# *Especificação e Verificação de um*

# *Sistema Electrónico de Controlo de Acessos*

# *Trabalho de AMSR*

*FEUP/MRSC/AMSR*
*MPR*



## *Problema a Resolver*

» Problema a concurso
- No SAM '04 – Fourth SDL AND MSC Workshop, Otava 2004
- http://http://www.sdl-forum.org/Events/SAM04.htm
- Com apresentações das soluções vencedoras (ver em “Programme”)

» Mas, adaptado a AMSR ....
- Mais simples ☺
- Especificação em Promela
- Verificação usando o xspin
  - Software e documentação na página de AMSR

# *EACS - Electronic Access Control System*

- The system controls access through a door to a secure area.
- To open the door an access code has to be entered at a console mounted near the door.
- The console has:
  - » a keypad with the digits ‘0’-‘9’, ‘*’ and ‘#’ to enter commands;
  - » a display with 3 lines of 20 ASCII characters;
  - » a tone-generator, able to generate confirmation, warning and alarm tones.
- The door has:
  - » a solenoid controlling the lock on the door;
  - » a micro-switch, which closes when the door is fully closed;
  - » a micro-switch, which closes when the door is fully open;
  - » a motor to open and close the door.



# *EACS - Electronic Access Control System*

- The door can be manually opened, so the lock controls access and the motor provides power assistance. As the motor is an auxiliary mechanism, the ACS does not rely on it working.
- When the door is closed the access code can be entered at the console keypad. The door is allowed to be open for a total of 30 seconds from the point the correct code is entered.
- If the door is not fully closed again within the allowed time, the console assumes it is blocked and generates an alarm tone.
- Tests show the motor takes at most 7 seconds to open or close the door.

# *EACS - Electronic Access Control System*

- To allow the door to open, the solenoid releasing the lock is turned on until the door has started to open. If the door does not start to open within 5 seconds the procedure aborts.
- Inside the secure area is a red, wall-mounted button connected to the EACS, which has the same effect as entering the access code at the console outside.
- The access code is four digits long, where each digit can have a value.
- The console display shows the door status, which may be overwritten briefly with acknowledgements or warnings.



# *EACS - Electronic Access Control System*

- The EACS has two commands:
  - » Stay Open: Allow the door to be open for longer. The command needs additional information for the time the door is allowed to be open for (i.e., HHMM, HH= hours, MM=minutes) and the access code.
  - » Close Now: If the door is open this command allows 15 seconds for the door to close.
- The Access Control System itself works with events and the hardware interface to the micro-switches and console can be assumed to work this way, i.e. to report changes in the state of the micro-switches, generate events for keys pressed and receive events controlling the display and tone-generator.

# *Trabalho em AMSR*

» Em grupo de 2 alunos

» O que deve ser feito
- Especificar o sistema em Promela
- Usando os mecanismos de verificação do XSPIN, demonstrar que:
  - o sistema é seguro (ex. que ninguém entra sem saber o código)
  - o sistema projectado satisfaz todos os requisitos enunciados

» Nota – Este trabalho poderá ser substituido por um outro, proposto pelos alunos, desde que
- Se relacione com um trabalho de mestrado, tese, ou profissional, e
- Seja aprovado pelo professor



# *Trabalho*

» O que deve ser entregue
- Um relatório (**papel + pdf**) que descreva
  - A solução proposta
  - A estratégia de verificação adoptada (ler papers recomendados)
- Em anexo devem ser incluídos
  - A especificação do sistema em Promela
  - Os resultados de verificação obtidos
  - Os traços (sequências de eventos) relevantes