Safety and Reliability of Autonomous Maritime Transportation: Human Still in the Loop

Ali Mosleh
Distinguished Professor
Evelyn Knight Chair in Engineering
Director, The B. John Garrick Institute for the Risk Sciences
University of California, Los Angeles

Keynote Presented at ICTIS 2017
The 4th International Conference on Transportation Information and Safety
August 8th-August 10th 2017
Banff, Alberta, Canada
One of the inherent characteristics of all engineered system is the inevitability of interface with humans; in design, in operation, in intended use, and unintended effects.

Autonomous systems are not immune, even though one of the main motivations and the core design feature of such systems is to eliminate or reduce the need for human operators.
Autonomy

«A system’s or sub-system’s own ability of integrated sensing, perceiving, analyzing, communicating, planning, decision-making, and acting, to achieve its goals as assigned by its human operator(s) through designed human-machine interface (HMI)"
Modern Engineered Systems

Interactions

Hardware

Software

Environment

Human
X-ware Systems

Definition: systems constituted of interacting components of hardware, software and human operators.

Interactions in X-ware system are mutual or reciprocal actions and/or influences in relation to certain functional, physical, and/or environmental interfaces which generally result in exchange of matter, energy, force, or information.
Failures of X-Ware Systems

Mars Polar Lander Crash on Mars

CRH D310 rear-ended CRH D3115 in 2011, China, 35 died, 211 injured
More on Modern Engineered Systems

- Socioeconomic Environment
- Regulatory Environment
- Physical Environment

SYSTEM
Maintenance ↔ Operation
ORGANIZATION
A Probabilistic Scenario-Based Method for Understanding the Complexity

• Determine potential *undesirable consequences* associated with use of systems and processes
• Identify *scenarios* where such consequences could materialize
• Estimate the *likelihood* (e.g., probability) of such events
• Provide *input to decision* makers on optimal strategies to reduce the levels of risk
Modeling Scenarios: The ESD Methodology

Generic Scenario

Undesired Aircraft States

Event causing deviation from normal operation (initiating event)

A

B

C

F (failure/accident)

Recovery

ESD Model
Detailed Causal Relations

Human, Organizational, and Regulatory Environment

SYSTEM

A Fails due to Inherent Causes
B Fails due to Inherent Causes
A Fails due to Organizational Factors
B Fails due to Organizational Factors
Organization

Fault Tree

Influence Diagram (e.g., BBN)
Modeling with Bayesian Network

Compact and seamless integration of the data model and System model
Software Failure Modeling

Functional Decomposition

Requirement Analysis of TRAC-M Level Controller-Design

X(1) (m): Vessel Water Level

X(2) (g/sec): Current time step head-water line mass flow rate (MM/h)

X(3) (g/sec): Current time step steam line mass flow rate (MM/h)

Cbcen1 (m): Water level set-point

Cbcen2 (g/sec): nominal steady state level-water line mass flow rate

©UQAM/ nkecedi
The European Maritime Safety Agency points to human error as the triggering factor in 62% of incidents involving EU-registered ships from 2011 to 2016.

Removing the human operator in all or majority of operational tasks is believed to prevent or reduce the likelihood of such accidents.
Example Autonomous Ship Projects

- **MUNIN (Maritime Unmanned Ships through Intelligence in Network)**
  - Collaborative research project, co-funded by the European Commissions under its Seventh Framework Program.
  - Aims to develop and verify a concept for an unmanned *autonomous merchant ship*.

- **DNV GL ReVolt project**
  - Developing a concept for an unmanned, zero-emission, *shortsea autonomous vessel*.

- **AAWA (Advanced Autonomous Waterborne Applications Initiative)**
  - Started by Rolls Royce.
  - Developing specifications and possible designs for the *next generation autonomous ships*.
While existing autonomous ship concepts have different views on how they should be operated in terms of autonomy level, in all cases human is still part of the system.

Examples include retained operator roles for some voyage phases (e.g., departure, and docking) or for taking over control in specific circumstances.

Therefore, autonomous ship operations would not be totally free of the possibility of accidents generated or aggravated by human error.

Analyzing the potential for human error, through a Human Reliability Analysis (HRA), is therefore important in ensuring the reliability and safety of autonomous ships.
AAWA Concept

Umanned during all voyage
Dynamic level of autonomy

Example: one phase of the voyage is set to be fully autonomous but the operation encounters a small problem and give the operator a “veto” option before solving it autonomously

<table>
<thead>
<tr>
<th>Level of Autonomy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Fully manual control</td>
</tr>
<tr>
<td>2</td>
<td>The computer offers a complete set of decision/action alternatives.</td>
</tr>
<tr>
<td>3</td>
<td>The computer narrows alternatives down to a few</td>
</tr>
<tr>
<td>4</td>
<td>The computer suggests one alternative</td>
</tr>
<tr>
<td>5</td>
<td>The computer executes that suggestion if the human approves</td>
</tr>
<tr>
<td>6</td>
<td>The computer allows the human a restricted time to veto before automatic execution</td>
</tr>
<tr>
<td>7</td>
<td>The computer executes automatically, then necessarily informs the human</td>
</tr>
<tr>
<td>8</td>
<td>The computer informs the human only if asked</td>
</tr>
<tr>
<td>9</td>
<td>The computer informs the human only if it decides to</td>
</tr>
<tr>
<td>10</td>
<td>Fully autonomous Control</td>
</tr>
</tbody>
</table>

Voyage planning
Unmooring and maneuvering out of harbor
Operations mode at open seas
Port approaching and docking

Phases of the Voyage
Voyage planning

- ensure that there is sufficient connectivity for the intended mission
- defining which legs shall be operated in remote control and which are executed autonomously.
- define navigational strategies along with fallback strategies for each leg

Unmooring and maneuvering out of harbor

- the operator can either have direct remote control or supervisory control
- In some areas it is potentially also feasible to go directly to autonomous mode instead of starting with teleoperation or supervisory control.

Operations mode at open seas

- the autonomy level of the vessel is high as long as the mission execution is proceeding according to the plan made by the operator.
- Veto Situation: vessel is deviating from the planned course but stays within specified margins the autonomous navigation system only notifies the operator and gives a possibility to veto for a limited time.
- Pan Pan Situation: if extremely large number of objects are detected and the path planning algorithms are not capable to identify them and thereby the system cannot determine how the navigation should proceed, the vessel will immediately send a “pan-pan” message to the operator indicating that it is in urgent need of assistance.

Port approaching and docking

- the operator can again choose to take teleoperation type control or increase the supervision level of the vessel, or it can be totally autonomous.
Human Error

- A significant factor in reliability for a number of industries; Power, Aviation, Manufacturing, Transportation
- Accounts for more than 50% of the industrial accidents
- An issue in different phases of a system life cycle
  - Design
  - Construction
  - Operation
  - Management
  - Maintenance
  - Decommissioning/Disposal
Examples of Error Modes and Their Impact

- **Error Modes**
  - Skipping procedural steps
  - Shortcut
  - Misdiagnosis
  - Delayed or premature execution of needed action
  - Error in executing an action given correct intention
  - Malicious intent

- **Impact on System (Time Dimension)**
  - Active (driver fails to brake)
  - Latent (brake inoperable due to mechanics error during repair or service)
HUMAN RELIABILITY ASSESSMENT (HRA)

- Identify human response (errors are the main focus) in probability safety assessment context
- Estimate failure (error) probabilities to be integrated into reliability
- Identify causes of errors to support development of preventive or mitigating measures

Related Disciplines:
- Human Factor Engineering
- Ergonomics
- Psychology
Main Elements of Conventional HRA Techniques

- Task Analysis
- Identification of Error Modes and, if Possible, Error Mechanisms
- Identification of Performance Influencing Factors (PIFs)
- Quantification of Error Probability and Uncertainty
- Incorporation of Results into Reliability /Safety /Risk Models
- Ranking of Contributors for Cost Effective Improvements
Task Analysis

- In collaboration with system analysts,
  - understand the scenarios
  - identify the important human-system interactions
  - specify the context and identify possible deviations of the human decisions and actions
  - identify the scenario context within which human error is likely and is significant to system safety

- If necessary decompose the overall response scenario into a few more basic events (e.g., actions) for analysis (analysis units)
  - Most HRA methods require task decomposition.
Three Types of Human Response

- An individual responses to a situation normally has three dimensions:
  - **Cognitive**: mental activities to understand the situation and plan/decide on action
  - **Emotional**: conscious and non-conscious feelings
  - **Physical**: the physical responses to the situation (movement, sound, etc.)

- These three types of activities are inter-dependent
Human Error

- Human error in HRA is a deviation of human behavior from the required or expected performance.

- The required or expected human performance is:
  - context-dependent
  - does not mean the best solution

- Error does not necessarily make things worse.
Examples of Human Error Classification (1/2)

- Intentional and unintentional errors
- Errors of Omission (EOOs) and Error of Commission (EOCs)
  - EOOs: Failure to take required actions
  - EOCs: Actions which should not be taken
- Skill-, Rule-, and Knowledge-Based Errors
  - Skill-Based Errors: Errors in performing highly skilled motor activities associated with achieving a goal
  - Rule-Based Errors: Errors in performing structured approach to achieving a goal
  - Knowledge-Based Errors: Errors in performing highly cognitive efforts to achieve a goal
Example of Error Classification (2/2)

- **Slip**
  - Errors due to attention failure (e.g., pushing the wrong button)

- **Lapse**
  - Errors due to memory failure (e.g., performing tasks in wrong order, skipping required actions, and delaying of action)

- **Mistake**
  - Errors due to failure of judgment (e.g., biased decisions)

- **Violation**
  - An intended action that has taken place in breach of a set of rules
    - Exceptional violation
    - Routine Violation: usually due to social forces (e.g., ignoring organizational or industrial practices)

- **Sabotage**
  - Willful actions to harm the system
Error Modes and Error Mechanisms

- **Error Mode:**
  - The functional form of error (or human failure)
  - Usually referred to as the visible causes that degrade system performance
  - Specific types and taxonomy depend on the classification system of the given methodology
    - E.g., EOO/EOC, action timing error, and action sequence error

- **Error Mechanism:**
  - The conditions, paths, or processes that lead to the occurrence of an error mode
  - Often refers to invisible underlying causes of error modes
    - E.g., failure in attention; failure in situation assessment
  - In principle requires a causal model to identify

- Sometimes used interchangeably
Error and Cause Identification

- HRA methods provide framework for error identification
- An explicit causal model is provided in some HRA methods to identify error causes
- Examples:
  - CREAM (Cognitive Reliability and Error Analysis Method)
  - IDA (Information, Decision, and Action)
Error Identification According to CREAM

- Errors are classified at the level of physical actions
  - Timing (e.g., too early, too late, and omission)
  - Duration (e.g., too long, too short)
  - Force (e.g., too much, too little)
  - Distance (e.g., too long, too short)
  - Speed (e.g., too fast, too slow)
  - Direction (e.g., wrong direction)
  - Object (e.g., wrong acted object)
  - Sequence (e.g., wrong action sequence)
Cognitive Process According to IDAC

Cognitive Engine Is Updated by the Perceived Information

System or Other Crew Member

Cognitive Activities Change Cognitive Engine State

Cognitive Engine (Mental State + Working Memory)

Goal

Strategy

output

Action

Operator's Action Changes System State or Other Crew Member's State
IDAC-Based Error Reference Points

External Error Reference Points

- System
- Procedure
- Crew

Internal Error Reference Points

- Diagnosis
- Decision
- Action

Process:
1. Information
2. Decision
3. Action

Flow:
1. (1) Information
2. (2) Decision
3. (3) Action

(1) External Error Reference Points
(2) Internal Error Reference Points
Human Error in IDA Model

# Mismatch between Action and System Need
1. Failure of A (Error In Execution)
2. Failure of A due to Error in D
3. Failure in D
4. Failure of D due to failure of I
5. Failure in I
6. Incorrect I from External Source

• Skip Step
• Delayed
• Premature
• Wrong Object
• etc.

Recovery
# Crew Activities, IDA phases, CFMs

<table>
<thead>
<tr>
<th>Types of crew activities</th>
<th>Human Response Model (IDA)</th>
<th>Information Processing (I)</th>
<th>Diagnosis/Decision making (D)</th>
<th>Action Taking (A)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Noticing / Detecting / Understanding</td>
<td>Situation assessment / Diagnosis</td>
<td>Decision making / Response planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>I1</td>
<td>I2</td>
<td>I3</td>
</tr>
<tr>
<td>Monitor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect / Observe</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communicate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate / Interprette</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compare</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adapt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adhere</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diagnosis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decide</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coordinate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execute</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Types of crew activities:

- Monitor
- Scan
- Detect / Observe
- Identify
- Communicate
- Evaluate / Interpret
- Record
- Compare
- Verify
- Adapt
- Adhere
- Diagnosis
- Decide
- Plan
- Coordinate
- Execute
- Regulate
- Maintain

### Human Response Model (IDA):

- **Information Processing (I)**
  - Noticing / Detecting / Understanding
  - I1: Key Alarm not Responded to (intentional & unintentional)
  - I2: Data Not Obtained (Intentional)
  - I3: Data Discounted
  - I4: Decision to Stop Gathering Data
  - I5: Data Incorrectly Processed
  - I6: Reading Error
  - I7: Information Miscommunicated
  - I8: Wrong Data Source Attended to
  - I9: Data Not Checked with Appropriate Frequency

- **Diagnosis/Decision making (D)**
  - Situation assessment / Diagnosis
  - D1: Plant/System State Misdiagnosed
  - D2: Procedure Misinterpreted
  - D3: Failure to Adapt Procedure to the situation
  - D4: Procedure Step Omitted (Intentional)
  - D5: Deviation from Procedure
  - D6: Decision to Delay Action
  - D7: Inappropriate Strategy Chosen

- **Action Taking (A)**
  - Action taking
  - A1: Incorrect Timing of Action
  - A2: Incorrect Operation of Component/Object
  - A3: Action on Wrong Component / object
High Level Event Sequence Model

- Successful voyage planning
- Successful manoeuvring ship out of harbor
- Successful Open Sea Voyage
- Successful Port Approaching and Docking

«veto» or «pan pan» situation on following phases
Voyage Planning

Operator is right
Operator is wrong

Op. goes autonomous
Docking goes autonomous
Unmooring goes autonomous

Operator is right
Operator is wrong

Op. goes autonomous
Docking goes manual
Unmooring goes manual

Operator defines appropriate navigation
Operator defines inappropriate navigation

Operator defines appropriate fallback strategy
Operator defines inappropriate fallback strategy

Operation is cancelled due to operators’ belief that there is no sufficient connectivity.
Decisions that will increase the probability of having problems ahead (in unmooring, open sea operation or port approaching and docking).
The operator is not correct but this will not bring major consequences ahead (in this case, resources and time will be consumed in a manual operation that could be autonomous).
Correct paths/decisions
Autonomous unmooring and maneuvering out of harbor

The operation goes without any problem

The operation encounters a problem

Small problem – «veto» alert and autonomous solving

Complex scenario – «pan-pan» alert

Operator gives «veto» and takes control – manual operation

Operator responds and does not give «veto» - autonomous solving

Operator does not respond - autonomous solving

Operator Takes control – Manual operation

Fallback strategy + operator supervision

Operator does not respond – fallback strategy

Succesful manual operation

Unsuccesful manual operation

Operator gives «veto» and takes control – manual operation

Operator responds and does not give «veto» - autonomous solving

Operator does not respond - autonomous solving

Succesful autonomous operation

Unsuccesful autonomous operation

Succesful fallback operation

Unsuccesful fallback operation

Succesful fallback operation

Unsuccesful fallback operation

Succesful manual operation

Unsuccesful manual operation

Succesful manual operation

Unsuccesful manual operation

Succesful manual operation

Unsuccesful manual operation

Succesful manual operation

Unsuccesful manual operation

Succesful manual operation

Unsuccesful manual operation

Succesful manual operation

Unsuccesful manual operation

Succesful manual operation

Unsuccesful manual operation

Succesful manual operation

Unsuccesful manual operation

Succesful manual operation

Unsuccesful manual operation

Succesful manual operation

Unsuccesful manual operation
# Human Failure Events: Voyage Planning Phase

<table>
<thead>
<tr>
<th>Human Failure Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to correctly assess connectivity level</td>
<td>The operator is wrong about the low level of connectivity. The operation goes on, and the low level of connectivity can lead to communication problems between the SCC and the ship.</td>
</tr>
<tr>
<td>Failure to correctly define primary strategy</td>
<td>During definition of the primary strategy for each leg the operator believes the conditions are adequate for autonomous operation when, in that situation, it should be manual (tele-operated)</td>
</tr>
<tr>
<td>Failure to define adequate navigational strategy</td>
<td>The operator defines an inadequate navigation strategy. This will increase the probability of having problems ahead and a “veto” or “pan-pan” situation</td>
</tr>
<tr>
<td>Failure to define adequate fallback strategy</td>
<td>The operator defines an inadequate fallback strategy. In case there is a “pan-pan” situation the fallback strategy will be followed by the ship, if the operator does not take manual control of the ship</td>
</tr>
</tbody>
</table>
# Human Failure Events: Navigation Phase

<table>
<thead>
<tr>
<th>Human Failure Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to respond to an alert</td>
<td>The operator does no respond to an alert, which may be a “veto” alert or a “pan-pan” alert.</td>
</tr>
<tr>
<td>Failure to remote-operate the ship</td>
<td>The operator is manually operating the ship, which may be after a “veto” or a “pan-pan” alert or may be from the beginning of that operation, in case it was defined to be manual.</td>
</tr>
<tr>
<td>Failure to take over control of the ship when necessary</td>
<td>The operator trusts the autonomous solution or fallback strategy and does not take over control of the ship in a situation where this is needed</td>
</tr>
</tbody>
</table>
Performance Influencing Factors (PIFs)

- Factors that could affect human performance

- Also called Performance Shaping Factors (PSF) or Performance Adjustment Factors (PAF) with slight differences in meaning
Evidence of Stress Affecting Human Behavior
(Yerkes-Dodson Law)

- Optimum level of arousal
- Good performance
- Poor performance
- Simple task
- Complex task
- Low to High level of arousal
Role of PIFs

Causal Model

Human Mind

Action

PIFs as Surrogate
Examples of PIF Classification (1/2)

- **Operator Factors**
  - e.g., Fatigue and Distraction

- **Operational Factors**
  - e.g., Time Constraint

- **Design Factors**
  - e.g., Control/Display Location and Control/Display Arrangement

- **Procedural Factors**
  - e.g., Erroneous Instructions or Directives

- **Training Factors**
  - e.g., Inadequate Knowledge and Training
Examples of PIF Classification (2/2)
(Affecting an Individual Worker within a Team)

- **Personnel**
  - Fitness for duty
  - Knowledge and skill
  - Attention and motivation

- **Resources**
  - Complete, technically accurate and usable procedures
  - Accurate and complete reference documentation
  - Appropriate tools and equipment
  - Supervision
  - Appropriate number of staff to accomplish the work

- **Physical Work Environment**
  - Design of human-system interfaces
  - Appropriate control and environmental factors (e.g., noise, vibration, temperature etc.)

- **Organizational Work Environment**
  - Effective verbal and written communications
  - Inter-group and intra-group coordination
  - An established safety culture
  - Planning and scheduling of work activities

## PIF Groups and Hierarchy

<table>
<thead>
<tr>
<th>Human - System Interface (HSI)</th>
<th>Team Effectiveness</th>
<th>Knowledge/Abilities</th>
<th>Bias</th>
<th>Stress</th>
<th>Task Load</th>
<th>Time Constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSI Input</td>
<td>Procedure Quality</td>
<td>Tools</td>
<td>Communication</td>
<td>Knowledge/Experience/Skill (Content)</td>
<td>Morale/Motivation / Attitude</td>
<td>Stress due to Situation Perception</td>
</tr>
<tr>
<td>HSI Output</td>
<td>Procedure Availability</td>
<td>Tool Availability</td>
<td>Communication Quality</td>
<td>Task Training</td>
<td>Safety Culture</td>
<td>Perceived Situation Urgency</td>
</tr>
<tr>
<td>Tool Quality</td>
<td>Communication Availability</td>
<td>Knowledge/Experience/Skill (Access)</td>
<td>Confidence in Information</td>
<td>Perceived Situation Severity</td>
<td>Cognitive Complexity due to External factors</td>
<td></td>
</tr>
<tr>
<td>Work Place Adequacy</td>
<td>Team Coordination</td>
<td>Attention</td>
<td>Familiarity with or Recency of Situation</td>
<td>Stress due to Decision</td>
<td>Execution Complexity</td>
<td></td>
</tr>
<tr>
<td>Leadership</td>
<td>Physical Abilities and Readiness</td>
<td>Competing or Conflicting Goals</td>
<td>Inherent Execution Complexity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Team Cohesion</td>
<td></td>
<td></td>
<td>Execution Complexity due to External factors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role Awareness</td>
<td></td>
<td></td>
<td>Extra Workload</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Team Composition</td>
<td></td>
<td></td>
<td>Passive Information Load</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Team Training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### KEY

- **Level 1 PIFs**
- **Level 2 PIFs**
- **Level 3 PIFs**
Some Examples of Bias Affecting Human Behavior

- Tendency to concentrate only on the information that is related to their prevailing hypothesis, neglecting other important information
- Giving too much weight to information that supports their predictions
- Holding on to their initial hypothesis, even in the light of contradicting evidence
- Tendency to focus on single, initial faults, ignoring other tasks
- Tendency to extrapolate non-linear functions towards linearity
- Tendency to underestimate situational factors and overestimate personal factors (if it does not involve themselves)
CFM-PIF BBN Model

Direction of influence

CFMs
Primary / Level PIFs
Level 2 PIFs
Level 3 PIFs
Human Operator BN Model (Civil Aviation)
Maintenance Quality BBN (Civil Aviation)
Context Analysis – Crew Response Tree

Event Sequence Diagram / Event Tree

- IE
- SYS A Fails
- HFE 1
- SYS B Fails
- HFE 2

PRA Scenarios

TIME

CRT

Decision / action Points

Crew Response Scenarios

Human Response Model

PIFs

Performance Influencing Factors

Nature of Activity
Failure Modes
Failure Mechanisms

Nature of Activity
Failure Modes
Failure Mechanisms

PRA Model

CRT
Context Analysis – Discrete Dynamic Event Tree

System Hardware State Model

Physical Variables Model

Crew State Model

System Software Model

Branch Points (BP)
- System Hardware State BP
- Physical Variables BP
- Human Action BP
- Software BP
- End State

$P_i \equiv \text{Branch Probability}$

$\text{Prob.(End State)} = P_1 P_2 P_3 P_4 P_5$

$t_i = i \Delta t$

$P_1 P_2 P_3 P_4 P_5$

Temperature $t_i$

$P_1$ $P_2$ $P_3$ $P_4$ $P_5$

0 $\Delta t$ $t_i$

Time
Thank You!
PIF State Representation

- **Quantitative Representation**
  - Use of numbers, integer or floating point, to represent the state of a PIF
  - Various scales are used, e.g., \([1, 5]\), \([1,7]\), and \([0, 10]\)

- **Qualitative Representation**
  - Use of words to describe PIF state
  - Various scales and types of descriptor are used depending on the type of PIF, e.g.,
    - Very Efficient / Efficient / Inefficient / Deficient
    - Low / Medium / High
    - Very Poor / Poor / Neutral / Good / Excellent
SLIM-MAUD METHOD
(Success Likelihood Index Method-Multi Attribute Utility Decomposition)

• Relies on expert judgment

• Procedure includes:
  • Identify the Performance Shaping Factors based on experts judgment
  • Assess the States (PSF₁, … , PSFₙ) and relative importance (weight factor, Wᵢ) of the PSFs
  • Calculate the Success Likelihood Index (SLI) :

\[
SLI(\text{Success Likelihood Index}) = \sum_{j=1}^{M} (\text{PSF}_j) \cdot W_j
\]
Human Error Probability (HEP) is calculated from

\[ HEP = e^{a \cdot SLI + b} \]

Parameters “a” and “b” are constants for a given type of actions.

Actions are classified based on their demands on mental effort (Skill-based, Rule-based, Knowledge-based).