4th SDL and MSC Workshop
SAM’04 Ottawa
1st-4th June 2004

Alkiviadis Yiannakoulias
NTUA
ayian@telecom.ece.ntua.gr
Presentation Layout

- Design issues
- Top level system design
- Use of tool chain (SAFI RE)
  - Implementation
  - Testing / Validation
  - Documentation
- Demonstration
- Summary
Design issues
The door is allowed to be open for a maximum period, once the correct code is entered (Max_Open_Duration_Tmr).

An alarm is generated when the door is not closed within the allowed time.

Time to open or close the door has a maximum value (Transition_Tmr).

Solenoid aborts releasing of lock procedure if door is not moving within the allowed time (Guard_Tmr).
Design issues (Contd.)

- Time is always displayed in the console.

- ACS Commands:
  - Stay Open: Allow door to be open for longer.
    - Information needed:
      - Time (HH:MM),
      - Access Code
  - Close Now: 15 seconds to close door
  - Supervisor mode
Supervisor Mode Commands

1. Double-check safety procedure,
2. Change supervisor code,
3. Statistics for:
   ✓ #Times door open outside,
   ✓ #Times door open inside,
   ✓ When was last opened and how long
4. Set time,
5. Exit.
Design issues (Contd.)

- Use of query mechanism to get door state, for controller state transitions
  - Reduce number of states
  - Data Hiding

- Reset procedure initializes configuration parameters and ACK completion
  - Improve testability
Top-Level Design
ACS Process (Contd.)

- **Door_Closed_ST**
  - ACS_Key_Update_LCD("OPENING DOOR", 1)
  - (Door_Opened_Inside)
  - SX_SBIP_Elapsed_Time_Init

- **Door_Opening_ST**

- **Door_Open_ST**
  - Key_Update_LCD("DOOR FULLY OPENED", 1)

- **Door_Opening_S**

- **Door_Open_S**

National Technical University of Athens
N.T.U.A.
Door Process
Design summary

- Clear organization
- Hierarchical structure
- Data hiding
- Use of types
  - Reuse of design information
- Simple language elements
Documentation of Test Harness
Test harness (UI)
Test harness (SIM)
Documentation of Test Suite / Test Purposes
Test Case Sample
(Door_Opening_TC)
Test Case Sample (Contd.)
Test Report
Test Report
System Execution Trace
Summary of results

- All test scenarios executed (PASS)

- Test coverage
  - All main transitions: timeouts and normal behavior

- Each transition has been tested independently
  - Assumes no interaction between transitions (reasonable as no global variables)
Conclusions

- Maximum usage of tool chain has minimized the effort for:
  - Design, Testing, Documentation

- Interesting challenge on how to keep design simple and use all the tool features to maximize automation