

COMPUTER ENGINEERING

COMPUTER CONTROLLED ELECTRIC TRAINS: A TESTBED FOR REAL-TIME SOFTWARE EXPERIMENTATION

SERIS SOFTWARE ENGINEERING FOR REAL-TIME SYSTEMS

E. Rosenfeld, A. Capili, T. Carley/D. Stewart



Objective

To implement a computer-controlled model train testbed on which to test new error handling and detection software architectures for embedded systems.



Motivation

Little has been done towards handling embedded system errors. Consequently, these systems do not even detect them.

How can software know which of these faults cause errors? Can a system recover without a program crashing or system aborting?

- integer overflow
- wrong station
- incorrect signal lights
- power loss to tracks
- sensor not connected
- misaligned sensor
- switch debouncing
- misaligned track
- train hit obstacle on track
- missed station
- missed sensor input
- too late/early
- process starvation
- blown diode
- hill too steep
- load too heavy
- cow on track
- ground problems w/ wiring
- out of memory
- OOPS!** (user error)
- track short
- deadlock
- overheating/fire
- runaway process
- gate not functioning
- I/O module blown
- disconnected wire
- control instability
- unsmooth train motion
- memory corruption
- control instability
- unsmooth train motion
- train derails
- blown fuse
- incorrect train location
- multiple trains on 1 track
- panic button pressed
- blown opto sensor



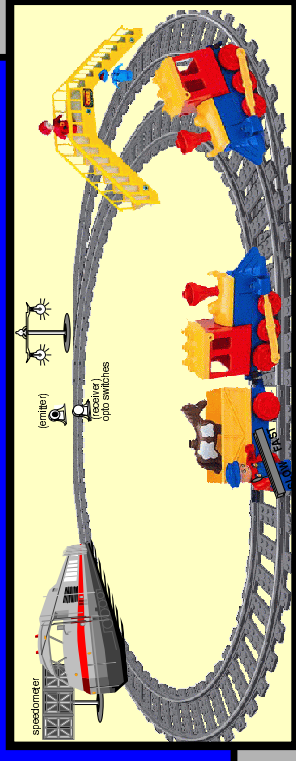
Top Ten Finish
MOTOROLA
Design Contest

Remember Ariane 5??



The rocket exploded seconds after launching due to software errors.

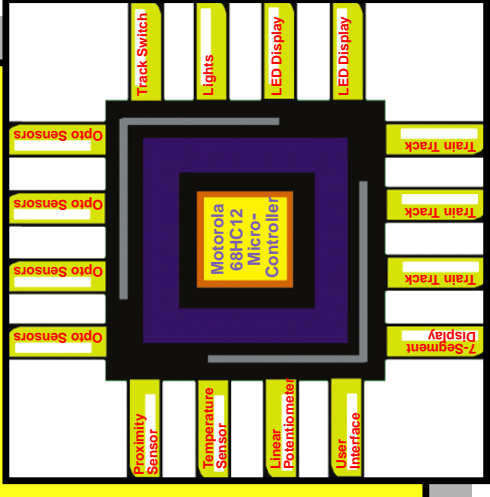
Model Train Testbed



Hardware Features

- Opto and mechanical sensors to detect trains' position
- Pulse width modulator on 68HC12 used to vary train speed
- Train speed measured using controller's timer and opto-to-opto time/distance
- Multiple digital I/O ports for lights, LEDs, 7-segment displays, opto & mechanical sensors
- Analog to Digital Converter on 68HC12 receives input from thermistor and linear potentiometer
- User interface through potentiometer, switches and LED displays

Motorola 68HC12 Architectural Decomposition



Control Flow Diagram for Train Control

