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 standalone 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

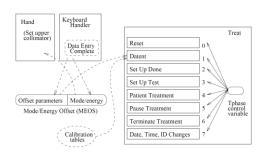
- Multiple errors
- A significant design flaw was a race condition

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM

Data entry

PATIENT NAME : TEST TREATMENT MODE : FIX		BEAM TYPE: X	ENERGY (Me	V): 25
		ACTUAL	PRESCRIBED	
UNIT RATE/MINUTE		0	200	
MONITOR UNITS		50 50	200	
TIME (MIN)		0.27	1.00	
GANTRY ROTATION (DEG)		0.0	0	VERIFIED
COLLIMATOR ROTATION (DEG))	359.2	359	VERIFIED
COLLIMATOR X (CM)		14.2	14.3	VERIFIED
COLLIMATOR Y (CM)		27.2	27.3	VERIFIED
WEDGE NUMBER		1	1	VERIFIED
ACCESSORY NUMBER		0	0	VERIFIED
DATE : 84-OCT-26 SY	STEM	· BEAM READY	OP MODE	TREAT AUTO
TIME : 12:55: 8 TF	REAT	: TREAT PAUSE		X-RAY 17377
OPR ID : T25V02-R03 RE	EASON	OPERATOR	COMMAND	t

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM Knowledge that will change your world



THE UNIVERSITY OF ALABAMA AT BIRMINGHAM

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	
Lace the UNIVERSITY OF	
LIABATE THE UNIVERSITY OF THE	
Datent	
${\bf if} \; {\rm mode/energy} \; {\rm specified} \; {\bf then} \\$	
begin calculate table index	
$egin{array}{c} \mathbf{repeat} \\ \mathbf{fetch} \ \mathbf{parameter} \end{array}$	
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 3if data entry is not complete then	
if reset command entered then set Tphase to 0 return	
L 2 THE UNIVERSITY OF ALABAMA AT IRRIPINSHAM Koowledge that will charge your world	
Magnet: Set bending magnet flag ← Indicates bending magnets	
repeat are being initialized Set next magnet	
call Ptime	
if mode/energy has changed, then exit until all magnets are set	
return	
Ptime: 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	
L'ET THE UNIVERSITY OF ALAGAMA AT BIRKINGHAM Kowleige that all Googy one world	
Commencingly of most state coloring. Sport sept no	

Mag	gnet:	
	Set bending magnet flag	
	repeat Set next magnet	
	call Ptime — Delay while magnet saturates	
	if mode/energy has changed, then exit	
	until all magnets are set return	
Ptin		
	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	
	A A TO THE INVESTMENT OF	
	LES ALEANA AT BERNINGHAM Knowledge that will change your world	
Mag	gnet:	
	Set bending magnet flag	
	repeat Set next magnet	
	call Ptime	
	if mode/energy has changed, then exit	
	until all magnets are set return	
	Monitor for edits while waiting	
Ptin		
	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	
		-
	THE UNIVERSITY OF ALBAMA AT BIRMINGHAM Knowledge that will change your world	
Mag	gnet:	
	Set bending magnet flag repeat	
	Set next magnet	
	call Ptime	
	if mode/energy has changed, then exit	
	until all magnets are set return	
Ptin		
	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 Bending magnet flag is Clear bending magnet flag	
	ordered ditter mot	
	magnet is set!!!	
	THE UNIVERSITY OF ALABAMA AT BIRMINGHAM Rowledge that will change your world	

Magnet:	
Set bending magnet flag repeat	
Set next magnet	
call Ptime if mode/energy has changed, then exit	
until all magnets are set ← Setting all magnets takes ~8	
return seconds. A fast user can edit mode & energy and return	
Ptime: cursor to home position.	
repeat if handing magnet flag is set then	
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	
THE UNIVERSITY OF ALABAMA AT BIRKINGHAM	
Knowledge that will change your world	
Magnet: Set bending magnet flag	
repeat	
Set next magnet	
call Ptime if mode/energy has changed, then exit	
until all magnets are set	
return After first magnet was set, East Texas therapist changed mode to electrons, but	
Ptime: bending magnet flag was no longer set and so changes were ignored!	
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	
2 THE UNIVERSITY OF ALRAMMA AT BIRMINGHAM	
Knowledge that will change your world	
Datent	
if mode/energy specified then	
begin	
calculate table index repeat	
fetch parameter while magnets were	
output parameter point to next parameter saturating, but	
until all parameters set parameters are still set	
call Magnet for 25 MV x-rays 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	
THE UNIVERSITY OF ALABAMA AT BIRMINGHAM	
A.A.BARIA AT BIRNINGHAM Knowledge that will change your world	

Datent	
if mode/energy specified then	
begin	
$\begin{array}{c} \text{calculate table index} \\ \textbf{repeat} \end{array}$	
fetch parameter	
output parameter point to next parameter flag is no longer set, so	
until all parameters set edits are ignored.	
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	
THE UNIVERSITY OF	
THE UNIVERSITY OF ALAMANA AT BIRTHINGHAM Knowledge that will change your world	
Datent	
if mode/energy specified then	
begin calculate table index	
repeat	
fetch parameter output parameter	
point to next parameter Cursor back at home	
until all parameters set position, indicating data	
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	
L 3 THE UNIVERSITY OF ALABAMA AT BIRMINISHAM	
Knowledge that will change your world	
Electron mode → turntable set Hand Handler	
→ turntable set to open position (Set upper collimator)	
(no x-ray target) Data Entry Reset	
Datent	
Set Up D	
Set Up T	
Offset parameters Mode/energy Patient T	
Mode/Energy Offset (MEOS)	
Terminat	
Calibration Date, Tir	
THE UNIVERSITY OF ALABAMA AT BIRMINGHAM Roselege that sell chappy your world	

Electron mode → turntable set to open position (no x-ray target)	Hand (Set upper collimator)	Keyboard Handler Data Entry Complete	Reset
	Offset paramete Mode/Energy	rs Mode/energy Offset (MEOS)	Set Up D Set Up T Patient T Pause Tr Terminat
25MV x-ray parameters → high beam current, no sc	anning	Calibration tables	Date, Tir

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!



THE UNIVERSITY OF ALABAMA AT BIRMINGHAI

Causal factors: Confusing reliability with safety		
Therac software was highly reliable Very few reports of erroneous behavior Deliability led to complete and the complete and		
Reliability led to complacency		
	THE UNIVERSITY OF ALABAMA AT BIRMINIGHAM Knowledge that will change your world	
Causal factors: Lack of defensive design		
No self-checks		
 Minimal audit logs due to limited memo User could not verify machine settings	ory	
No check for chamber saturation		
	THE UNIVERSITY OF BALBAMA AT BIRMINGHAM Knowledge that will change your world	
Causal factors:		
Software reuse		
Therac-20 software had many of the sal hardware interlocks prevented accident		
Reusing software modules does not guarantee.		
	THE UNIVERSITY OF	
	THE UNIVERSITY OF ALABAMA AT BIRMINGHAM Knowledge that will change your world	

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	
THE INNESCRITY OF	
THE UNIVERSITY OF Line 3 THE UNIVERSITY OF Knowledge that will change your world	
Further reading	
Medical Devices: The Therac-25*	
Nancy Leveson	
University of Washington	
http://sunnyday.mit.edu/papers/therac.pdf	
国際器画	
D40000000	
0.8 8 800007	
高級組織	
LEUE ÇT. TU FAY	
HE UNIVERSITY OF ALABAMA AT BIRMININGAM Knowledge that ill dharpe your world	