WELCOME TO THE

SAFE CONTROL SYSTEMS

INVITED SESSION

INTRODUCING TALK

METHODS FOR SAFE CONTROL SYSTEMS

DESIGN AND IMPLEMENTATION

Jean-Marc Faure, Jean-Jacques Lesage

AIM OF THE SESSION
METHODS CLASSIFICATION
OFF-LINE METHODS
- General case
- Discrete Event Systems

SESSION STRUCTURE

AIM OF THE SESSION

Strong industrial demand for safe control systems

Standards specific to industrials field (railway, power conversion, …)

IEC 61508 standard for E/E/PE safety-related systems

- safety life-cycle
- SIL (Safety Integrity Level)

Numerous research results contributing to safety (synthesis and analysis of control systems, fault tolerant systems, redundancy in man-machine systems, …)

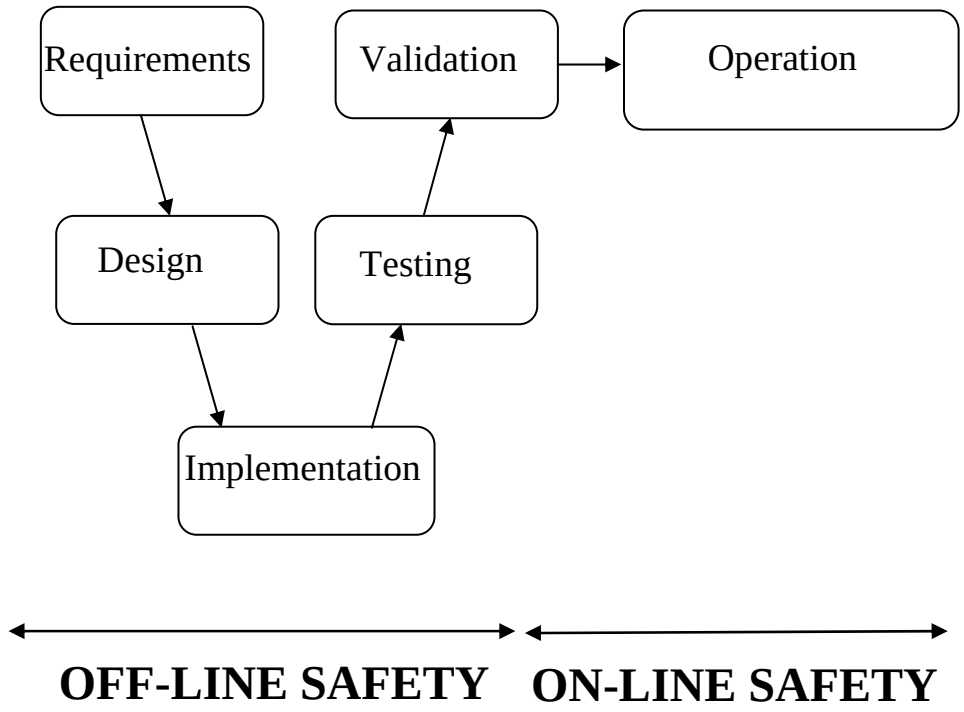
To federate complementary works in the field of safe control systems

METHODS CLASSIFICATION

Life-cycle criterion

Off-line methods aim at minimising the fault risk during realisation

On-line methods are developed to ensure safety in an existing and running system



OFF-LINE METHODS - General case

Verification

Are we building the product right ?

Intrinsic properties (stability, liveness, deadlock, …) checking

Validation

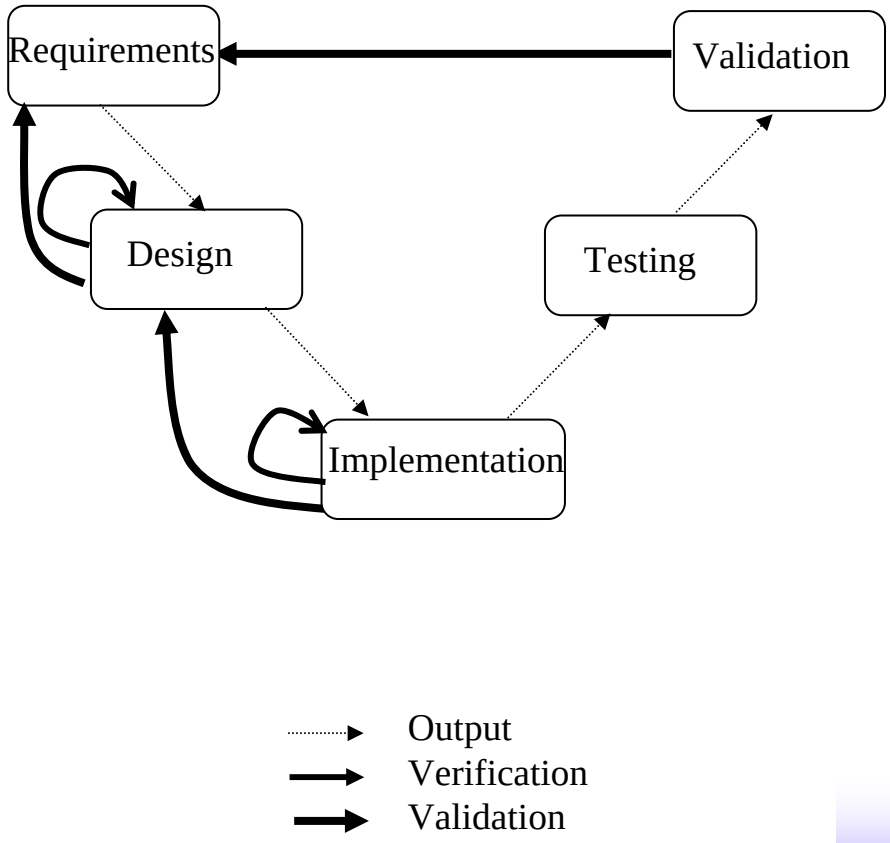
Are we building the right product ?

Consistency checking

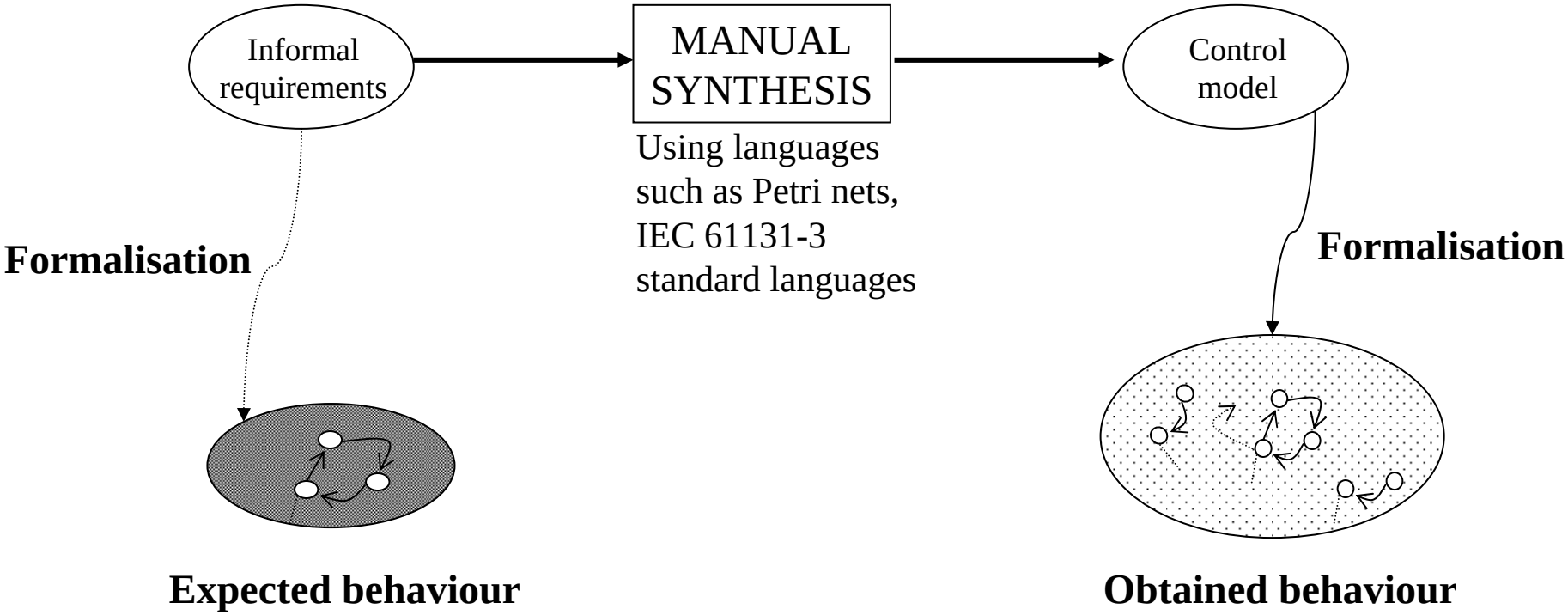
Methodological helps

Useful for project management

Sound formalisation required (especially for validation)



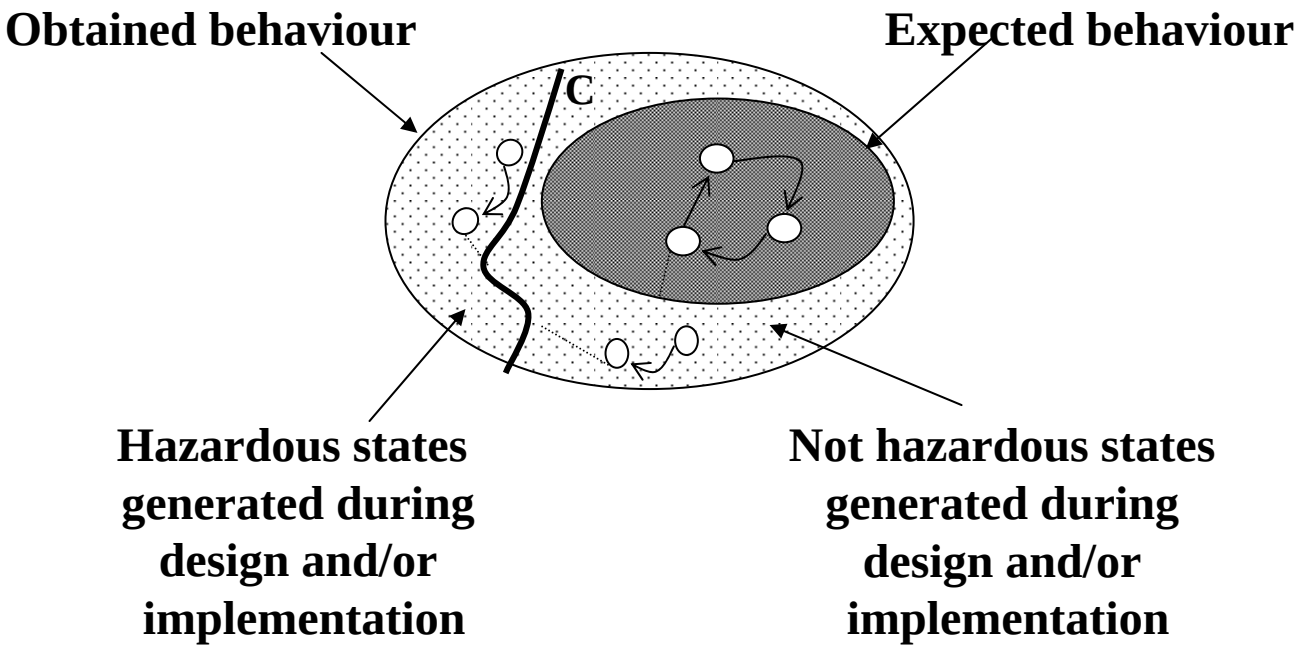
OFF-LINE METHODS - Case of DES (Discrete Event Systems) control



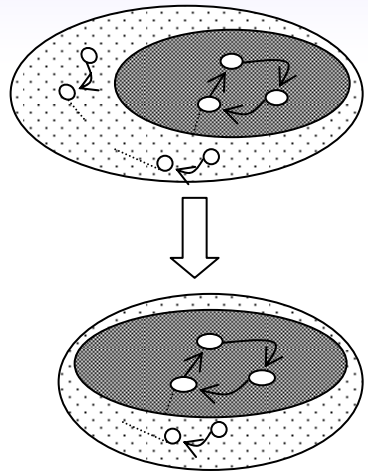
Are there any hazardous differences ?

OFF-LINE METHODS - Case of DES (Discrete Event Systems) control

Safety and state spaces

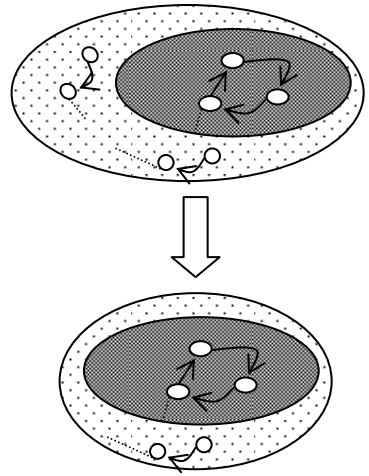


OFF-LINE METHODS - Case of DES
How to insure safety ?



To increase the size of the expected state space

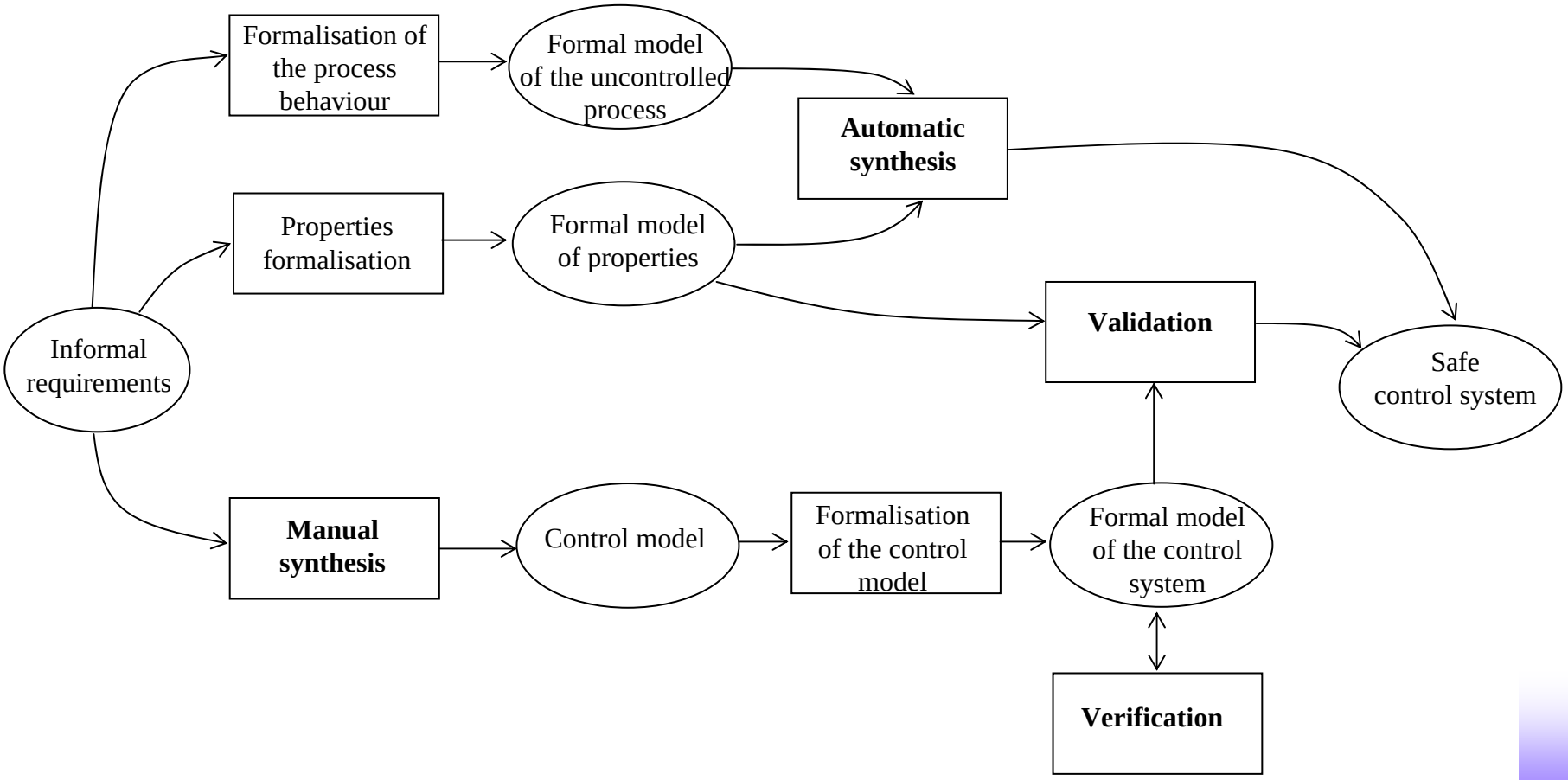
- by using a generic model of the control system
- by defining design or implementation rules



To reduce the gap between the two spaces

- during the elaboration of the control model (a priori checking)
- after this model has been built (a posteriori checking)
  - simulation
  - formal methods (model checking, theorem proving)

OFF-LINE METHODS - Case of DES
Several ways to reach safety



SESSION STRUCTURE

Five talks by researchers from laboratories belonging to GRP (French research group in Production Engineering)

Three papers dealing with OFF-LINE methods

- Bridging the gap between semi-formal and formal
- Automatic synthesis using supervision theory
- Formal verification of industrial control systems

Two papers for ON-LINE methods

- Modes management for fault tolerant systems
- Co-operative redundancy in man-machine systems

Synthesis (open discussion)