Risk Taking in Life-Critical Systems

Risk in Process Control: 
*Do not forget human Imagination*

Prof. Patrick Millot

patrick.millot@univ-valenciennes.fr
pmillot@fit.edu

P. Millot RTLCS March 5, 2014
The present workshop *Risk Taking in Life Critical Systems* results of a collaboration between HCDi at FIT (FL, USA) and LAMIH at the University of Valenciennes (F) and founded by Partner University Found (PUF Face).

It follows a first issue organized at the University of Valenciennes (F) on July 1-5, 2013 by Patrick Millot, Guy A. Boy & Frédéric Vanderhaegen and related to *Risk Management in Life Critical Systems* as shown bellow.

A book is under press:
Organized by:
Patrick Millot, Guy A Boy, Frédéric Vanderhaegen

Secretary:
Philippe Polet, Marie Claude Rossillol, Véronique Landrain, Corine Aureggi
Life Critical Systems belong to domains such as:
- transportation (trains, cars, aircraft flying, air traffic control),
- space exploration, energy (nuclear, chemical engineering),
- health and medical care,
- telecommunication networks,
- cooperative robot fleet, manufacturing,
- and services leading to complex and time-critical issues regarding safety, efficiency and comfort.

Life Critical Systems are potentially highly automated.

We are focusing on “human(s) in the loop” systems and simulations, taking advantage of human ability to cope with unexpected dangerous events on one hand, and attempting to recover from human errors and system failures on the other hand.

Our approach deals with Human-Computer Interaction and Human-Machine System.
Risk management deals with prevention, decision-making, action taking, crisis management and recovery, taking into account consequences of unexpected events.

The approach consists in three complementary steps:

- **prevention**, where any unexpected event could be blocked or managed before its propagation;

- **recovery**, before the event results in an accident, making protective measures mandatory to avoid the accident or to minimize the damages;

- and possibly after the accident occurs, **management of consequences** to minimize or remove the most severe ones. Global crisis management methods and organizations are considered.
STRA TE GY FOR RISK MANAGEMENT

Through Enhancing Resilience:

- Adapted Methods & practices
- Dedicated & adaptive tools
- Flexible Organization
- Human intervention + imagination
An interesting definition of Resilience  (Amalberti 2014 this workshop)
Resilience next challenge (Amalberti 2014 this workshop)
STRATEGY FOR RISK MANAGEMENT

Unëxpected Event \(\rightarrow\) Prevention \(\rightarrow\) Recovery \(\rightarrow\) Consequences management

Predicting & anticipating:
- Maintenance
- Supervision (monitoring, fault detection)
- Barriers (Norms, Procedures)
- DSS: HM Cooperation
- Situation Awareness

Short term corrective Action:
- Procedures
- DSS for event detection, compensation ... HM cooperation
- Support System for action correction (Brakes, Emergency stop...)
- Situation Awareness

Consequence Anticipation:
- System Robustness
- Emergency Care
- Containment devices...
Human Centered Design Approach for Risk management

PARAMETERS RELATED TO HUMAN MACHINE SYSTEMS:
- Technical aspects (Complexity, Reliability, Criticality, Safety, Security…)
- Human aspects (physical, cognitive, social)
- Human-machine Interaction (Task, Organization, Situations)

PARAMETERS INFLUENCING H-M INTERACTION
- Understanding the system complexity
- Understanding the Human complexity
- Levels of Automation, Autonomy, Authority

HUMAN OPERATOR ROLES
- Negative role = human error
- Positive role = human capability to detect and recover technical as well as human errors
Levels of automation (LOA) (Sheridan, 1992) and AUTHORITY

1. The computer offers no assistance; human must do it all.
2. The computer offers a complete set of action alternatives, and
3. narrows the selection down to a few, or
4. suggests one, and
5. executes that suggestion if the human approves, or

...... Human may not always be maintained as the final Authority......

6. allows the human a restricted time to veto before automatic execution, or
6.5 executes automatically after telling the human what it is going to do, or
7. executes automatically, then necessarily informs humans, or
8. informs him after execution only if he asks, or
9. informs him after execution if it, the computer, decides to.
10. The computer decides everything and acts autonomously, ignoring the human.
Levels of automation (LOA) and AUTHORITY (revisited by Moray Inagaki Itoh 00)

1. The computer offers no assistance, human must do it all.
2. The computer offers a complete set of action alternatives, and
   narrows the selection down to a few, or
4. suggests one, and
5. executes that suggestion if the human approves, or

... Human may not always be maintained as the final Authority......

6. allows the human a restricted time to veto before automatic execution, or
6.5 executes automatically after telling the human what it is going to do, or
7. executes automatically, then necessarily informs humans, or
8. informs him after execution only if he asks, or
9. informs him after execution if it, the computer, decides to.
10. The computer decides everything and acts autonomously, ignoring the human.
1. The computer offers no assistance; human must do it all.
2. The computer offers a complete set of action alternatives, and
3. narrows the selection down to a few, or
4. suggests one, and
5. executes that suggestion if the human approves, or

... Human may not always be maintained as the final Authority......

6. allows the human a restricted time to veto before automatic
execution, or
6.5 executes automatically after telling the human what it is going to do, or
7. executes automatically, then necessarily informs humans, or
8. informs him after execution only if he asks, or
9. informs him after execution if it, the computer, decides to.
10. The computer decides everything and acts autonomously, ignoring the human.
Example of Car Driving and road safety management:
Example of Car Driving and road safety management:

ABV project: Automated driving at low speed (LT 50 km/h)
Human Centered Design Approach for Risk management

PARAMETERS RELATED TO HUMAN MACHINE SYSTEMS:

- Technical aspects (Complexity, Reliability, Criticality, Safety, Security…)
- Human aspects (physical, cognitive, social)
- Human-machine Interaction (Task, Organization, Situations)

PARAMETERS INFLUENCING H-M INTERACTION

- Understanding the system complexity
- Understanding the Human complexity
- Levels of Automation, Autonomy, Authority

HUMAN OPERATOR ROLES

- Negative role = human error
- Positive role = human capability to detect and recover technical as well as human errors
HUMAN OPERATOR ROLES

- Negative role = human error
- Positive role = can detect and recover human errors as well as technical errors

Automation dilemma

adapted from G. Boy
HUMAN OPERATOR ROLES
- Negative role = human error
- Positive role = can detect and recover human errors as well as technical errors

Automation dilemma:
- Balanced Level Of Automation
- Decision Support System (DSS)
- Human-DSS cooperation
- Situation Awareness
Team – Situation Awareness (Salmon et al 2008)

Data

SA Development
- Perception
- Comprehension
- Projection

Taskwork

Individual SA
- Team member A
- Team member B
- Team member N

Teamwork

Team Processes
- Communication
- Collaboration
- Co-operation
- Shared mental models

Team SA
- Individual SA
- SA of other Team members
- SA of entire Team
- Common/Shared Picture
HUMAN OPERATOR ROLES
- Negative role = human error
- Positive role = can detect and recover human errors as well as technical errors

Automation dilemma:
- Balanced Level Of Automation
- Decision Support System (DSS)
- Human-DSS cooperation
- Situation Awareness & Human imagination
Besides Technical Supports & H M Cooperation...

... Enhance Human Situation Awareness & Human Imagination ...

An approach to DSS for Nuclear Power Plant simulator ... revisited ...
Nuclear Power Plant Principle
Alliance Project: the Process
NPP simulator: 700 instrumented variables
Supervision team in the control room

- 1 chief Engineer  head of the team (KBB: deep knowledge in nuclear physics and control engineering)

- 2 technicians (RBB: good knowledge on procedures)

- 1 operator make rounds in the plant (rondier)

- Work schedule:
  3 periods of 8 hours / day,  7days / week
Two parts of the Human operators supervision tasks (what they are supposed to do!)

1) Monitoring (surveillance) in order to detect a defect
2) Trouble shooting:
   - Perception of relevant information
   - Diagnosis (Understanding what happens)
   - Prognosis (Projection of future state)
   - Decision making (chose, formulate an action or a sequence of actions, … or invent it)
   - Application of the action
   - … and monitor the action effect (return to the top)
Two parts of the Human operators supervision tasks
(what they are supposed to do!)

1) Monitoring (surveillance) in order to detect a defect
2) Trouble shooting:
   - Perception of relevant information
   - Diagnosis (Understanding what happens)
   - Prognosis (Projection of future state)
   - Decision making (chose, formulate an action or a sequence of actions, ... or invent it)
   - Application of the action
   - ... and monitor the action effect (return to the top)
Variable temporal evolution and Alarm Thresholds for monitoring and fault detection

P04 (t)

HEST  High Emergency Stop Threshold

HAT  High Alarm Threshold

t (min)

LAT  Low Alarm Threshold

LEST  Low Emergency Stop Threshold

Set Value P0A
Effect of the malfunction on variable var(t)

A malfunction occurs

HAT risks to be crossed ... Alarm

- HEST: High Emergency Stop Threshold
- HAT: High Alarm Threshold
- LAT: Low Alarm Threshold
- LEST: Low Emergency Stop Threshold

Var(t)
Set Value

P. Millot RTLCS March 5, 2014
Alliance Project: Decision Support System Functionalities (DSS)

. Prediction capabilities through a process model simulation

. Provides a diagnosis and preventive advices based on Qualitative Physics principle (Gentil, Montmain 04)
DSS for trouble shooting

DSS

HMI Animation Program

Fact Base

Process Data Base

Supervision and Control Computer

Process

Human supervision team

Animated images Adviices

Navigation Commands Requests

Control

P. Millot RTLCS March 5, 2014
Human-DSS Cooperation: a vertical structure

Human Operator: decisions

Automated Process

Performance

Objectives

Orders Assistance requirements

Know-How

Advises

Decision Support System

Know-How

Production

P. Millot RTLCS March 5, 2014
Scenario of unknown malfunction on Var(t)

A malfunction occurs...

HAT is crossed ... Alarm

HEST
HAT
LAT
LEST
Monitoring View of the Process Operation and Fault Detection (1)

Regular Star-View of the 7 significant variables

Normal operation mode

P. Millot RTLCS March 5, 2014
Monitoring View of the Process Operation and Fault Detection (2)

Irregular Star-View of the 7 significant variables

Abnormal operation mode

P. Millot RTLCS March 5, 2014
Projection of future state: Star-view Animation

Prediction Date $T_p$

$T_p+1$ minute

$T_p+4$ minutes

$T_p+5$ minutes

P. Millot RTLCS March 5, 2014
### Monitoring Screen

#### Variable: Dna4
- **Action**: U pem03
- **Sens**: -1
- **Avant**: +2:20

#### Variable: Tna15
- **Action**: C-P02
- **Sens**: +1
- **Avant**: +3:30
H-M Cooperation structure: a vertical one

Human Operator decisions

Automated Process

Possible conflict?

Orders Assistance requirements

Performance

Objectives

Know-How

Advices

Decision Support System

Know-How

Production

P. Millot RTLCS March 5, 2014
H-M Cooperation structure: a vertical one

- Objectives
- Performance
- Human Operator decisions
  - Decision Support System
    - Know-How
    - Orders Assistance requirements
    - Know-How to Cooperate
  - Advices
  - Automated Process
- Production

P. Millot RTLCS March 5, 2014
Synthesis of the decisional conflict pathway between the HO and the DSS

P. Millot RTLCS March 5, 2014
1rst justification level: Propagation View

Defect propagation Network on a Simplified Process Synopsis
2nd justification level: significant variables

. Historic
. Prediction
But, what happens when neither DSS nor Human have a solution? ...

... the Human must deal with the problem!

... s/he must develop a strategy for Risk taking & invent a solution
Scenario of a malfunction not solved by DSS (1)

A malfunction occurs HAT is crossed

Var(t)

Set Value

HEST

HAT

t (min)

LAT

LEST

P. Millot RTLCS March 5, 2014
Scenario of a malfunction not solved by DSS (2)

A malfunction occurs

Increasing risk for system

Increasing risk for human operators

HEST

HAT

t (min)

LAT

LEST

HEST risks to be crossed

Var(t)

Set Value

Var(t)
Scenario of a malfunction not solved by DSS (3):
HO has no solution but adopt a strategy to save time
Scenario of a malfunction not solved by DSS (4): HO applies the strategy to save time

Set Value

Var(t)

Var(t) occurs

Stabilize to save time

A malfunction

Command

HEST risks to be crossed

HEST

HAT

t (min)

LAT

LEST

P. Millot RTLCS March 5, 2014
2nd example in Air Traffic Control

A cooperative function allocation between human controllers & a dedicated DSS showed:

- DSS & a coherent cooperation with the humans increase performance: air misses (errors) were divided by 2 ... but errors remain

- A cognitive analysis of the controllers activities showed:
  - The Controllers do not have any lack of expertise: they always know the solution
  - But, as they solve the problem in anticipation, the risk is they forget a problem, i.e.: to apply the solution at the right time
Lessons & discussion

- Even with Support systems and experts in the supervision loop, systems have limits and risk does not disappear

- In Process control,
  - managing Risks needs humans in the loop,
  - designers should take the operators real Needs into account when designing
  - Designers should allow more liberty to human Imagination


References (2)


