Halt and Catch Fire: Worst Software Programming Failures and Tips To Avoid Them
Richard Popple
Rex Cardan
Carlos Anderson

HCF – Halt and Catch Fire

A fictitious op-code that causes a CPU to stop operation and start switching so fast that it overheats and burns.

Halt and Catch Fire
Do This Not That:
The Therac-25 Control Software

Richard Popple, Ph.D.
The machine

- Therac-6 and Therac-20 stand-alone machines that could be controlled using a PDP-11
- Therac-25 designed for computer control
- Therac-25 relied on software for safety – significantly fewer hardware interlocks
- Therac-25 software based on Therac-6 & Therac-20 software

The accidents

- Kennestone Regional Oncology Center, June 1985
- Ontario Cancer Foundation, July 1985
- Yakima Valley Memorial Hospital, December 1985
- East Texas Cancer Center, March 1986
- East Texas Cancer Center, April 1986

East Texas Cancer Center

- 22 MeV electron treatment to back, 180 cGy / fraction
- During prescription entry, therapist initially selected x-ray mode but quickly corrected to electron mode.
- At beam-on, patient felt as if he had received electric shock or had hot coffee poured on his back.
- Patient died of radiation overdose 5 months after accident.
- Estimated dose was 165 to 250 Gy delivered in 1 second to an area approximately 1 cm².
Software design errors

- Multiple errors
- A significant design flaw was a race condition

Data entry

<table>
<thead>
<tr>
<th>PATIENT NAME</th>
<th>TEST</th>
<th>BEAM TYPE</th>
<th>ENERGY (MV): 25</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIT RATE: 85</td>
<td>60</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>TIME: 0:25</td>
<td>500</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>Gantry Rotation (deg)</td>
<td>0.0</td>
<td>0</td>
<td>VERIFIED</td>
</tr>
<tr>
<td>Collimator Rotation (deg)</td>
<td>359.2</td>
<td>359</td>
<td>VERIFIED</td>
</tr>
<tr>
<td>Collimator X (cm)</td>
<td>14.2</td>
<td>14.3</td>
<td>VERIFIED</td>
</tr>
<tr>
<td>Collimator Y (cm)</td>
<td>27.2</td>
<td>27.3</td>
<td>VERIFIED</td>
</tr>
<tr>
<td>WEDGE NUMBER</td>
<td>1</td>
<td>1</td>
<td>VERIFIED</td>
</tr>
<tr>
<td>ACCESSORY NUMBER</td>
<td>0</td>
<td>0</td>
<td>VERIFIED</td>
</tr>
<tr>
<td>DATE: 6/26</td>
<td>SYSTEM</td>
<td>DATE</td>
<td>OPP. ID: 123456-789</td>
</tr>
<tr>
<td>TIME: 12:55:4</td>
<td>TREAT</td>
<td>TREAT</td>
<td>OPERATOR: COMMAND</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>X-RAY: 13777</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TREAT: PAUSE</td>
</tr>
</tbody>
</table>
Datent

if mode/energy specified then
begin
  calculate table index
  repeat
    fetch parameter
    output parameter
    point to next parameter
  until all parameters set
  call Magnet
  if mode/energy changed then return
end
if data entry is complete then set Tphase to 3
if data entry is not complete then
  if reset command entered then set Tphase to 0
return

Datent

if mode/energy specified then
begin
  calculate table index
  repeat
    fetch parameter
    output parameter
    point to next parameter
  until all parameters set
  call Magnet
  Saturate bending magnets
  if mode/energy changed then return
end
if data entry is complete then set Tphase to 3
if data entry is not complete then
  if reset command entered then set Tphase to 0
return

Magnet:

Set bending magnet flag
repeat
  set next magnet
  call Pprime
  if mode/energy has changed then exit
until all magnets are set
return

Pprime:

repeat
  if bending magnet flag is set then
    if editing taking place then
      if mode/energy has changed then exit
    until hysteresis delay has expired
    Clear bending magnet flag
  return

East Texas therapist had set parameters for 25 MV x-rays
Delay while magnet saturates

Monitor for edits while waiting for magnet delay time to elapse

Bending magnet flag is cleared after first magnet is set!!!
Setting all magnets takes ~8 seconds. A fast user can edit mode & energy and return cursor to home position.

After first magnet was set, East Texas therapist changed mode to electrons, but bending magnet flag was no longer set and so changes were ignored!

Mode set to electrons while magnets were saturating, but parameters are still set for 25 MV x-rays.

Datent

if mode/energy specified then
begin
  calculate table index
  repeat
    fetch parameter
    output parameter
    point to next parameter
    until all parameters set
  call Magnet
    if mode/energy changed then return
  end
  if data entry is complete then set TPhase to 3
  if data entry is not complete then
    if next command entered then set TPhase to 0
  return
end
if mode/energy specified then
  begin
    calculate table index
    repeat
      fetch parameter
      output parameter
      point to next parameter
      until all parameters set
    call Magnet
    if mode/energy changed then return
  end
if data entry is complete then set Tphase to 3
if data entry is not complete then
  if reset command entered then set Tphase to 0
return
Machine behavior at beam-on

- High current, unscanned electron beam
- Monitor chamber saturated
- Machine stopped
- Console indicated Malfunction 54 – only documentation was a sheet on side of machine that described Malfunction 54 as “dose input 2”
- Console showed 6 monitor units delivered
- Software allowed treatment to be resumed

Causal factors:
Operator error was NOT a factor

Operator error was NOT a contributing factor!

SAM ALERT
Causal factors:
Confusing reliability with safety
- Therac software was highly reliable
- Very few reports of erroneous behavior
- Reliability led to complacency

Causal factors:
Lack of defensive design
- No self-checks
- Minimal audit logs due to limited memory
- User could not verify machine settings
- No check for chamber saturation

Causal factors:
Software reuse
- Therac-20 software had many of the same flaws, but hardware interlocks prevented accidents
- Reusing software modules does not guarantee safety
Causal factors:
Inadequate software engineering practices

- Lack of specifications and documentation
- Insufficient quality assurance practices
- Inadequate testing at the module level (unit testing)
- Poorly designed error messages and insufficient documentation

Further reading

Medical Devices: The Therac-25

Nancy Leveson
University of Washington