STPA Analysis of Intravenous Patient-Controlled Analgesia

John Thomas

Ying Hann Ang
Kristie Chung
Olivia Qing Gao
Intravenous Patient-Controlled Analgesia (IV-PCA)

- Allows self-administration of analgesia for pain management
- Safety features
  - Pump delay
  - Lock out interval
  - Limit on total dosage per time interval
- 56,000 FDA reports of problems caused by drug infusion pumps
- 500 deaths from 2005-2009**
  - About 67% due to equipment failure
  - About 33% are operator-related
- 60% of pump infusions contained some type of error*
  - 65% of errors due to violations of labeling and tubing change policies
- 87 PCA infusion pumps recalled due to safety issues

**Hankin, et al. 2007
Historical problems with PCA pumps

• Equipment failures
  • E.g. failures in tube, clamp, syringe barrel, seal, etc.

• Misprogramming
  • 19-year old woman underwent a C-section, killed by overdose due to a programming error that mismatched drug dosage with drug cassette type (Vicente et al.)

• Over-sedation
  • Extreme over-sedation, respiratory depression, respiratory arrest
  • By proxy: US Pharmacopeia reported at least 15 cases

• Drug mix-up
  • E.g. hydromorphone mixed up with morphine
Integrated Clinical Environment (ICE)

- Allows interoperability between medical devices
- Allows new safety interlock systems
  - Read from pulse oximeter
  - Read from capnogram
  - Detect patient condition
  - Alert clinicians about a patient in distress
  - Stop drug administration

MD PnP OpenICE
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- **Step 1:** Identify unsafe control actions
- **Step 2:** Identify causal scenarios

Can capture software problems, human errors, design flaws, etc.

(Leveson, 2012)
STPA: Identify accidents and hazards

Accidents (Losses)

• **A1**: Loss of life or serious injury to patient
• **A2**: Patient’s pain is not relieved
• **A3**: Loss of protected patient or proprietary hospital information
• **A4**: Financial loss or loss of hospital reputation

System Hazards

• **H1**: Opioid overdose \([A1, A4]\)
• **H2**: Opioid under-dose \(A2\)
• **H3**: Unauthorized access to hospital/patient information \([A3, A4]\)
STPA
(System-Theoretic Process Analysis)

- Identify accidents and system hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal scenarios

(Leveson, 2012)
Control Structure

Emergency care

Clinicians

Program

Patient Status, Alarms

O2 level, Alarm

CO2 level, Alarm

Integrated Patient Monitoring System

CO2 level

O2 level

Pulse Oximeter

Capnography

Vital signs

Verbal or Physiological feedback

Patient

Request

PCA Infusion Pump Controller

Request

Flow rate

Feedback

Pump

Sensor

Proxy

Verbal or Physiological feedback

Pain Relief

Administering Opioid, Stop Pump

Pumps Analgesia

Administration of opioids

Flow rate

Stop Command

Alarm, Flowrate

PCA Infusion Pump
STPA
(System-Theoretic Process Analysis)

- Identify accidents and hazards
- Draw the control structure
- Step 1: Identify unsafe control actions
- Step 2: Identify causal factors and create scenarios

(Leveson, 2012)
Unsafe Control Actions

[Diagram showing the flow of control actions and interactions among clinicians, patient status, and monitoring systems.]
# Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Wrong timing/Order causes hazard</th>
<th>Stopped too Soon/Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administer Opiod</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Wrong timing/Order causes hazard</th>
<th>Stopped too Soon/Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administer Opiod</td>
<td>UCA-PCA-1: PCA controller does not administer opioid when patient is in pain [H-2]</td>
<td>UCA-PCA-2: PCA controller administers opioid when patient has already been given too much opioid [H-1]</td>
<td>UCA-PCA-3: Delay in PCA controller administering opioid beyond TBD seconds/minutes [H-2]</td>
<td>UCA-PCA-4: PCA controller stops administering opioid before programmed dosage is fully administered [H-2]</td>
</tr>
</tbody>
</table>

### Hazards
- **H1**: Opioid overdose [A1, A4]
- **H2**: Opioid under-dose [A2]
- **H3**: Unauthorized access to hospital/patient information [A3, A4]
## Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Wrong timing/Order causes hazard</th>
<th>Stopped too Soon/Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop Command</td>
<td>UCA-IPMS-01. IPMS does not send a STOP command to PCA when patient has been given too much opioid [H-1]</td>
<td>UCA-IPMS-02. IPMS sends a STOP command to PCA when there is no emergency. [H-2]</td>
<td>UCA-IPMS-03. IPMS takes too long to send a STOP command in an emergency. [H-1]</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Hazards

- **H1**: Opioid overdose [A1, A4]
- **H2**: Opioid under-dose [A2]
- **H3**: Unauthorized access to hospital/patient information [A3, A4]
# Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Wrong timing/Order causes hazard</th>
<th>Stopped too Soon/Applied Too Long</th>
</tr>
</thead>
</table>

### Hazards

- **H1:** Opioid overdose [A1, A4]
- **H2:** Opioid under-dose [A2]
- **H3:** Unauthorized access to hospital/patient information [A3, A4]
## Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Wrong timing/Order causes hazard</th>
<th>Stopped too Soon/Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program IPMS</td>
<td>UCA-CLN-06. Clinician does not program IPMS prior to use [H-1, H-2]</td>
<td>UCA-CLN-07. Clinician programs IPMS with incorrect value [H-1, H-2]</td>
<td>UCA-CLN-06. Clinician programs IPMS too late while it is already in use [H-1, H-2]</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Hazards

- **H1**: Opioid overdose [A1, A4]
- **H2**: Opioid under-dose [A2]
- **H3**: Unauthorized access to hospital/patient information [A3, A4]
Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Wrong timing/Order causes hazard</th>
<th>Stopped too Soon/Applied Too Long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide PCA handling instructions</td>
<td>UCA-CLN-08. Clinician does not provide instructions to patient or provided in a way that patient does not understand (e.g., language or culture issues) [H-1, H-2]</td>
<td>UCA-CLN-09. Clinician provides incorrect instructions to patient [H-1, H-2]</td>
<td>UCA-CLN-10. Clinician provides instructions too soon or too late [H-1, H-2]</td>
<td></td>
</tr>
</tbody>
</table>

**Hazards**

- **H1**: Opioid overdose [A1, A4]
- **H2**: Opioid under-dose [A2]
- **H3**: Unauthorized access to hospital/patient information [A3, A4]
# Creating safety constraints

<table>
<thead>
<tr>
<th>Unsafe Control Actions</th>
<th>Safety Constraints</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UCA-IPMS-01</strong></td>
<td><strong>SC-1</strong></td>
</tr>
<tr>
<td>IPMS does not send a STOP command to PCA when patient has been given too much opioid [H-1]</td>
<td>IPMS must send STOP command to PCA when patient has been given too much opioid</td>
</tr>
<tr>
<td><strong>UCA-IPMS-02</strong></td>
<td></td>
</tr>
<tr>
<td>IPMS sends a STOP command to PCA when there is no emergency [H-2]</td>
<td>IPMS must not send STOP command unless an emergency condition is indicated</td>
</tr>
<tr>
<td><strong>UCA-IPMS-03</strong></td>
<td></td>
</tr>
<tr>
<td>IPMS takes too long to send a STOP command in an emergency [H-1]</td>
<td>IPMS must send STOP command within TBD seconds of emergency</td>
</tr>
<tr>
<td>Etc.</td>
<td>Etc.</td>
</tr>
</tbody>
</table>
STPA
(System-Theoretic Process Analysis)

• Identify accidents and hazards
• Draw the control structure
• Step 1: Identify unsafe control actions
• Step 2: Identify causal scenarios

(Leveson, 2012)
UCA-IPMS-1:
IPMS does not send a STOP command to PCA when patient has been given too much opioid.

IPMS does not believe patient is in overdose condition.

Messages discarded due to clock drift / incorrect time synchronization.
Identify causal scenarios

Potential solutions:
- Implement time synchronization function in IPMS (e.g. Berkeley algorithm, NTP, etc.)
- Implement periodic synchronization checks
Identify causal scenarios

Clinician Scenario #9:
- PCA pump properly programmed
- Patient goes into respiratory depression.
- Clinician on day shift responds, removes PCA pump, overrides the alarm.
- Clinician shift change
- Patient complains about pain
- Clinician reconnects PCA pump
- Patient goes into respiratory depression for second time
- Physician not aware of situation, prescribes stronger oral pain management

UCA-CLN-02. Clinician administers PCA pump when it is not appropriate
Identify causal scenarios

Clinician Scenario #9:
- PCA pump properly programmed
- Patient goes into respiratory depression.
- Clinician on day shift responds, removes PCA pump, overrides the alarm.
- Clinician shift change
- Patient complains about pain
- Clinician reconnects PCA pump
- Patient goes into respiratory depression for second time
- Physician not aware of situation, prescribes stronger oral pain management

Potential solutions:
- Procedures regarding PCA event communication, documentation
- IPMS could automatically record emergency incidents, further updated in the EHR system
Conclusions

• Captured potential human errors, software problems, interoperability issues
• Captures system-level behavior, context
• Captures interaction accidents without failures
  – Even when system operates exactly as designed
• Can be used to help develop solutions
  – Prevent unsafe scenarios
  – Ensure unsafe scenarios are observable and reversible
  – Detect missing feedback loops, e.g. operators and product designers
• Can be applied to organizational and social aspects