Smart Card Software

Smart Cards software and security issue related to the panel questions:

- Secure and safety critical vs. insecure, non-safety critical embedded systems: Do they require completely different design approaches?
Smart Card Software

1st step: pioneer period 1974-1984
• High memory constraints, assembler

2d step: adoption period 1984-1994
• Evolution from “silicon” culture to “software” culture, high level language used

3rd step: large deployment 1994-2004
(more than 1 billion cards on the field today)
On the last period:

- Java was introduced in card as language and model with Cardlet,

- Formal Methods are also used and performed on some specific part of the development:
  - By request (ITSEC and CC) or,
  - By necessity (high level complexity on some part of software platform like firewall, byte code verification, ...).
But the life is not so simple

During all the steps the attackers know how also progress on attacks:

- On failures (!),
- By observation (consumption, SPA, DPA,…),
- By injection of faults.

And what means in term of development?
Come back to the roots!

- Compiler, automated code generator, FM, component approach, … open the door to attacker.

Why?

- PIN_Code_Verification MAY not program in a simple way. The chip behaviors (time, consumption, electromagnetism radiation, …) MUST be identical in any case!
- Developers return to the assembler language where chip comportment MAY be handled.