IT in the process control domain

Usability and work environment for process operators

Assignment 3

Bengt Sandblad

http://www.it.uu.se/research/hci
To implement technology in a specific work domain

- What is needed?
- What must be avoided?

- One important example
  - Process control (human control of dynamic complex systems)
Agenda

- A model of human control
- Work environment problems
- Human error and barriers
- Situation awareness
- Alarms
- Design of operator interfaces
- An example
  - Train traffic control
- Assignment 3 specification
ISO 9241:

Remember the definition of usability:

"The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"
This means:

- To successfully design, develop and deploy an information system (IT, computers, technology) we must know and understand:
  - The work domain (context...)
  - The users (situation, needs, competencies...)
  - The goals (of users, organisation...)
Specific contexts

- Some application contexts are especially problematic, and requires special considerations, e.g.
  - Health care
  - Control of complex systems
  - More....
Some examples of complex dynamic control situations

What is complex?
What is dynamic?
Train traffic control
Train traffic control
Train traffic control
Train drivers
HSC bridge design
IT and process control

Dept of Information Technology | Human-Computer Inte
Forest harvesters
Stone crushers
Nuclear power plants
Paper mills
Also health care....
Are there problems?

- Processes are *complex* and *dynamic*.
- Control is indirect, via a *control system* and an *interface*.
- *Demands* are high (speed, accuracy, quality, safety, ....)
- Control systems and operator interfaces sometimes provide *inadequate support*.
- *Operator performance* not always satisfying (optimality, errors...).
- *Work environment* problems.
- More....
What to do?

What are important things to know and do, in order to develop efficient systems in such complex environments?
A model of control

- We need a model that helps us to
  - describe,
  - analyse,
  - design,

control of a complex dynamic system
The GMOC model

To control a dynamic system requires:

• Goal (G)
• Model (M)
• Observability (O)
• Controllability (C)
Goals

- Goals are often complex
- Contains conflicts
- Goals are e.g.:
  - Formal - informal
  - Organisational - individual
- Operators have their own goals...

- To relate design to the goals, we must understand the goals!
Models

- Models are *mental* models.
- Models are individual and subjective.
- Models are (mainly) developed during work. This takes time!
- Different operators often have (very) different models.
- Organisational development of models and control strategies can solve many problems.
Observability

- We can only observe what the interface shows.
- We often lack information and precision in information.
- Often observations require actions.
- We can overview (very) much but remember little.
- Difficulties to identify and understand complex patterns.
Controllability

■ We can only control what the interface allows us to control.
■ We can sometimes only control a process at certain times.
■ Different control modes can cause confusion.
■ Time delays make control complex.
■ Problems with feed-back.
Work environment

- Physical
  - Ergonomics
- Psychosocial
  - Support
  - Group
  - Leadership
- Cognitive
  - Support operators work
  - Provide prerequisites for efficient work

- We must provide a good work environment for the operators.
A good and healthy work

- Karasek & Theorell:

Here *control* is especially important. Control over: process, work situation, work environment, work planning, work processes, systems and tools etc.

Demands are almost always high. Support must be strong.
A bad and dangerous work
Some important concepts

- **Human error**
  - See e.g. Reason, J., 1990
  - See e.g. S Dekker, 2006

- **Barriers**

- **Resilience engineering**
  - See e.g. Hollnagel, http://www.resilience-engineering.org/

- **Situation awareness**
  - See e.g. Endsley. M.R., 1999

- **Automation problems**
  - See e.g. Bainbridge, L., 1987

- **Alarm systems**

- **User centred development**
Human error (reliability)

- Human errors:
  - Slips (e.g. wrong action)
  - Mistakes (e.g. wrong interpretation of information)
  - Violations (e.g. breaking of rules)

- If it is possible to make an error, it will happen – sooner or later!

- If somebody makes an error – who is to blame?
Barriers

- Two different approaches
  - Prevent the operator from doing wrong
  - Help the operator to act correctly (e.g. “resilience engineering”)

- Technical
- Informational
- Competencies
- Organisation (Culture)
Technical barries – train protection

- Balises in the track gives information about position, signals and max speed.
- ATC-computer calculates break curve.
- ATC-computer "takes over" if the driver do not break in time.
- The driver can not (?) drive against red or drive too fast.
- The driver manually enters train parameters.
Information barrier

Does not show decision relevant info

Shows decision relevant information
Situation awareness

- Situation awareness – to always be “in control”, “in the loop”.

- Three levels:
  - Perception (observation)
  - Comprehension (understanding the significance of the information)
  - Projection (prediction, evaluation of actions)

- Two different approaches to control:
  - Control by exception
  - Control by awareness
Example

- Temperature
  - Static vs dynamic presentation

Temp (°C): +85
Automation problems

- Automation surprises
  - Difficulties to predict
  - Not transparent
- The irony of automation
  - No help when it is most needed...

- E.g. the problems with autonomous automatic systems (autopilots)
- The “turn off” effect
Alarms and alarm problems

- Alarm – warning for something important
- Explain the situation – support adequate actions
- Often one alarm results in many other secondary alarms
- Large disturbances occur seldom
- Many alarms during a short time period
  - 800,000 alarms during the first 2 h after the Harrisburg incident.
  - The operators could not understand the situation
- How to design supportive and “intelligent” alarm systems?
Alarms...

- Cause -> effects not clear
- Many causes are possible
- Mix of many different alarms and sounds
- The alarm list unusable
- Difficult to restore the situation
- Stress
## Alarm List

<table>
<thead>
<tr>
<th>Time</th>
<th>In Alarm</th>
<th>Alarm Description</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 4 High Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 4 Low Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 4 Pump Running Aux Contact Feedback Lost</td>
<td>3000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Temp Tank 4 SP: 0 Actual: 8</td>
<td>4000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 9 High Level Alarm</td>
<td>3000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 9 Low Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 9 Pump Running Aux Contact Feedback Lost</td>
<td>3000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 9 Agitation Did Not Stop On Center Switch</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Temp Tank 9 SP: 0 Actual: 8</td>
<td>4000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 10 High Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 10 Low Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 10 Pump Running Aux Contact Feedback Lost</td>
<td>3000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 10 Agitation Did Not Stop On Center Switch</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Temp Tank 10 SP: 0 Actual: 0</td>
<td>4000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 11 High Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 11 Low Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 11 Pump Running Aux Contact Feedback Lost</td>
<td>3000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 11 Agitation Did Not Stop On Center Switch</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Temp Tank 11 SP: 0 Actual: 0</td>
<td>4000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 14 High Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 14 Low Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Temp Tank 14 SP: 0 Actual: 0</td>
<td>4000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 15 High Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 15 Low Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 15 Pump Running Aux Contact Feedback Lost</td>
<td>3000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 15 Agitation Did Not Stop On Center Switch</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Temp Tank 15 SP: 0 Actual: 0</td>
<td>4000</td>
</tr>
<tr>
<td>12:49:44</td>
<td>No</td>
<td>Tank 16 High Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 16 Low Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 16 Pump Running Aux Contact Feedback Lost</td>
<td>3000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 16 Agitation Did Not Stop On Center Switch</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Temp Tank 16 SP: 0 Actual: 0</td>
<td>4000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 19 High Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 19 Low Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 19 Pump Running Aux Contact Feedback Lost</td>
<td>3000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 19 Agitation Did Not Stop On Center Switch</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Temp Tank 19 SP: 0 Actual: 0</td>
<td>4000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 24 High Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 24 Low Level Alarm</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 24 Pump Running Aux Contact Feedback Lost</td>
<td>3000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Tank 24 Agitation Did Not Stop On Center Switch</td>
<td>2000</td>
</tr>
<tr>
<td>00:00:06</td>
<td>No</td>
<td>Temp Tank 24 SP: 0 Actual: 0</td>
<td>4000</td>
</tr>
</tbody>
</table>
HSC Sleipner before.....
....and after!
Design of systems and interfaces in process control

- Control systems and operator interfaces must support efficiency, safety, a good work environment etc.
- I.e. they must have a high usability for the operators.
ISO 9241:

Definition of usability:

"The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"
Interface design principles

- Interface design can not be separated from design of control strategies
- Design for skilled users and high efficiency
- Support control by awareness
  - Show dynamic information
  - Support understanding of the process
  - Support building mental models
- Efficient visualisation and interaction
  - Support overview
  - Show information simultaneously
  - Show much information!!
  - Efficient information coding
  - Minimize input activities
- Make the design complete, minimize manipulation
- Make it error tolerant, allow experiments
- Supportive alarms
An example

- Train traffic control
- Today’s systems and interfaces
- A new control strategy
- Future operator interfaces
- Implementation of a new system
Today’s traffic control
The graph
The information environment
Today’s control system

- Time-Distance Graph on paper
- Information Systems
- Train Dispatcher
- Control System
  - Remote Blocking
  - Automatic Traffic Control System
  - A complex environment
    - Drivers
- Train Traffic Process
- Dept of Information Technology | Human-Computer Interaction | http://www.it.uu.se/research/hci/
Domain and user analysis

- The analysis was based on many observations and interviews
- The GMOC model was used to describe, analyse and design
- Active work groups of skilled professionals supported the work
- Ideas and prototypes were developed iteratively.
The problems.....

- Lack of overview.
- Separated information systems.
- Focus on control of the technical infrastructure, not on the traffic.
- Lacking observability.
- Lack of precision in data.
- Complexity caused by autonomous automatic functions.
- Difficulties to identify disturbances.
- Time consuming communication with train drivers.
- Dispatchers lack efficient support when this is most needed!!
A new control strategy

- From control tasks to real-time *re-planning* of a *traffic plan*
- *Automatic execution* of the continuously updated traffic plan
- Manual execution when needed
- Automatic functions are made *predictable*
  - *does not* autonomously change track usage or train order
- Continuous information exchange between train and control centre
The new control strategy

Train Traffic Controllers

- Re-Planner role
- Executor role

Decision Support System/plan verification

Operator-Process Interface
- Time-Distance diagram
- Track diagram

Executor function
- Manual
- Automatic

Real-Time Data Base
- Traffic Plan
- Process Status

Train Traffic Process

A complex environment
- Drivers
- ………

IT and process control

Dept of Information Technology | Human-Computer Interaction | http://www.it.uu.se/research/hci/
The new user interface

- Presents dynamic traffic data:
  - the operator is always “in full control”
  - supports “situation awareness”
- Supports planning tasks.
- Supports early detection of conflicts.
- Shows possible solutions.
- Integrated information presentation.
- Minimal cognitive load.

**Design structure:**
Time-Distance diagram (re-planning tool)

Actual Plan:
- Time Table
- Track Usage

Prediction
- Deviation
- Conflict detection
- Plan verification and test

Track Diagram
- line, station, track, train;
- track usage, train routes,
- actual position; track work

History, time distance graph
Conflicts are identified

Different types of conflicts are identified and visualized
Re-planning in the graph

- Re-planning directly in the planning view
- Available tracks and track usage
- Planned graph for selected train
- Departure time, track usage etc can easily be changed here
STEGER- Background

STEGER – control by planning in a computerized time-distance graph.

- A “sharp” implementation in order to test the concepts in a real traffic control centre.

- The complexity of the real work situation can not be generated in a laboratory.

- A completely new role as “real-time re-planner” is introduced.
STEGER - Objectives

- To obtain knowledge for future decisions about new national control systems.

- To evaluate
  - Work procedures and control principles
  - Functionality and algorithms
  - User interface and interaction
  - Technical requirements and specifications
  - Risks
  - Cost benefit analysis
From research to implementation

- The importance of a solid knowledge base
- The close collaboration between researchers and the rail administration
- The user centred approach
- Collaboration in all phases (research, specifications, development, deployment, evaluation)
- Focus on efficiency and work environment
The test workplace
User centered development – a “must”

- The users are experts on their own work.
- In process control the operators have skills developed over many years.
- Many skills are “tacit”
- An iterative process in the design of systems and interfaces is a necessity.
Assignment 3

- Assignment 3: Developing for usability in special domains
  - Example: Process control
- Optional assignments – choose one aspect or application.
Assignment 3 Process control, operator systems and interfaces

- Write a summary of a relevant theory and describe/analyse its relevance in an application, effects on design, e.g.:
  - Situation awareness, human error, barriers, resilience engineering, automation, alarms etc.
  - E.g. how ATP prevents human error in train traffic, or does it really??
Or..

- Analyse an incident or accident in process control and analyse it with regard to HCI aspects. Problems and solutions? E.g.
  - Train accidents
  - Flight disasters
  - Nuclear power plant incidents (Harrisburg, Tjernobyl, Forsmark)
Remember the purpose

- What is important in order to provide usability and successful design of information (control) systems in a specific domain.
OLYCKSPLATS
BORLÄNGE BANGÅRD