike, Galois Inc.

Why Control Systems?

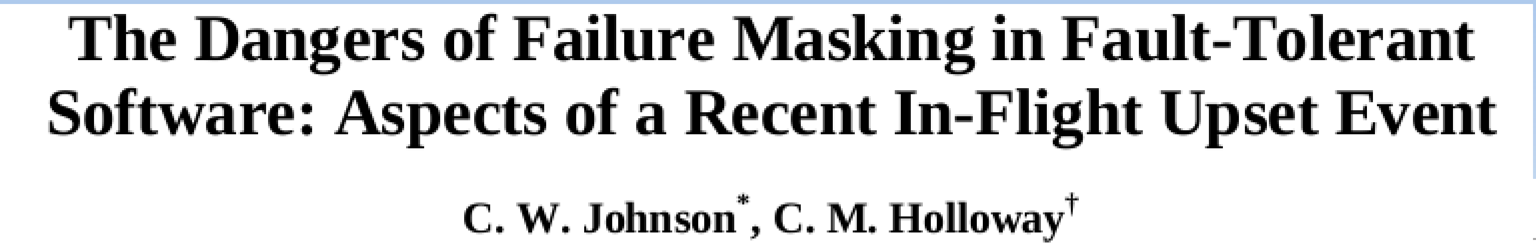
2000-01-01 12:10

Temperature (degC): 24.02
Level (m): 1.80

LEGEND:
🟩 Run/Open
🟥 Stop/Closed
🟨 Trip/Failed

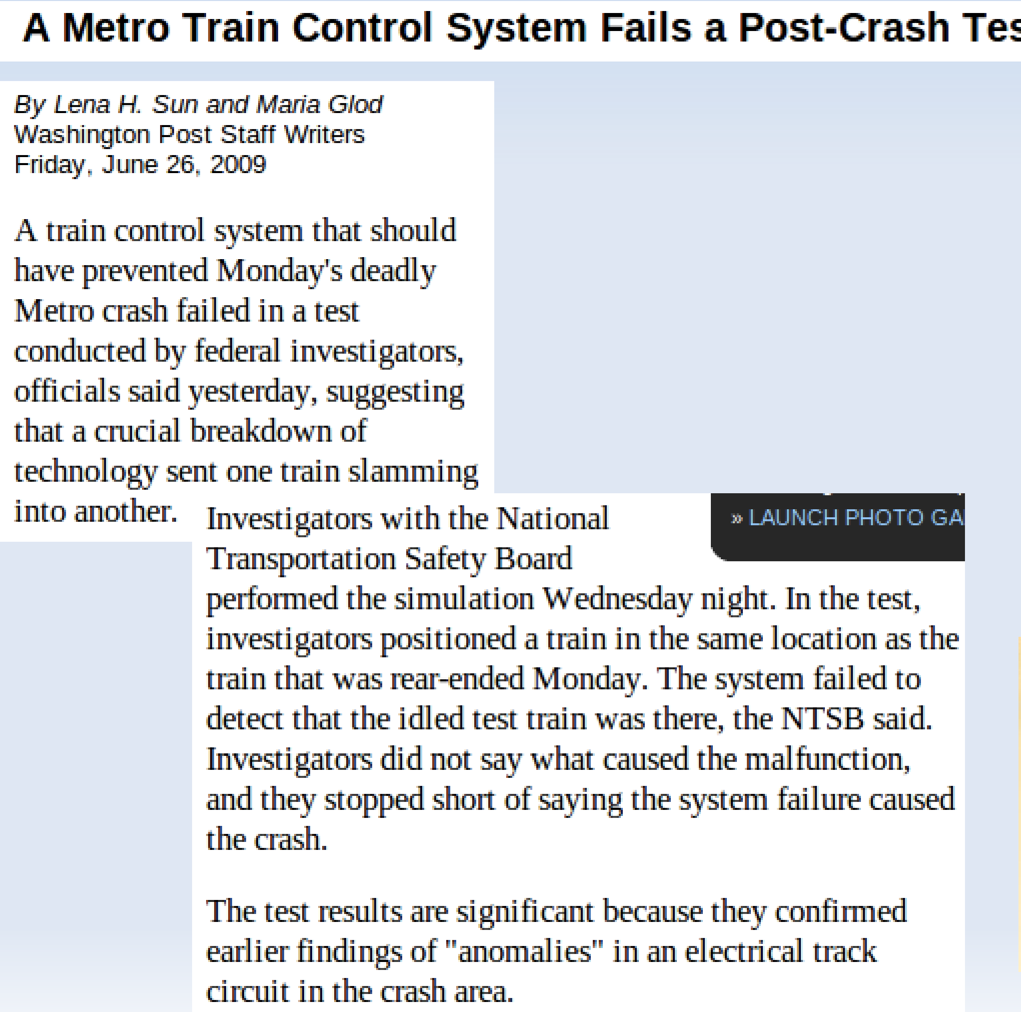
Example of ACAS Protection Volume between 5000 and 10000 feet

What's Not Working?



The Dangers of Failure Masking in Fault-Tolerant Software: Aspects of a Recent In-Flight Upset Event

C. W. Johnson[*], C. M. Holloway[†]



A Metro Train Control System Fails a Post-Crash Test

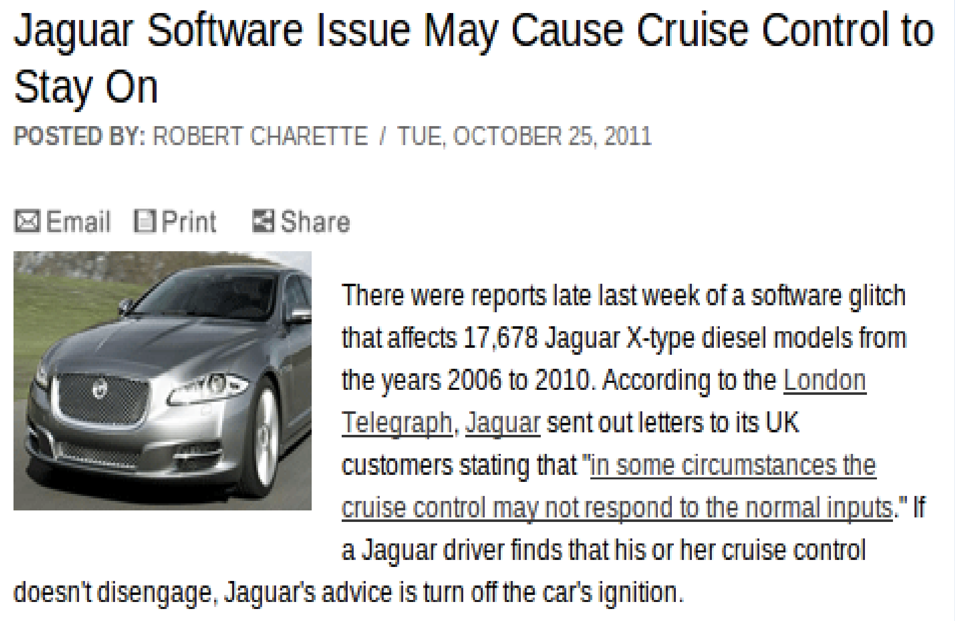
By Lena H. Sun and Maria Glod
Washington Post Staff Writers
Friday, June 26, 2009

A train control system that should have prevented Monday's deadly Metro crash failed in a test conducted by federal investigators, officials said yesterday, suggesting that a crucial breakdown of technology sent one train slamming into another.

» LAUNCH PHOTO GA

Investigators with the National Transportation Safety Board performed the simulation Wednesday night. In the test, investigators positioned a train in the same location as the train that was rear-ended Monday. The system failed to detect that the idled test train was there, the NTSB said. Investigators did not say what caused the malfunction, and they stopped short of saying the system failure caused the crash.

The test results are significant because they confirmed earlier findings of "anomalies" in an electrical track circuit in the crash area.



Jaguar Software Issue May Cause Cruise Control to Stay On

POSTED BY: ROBERT CHARETTE / TUE, OCTOBER 25, 2011

✉ Email Print Share

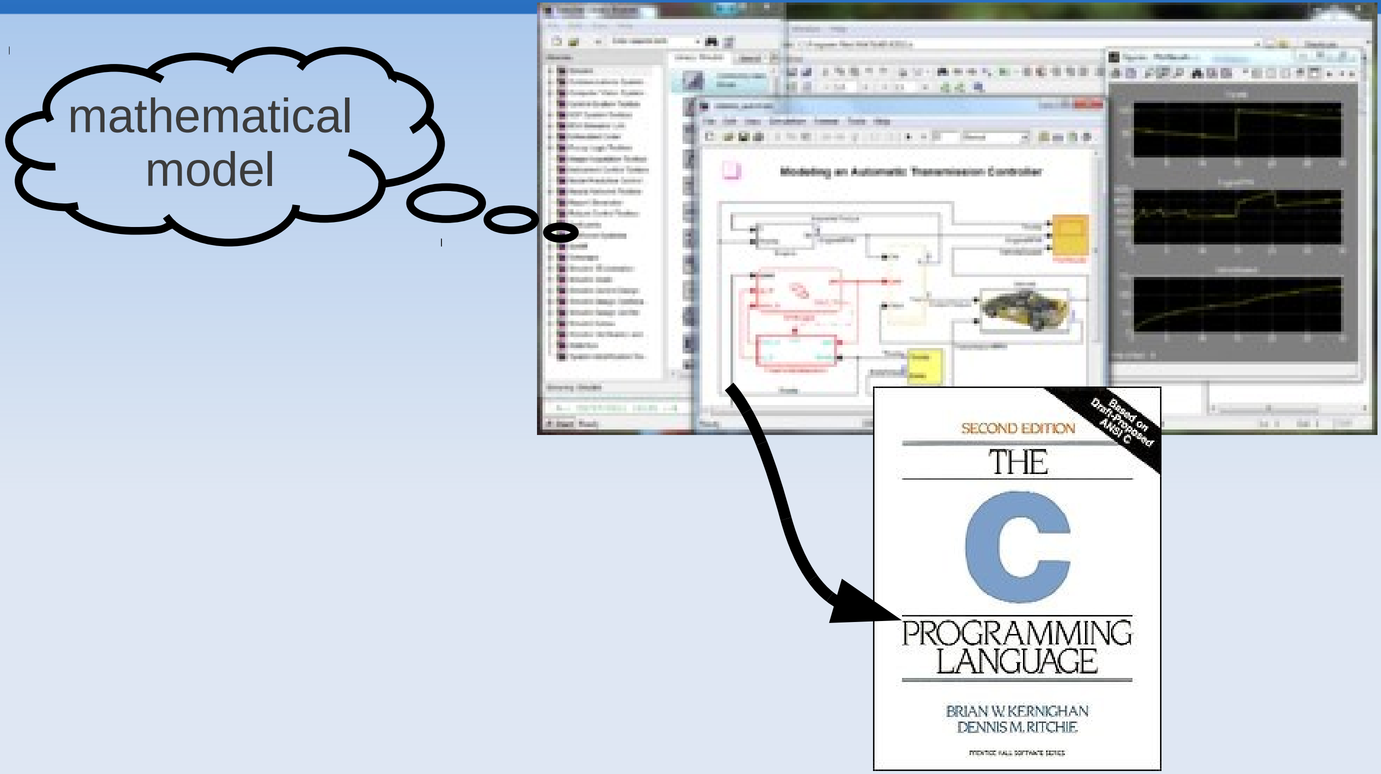
There were reports late last week of a software glitch that affects 17,678 Jaguar X-type diesel models from the years 2006 to 2010. According to the London Telegraph, Jaguar sent out letters to its UK customers stating that "in some circumstances the cruise control may not respond to the normal inputs." If a Jaguar driver finds that his or her cruise control doesn't disengage, Jaguar's advice is turn off the car's ignition.

W32.Stuxnet Dossier

Version 1.4 (February 2011)

Nicolas Falliere, Liam O Murchu, and Eric Chien

What Is a Control System?



mathematical model

Modeling an Automatic Transmission Controller

SECOND EDITION

Based on Draft-Proposed ANSI C

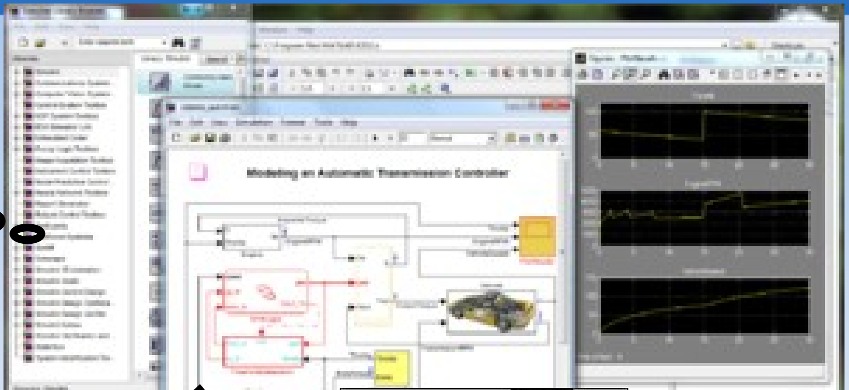
THE C PROGRAMMING LANGUAGE

BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

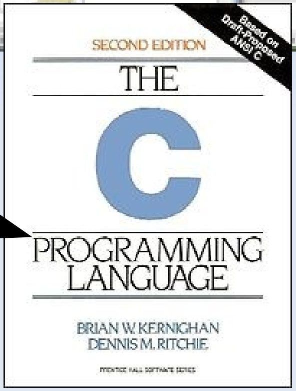
PRENTICE HALL SOFTWARE SERIES

What Is a Control System?

mathematical model



Modeling an Automatic Transmission Controller



Based on Draft-Proposed ANSI C

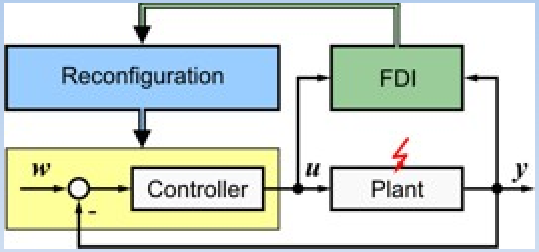
SECOND EDITION

THE C PROGRAMMING LANGUAGE

BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

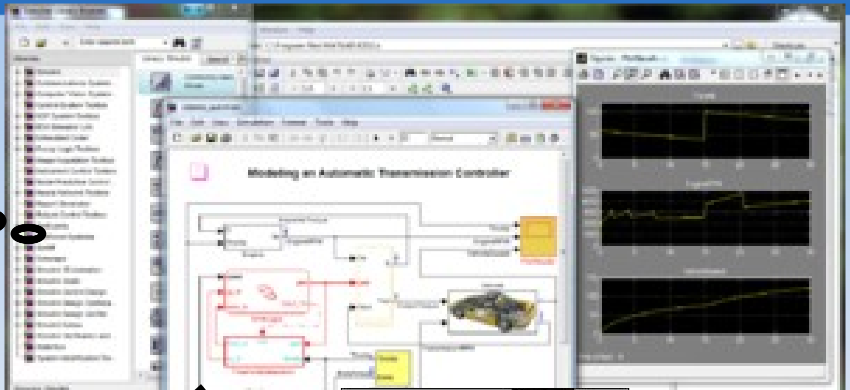
PRENTICE HALL SOFTWARE SERIES

reconfigurable control

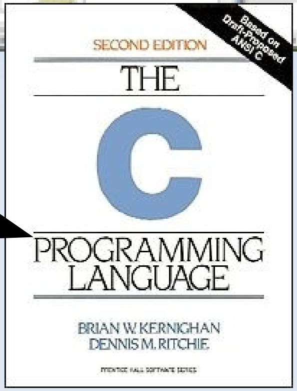


What Is a Control System?

mathematical
model



Modeling an Automatic Transmission Controller



SECOND EDITION

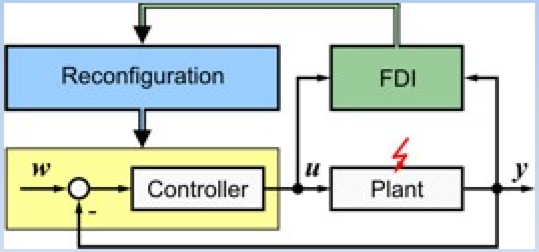
Based on Draft-Proposed ANSI C

THE C PROGRAMMING LANGUAGE

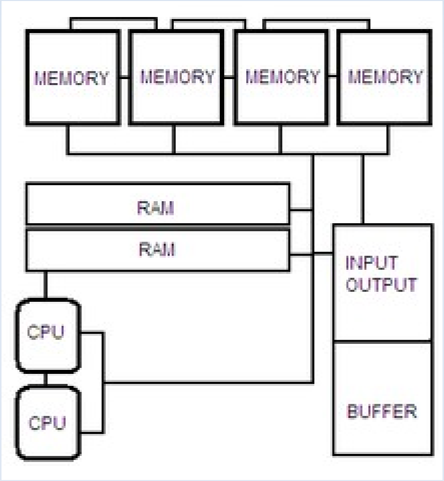
BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

PRENTICE HALL SOFTWARE SERIES

reconfigurable control

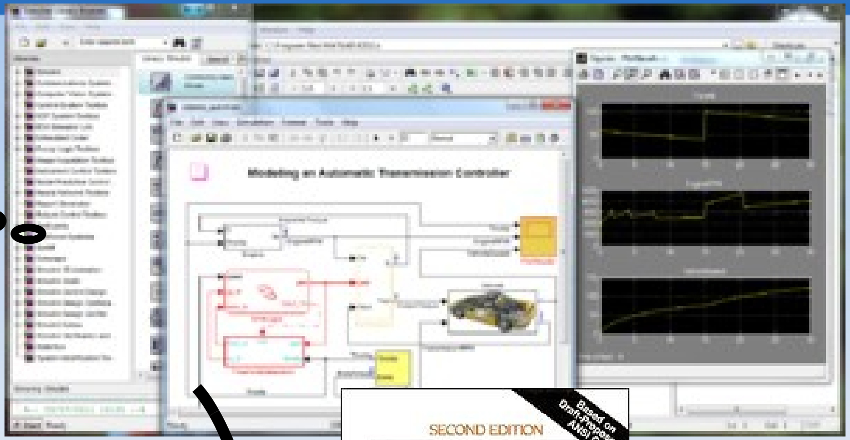


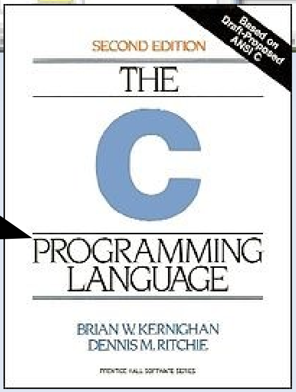
fault tolerance



What Is a Control System?

mathematical model





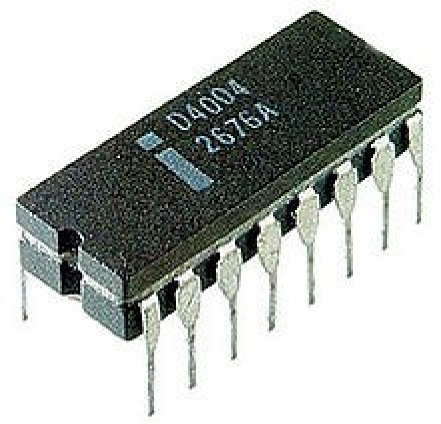
Based on Draft-Proposed ANSI C

SECOND EDITION

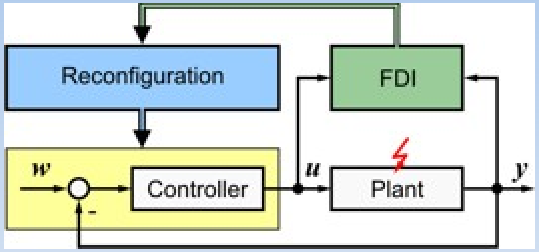
THE C PROGRAMMING LANGUAGE

BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

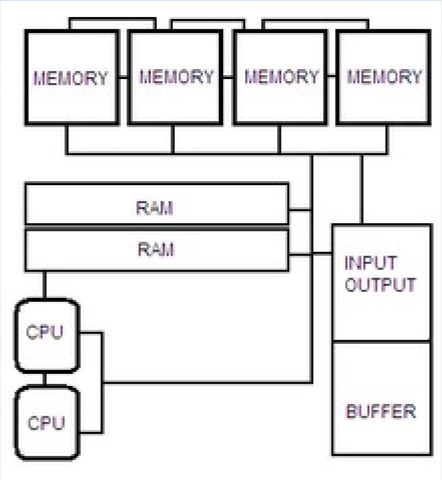
PRENTICE HALL SOFTWARE SERIES



reconfigurable control

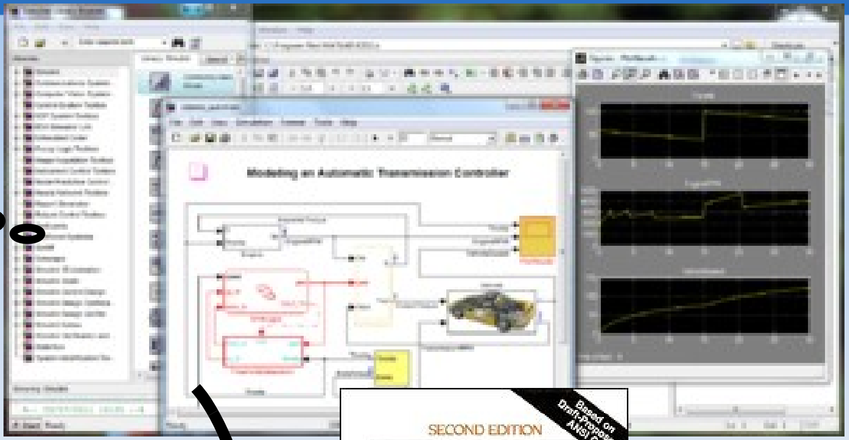


fault tolerance

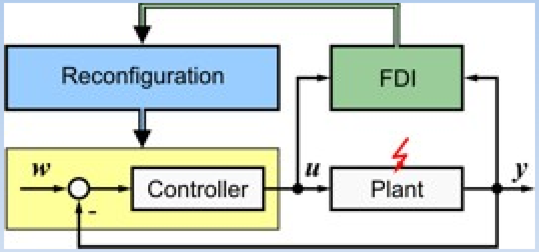


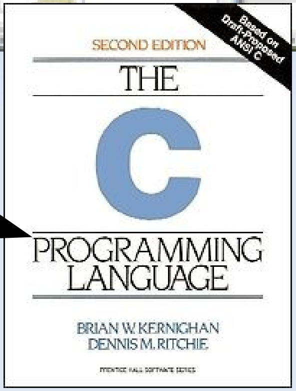
What Is a Control System?

mathematical model



reconfigurable control





Based on Draft-Proposed ANSI C

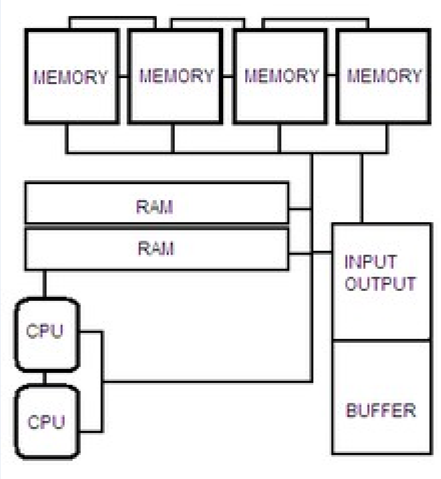
SECOND EDITION

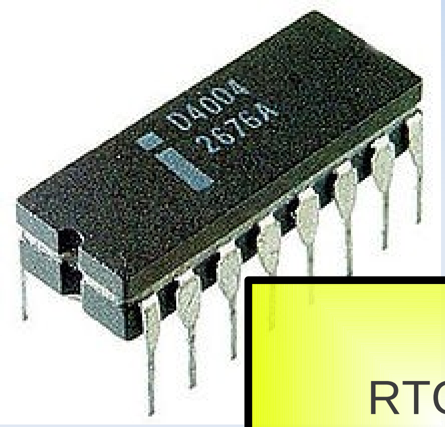
THE C PROGRAMMING LANGUAGE

BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

PRENTICE HALL SOFTWARE SERIES

fault tolerance

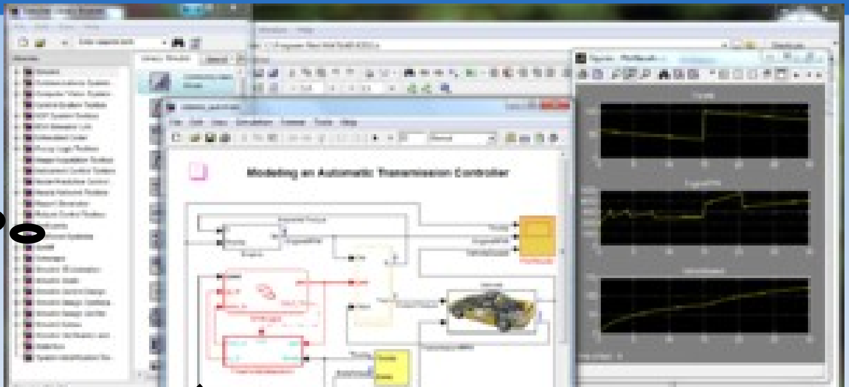




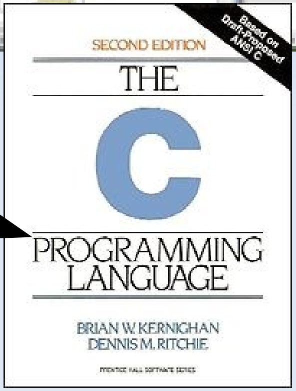
RTOS/
Middleware

What Is a Control System?

mathematical model



Modeling an Automatic Transmission Controller



SECOND EDITION

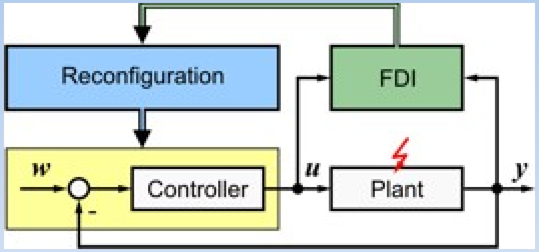
Based on Draft-Proposed ANSI C

THE C PROGRAMMING LANGUAGE

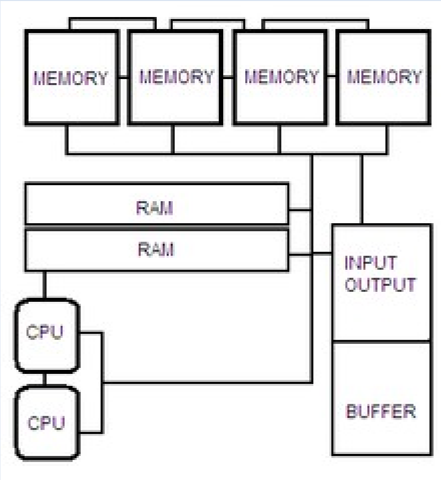
BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

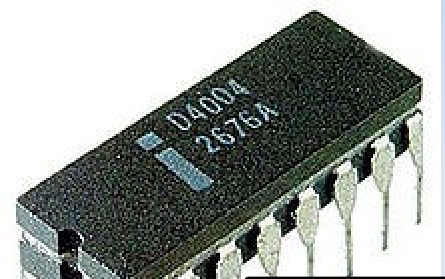
PRENTICE HALL SOFTWARE SERIES

reconfigurable control



fault tolerance

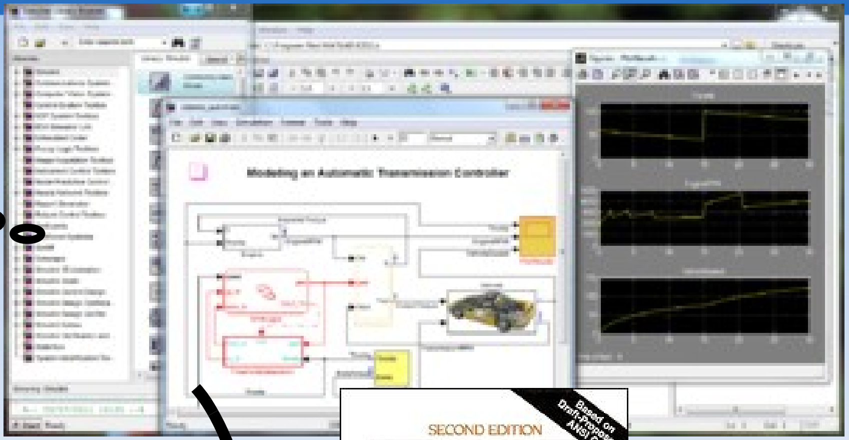




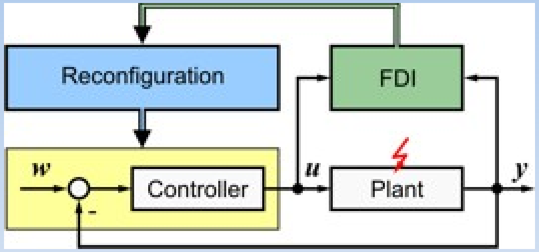
RTOS/
Middleware

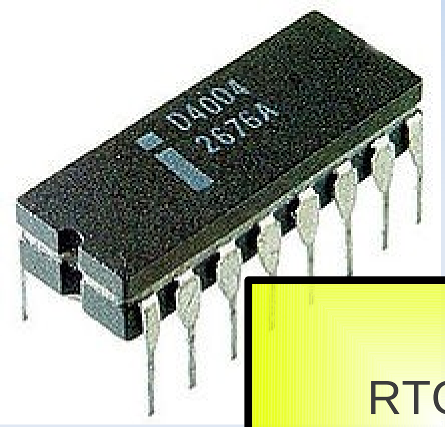
What Is a Control System?

mathematical
model

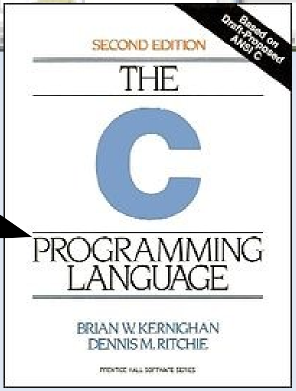


reconfigurable control





RTOS/
Middleware



Based on Draft-Proposed ANSI C

SECOND EDITION

THE

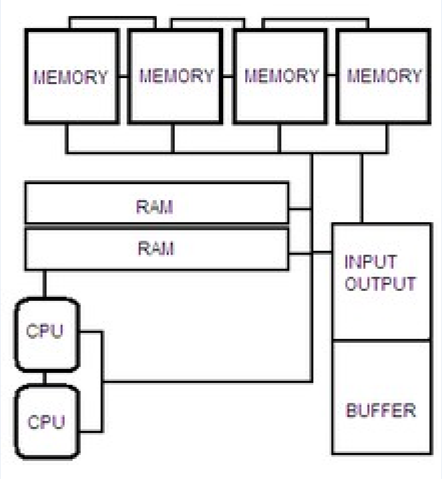
C

PROGRAMMING
LANGUAGE

BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

PRENTICE HALL SOFTWARE SERIES

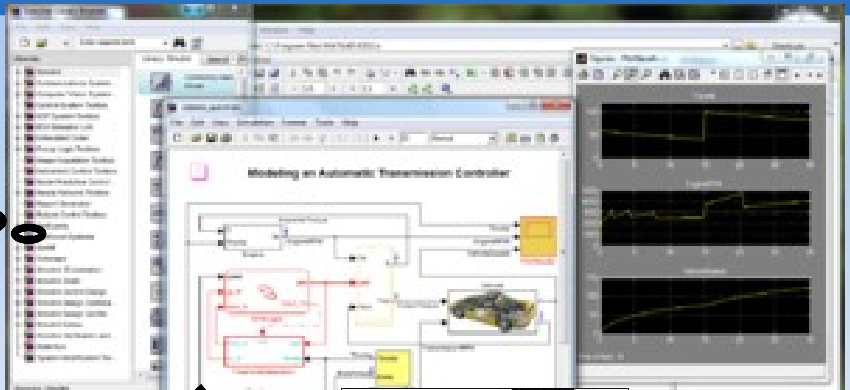
fault tolerance



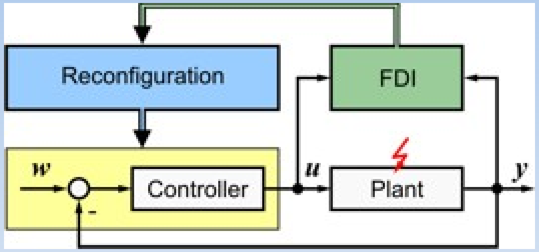
field-bus communication

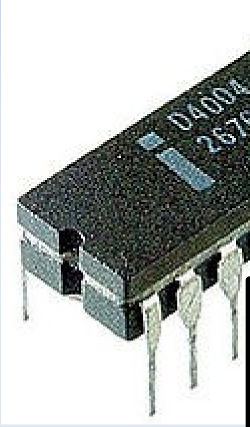
What Is a Control System?

mathematical model

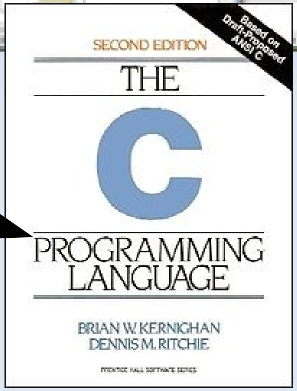


reconfigurable control





RTOS/
Middleware



SECOND EDITION

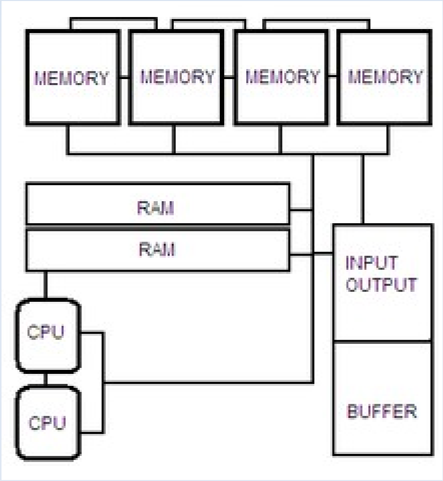
Based on Draft-Proposed ANSI C

THE C PROGRAMMING LANGUAGE

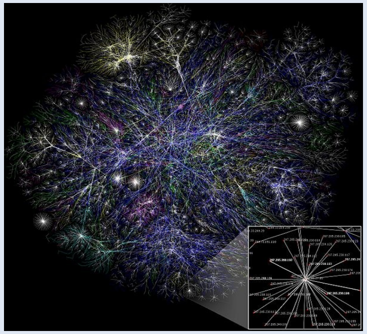
BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

PRENTICE HALL SOFTWARE SERIES

fault tolerance



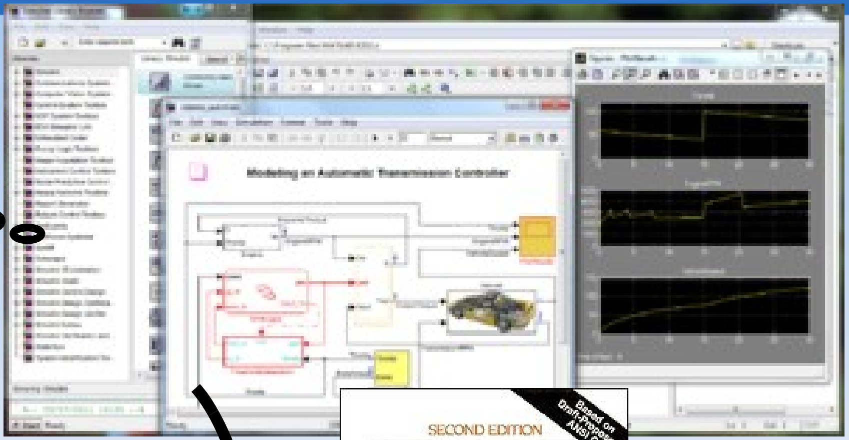
networking



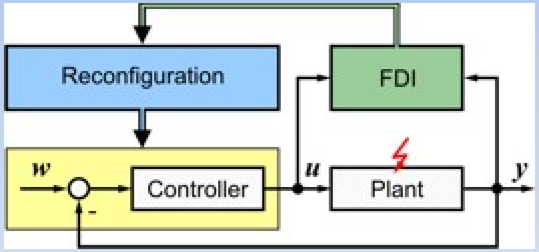
field-bus communication

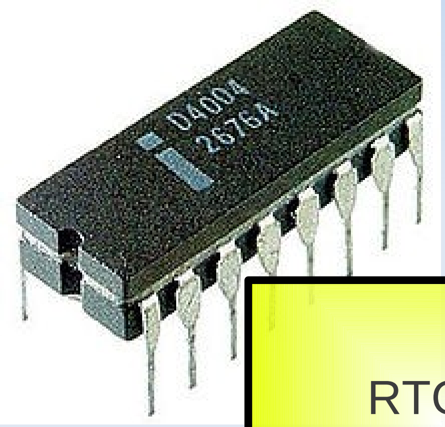
What Is a Control System?

mathematical
model

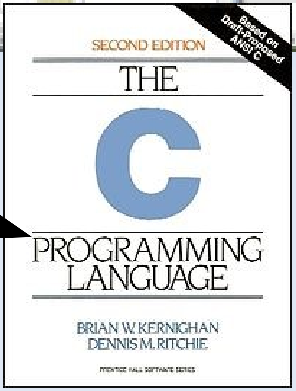


reconfigurable control





RTOS/
Middleware



SECOND EDITION

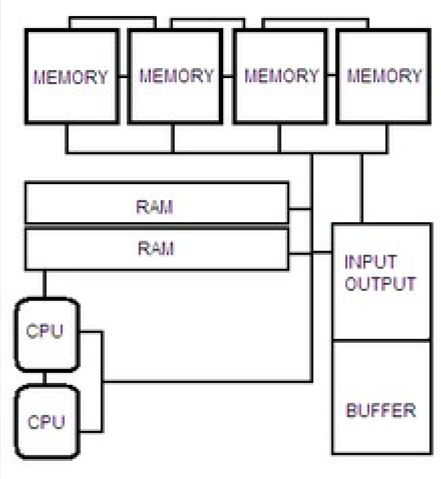
Based on Draft-Proposed ANSI C

THE
C
PROGRAMMING
LANGUAGE

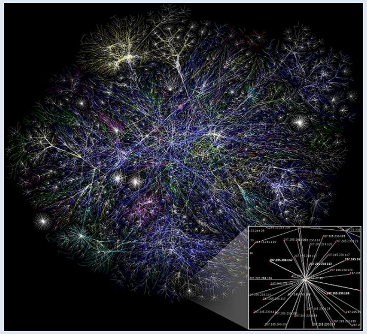
BRIAN W. KERNIGHAN
DENNIS M. RITCHIE

PRENTICE HALL SOFTWARE SERIES

fault tolerance



networking



field-bus communication

power management

Why FMCAD?

- Sweet spot in HW/SW verification
- Researchers need real case-studies to drive tool development
- Something for everyone: interactive theorem-proving, model-checking, decision procedures

Why FMCAD?

- Sweet spot in HW/SW verification
- Researchers need real case-studies to drive tool development
- Something for everyone: interactive theorem-proving, model-checking, decision procedures
- Save lives!

Why FMCAD?

- Sweet spot in HW/SW verification
- Researchers need real case-studies to drive tool development
- Something for everyone: interactive theorem-proving, model-checking, decision procedures
- Save lives!

But...

There's a translation problem!

Themes

- What do control engineers worry about?
  - What *should* they worry about?
- What's the low-hanging fruit for FM?
- Where are tools for designing control systems heading?
- How can FM augment testing/simulation/model-based design as it's done today?

Our Experts

- Darren Cofer, Rockwell Collins
- Eric Feron, Georgia Tech
- Natasha Neogi, National Institute of Aerospace
- Hakan Yazerel, Toyota