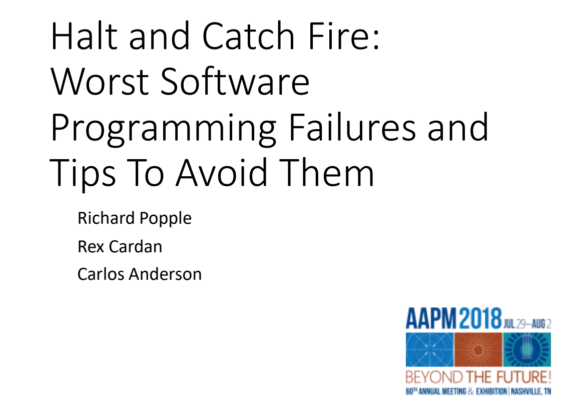
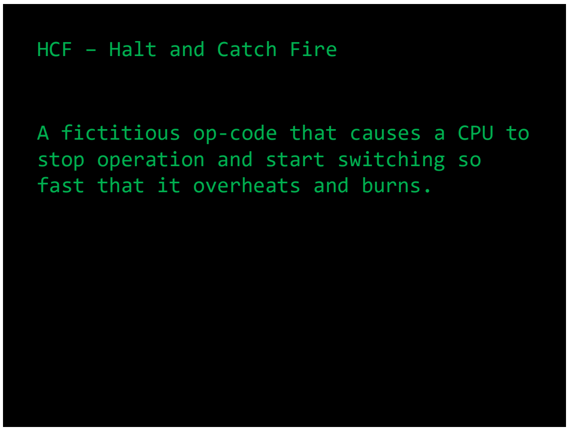


# Halt and Catch Fire: Worst Software Programming Failures and Tips To Avoid Them

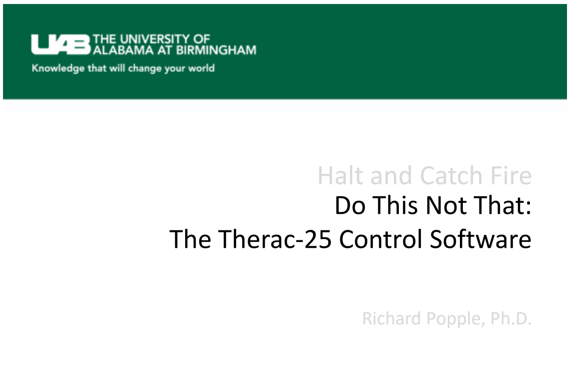
Richard Popple
Rex Cardan
Carlos Anderson

AAPM2018 JUL 29–AUG 2
BEYOND THE FUTURE!
60TH ANNUAL MEETING & EXHIBITION | NASHVILLE, TN



```
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.
```



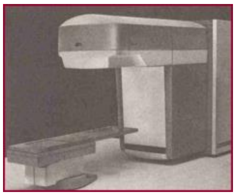
THE UNIVERSITY OF ALABAMA AT BIRMINGHAM
Knowledge that will change your world

## 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

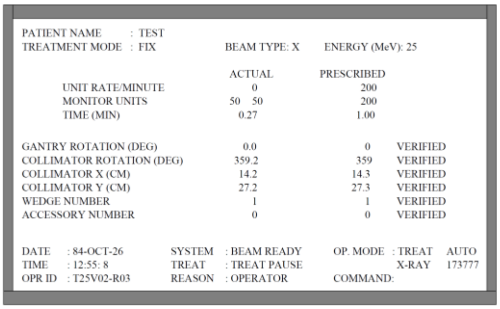
## East Texas Cancer Center

- 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 $cm^2$.

## Software design errors

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

## Data entry

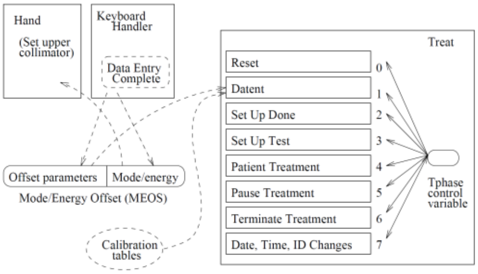


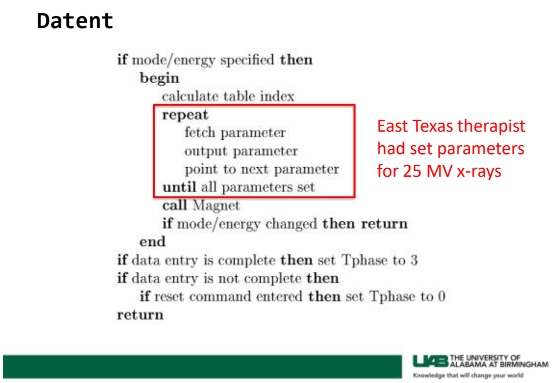
```
PATIENT NAME      : TEST
TREATMENT MODE    : FIX              BEAM TYPE: X     ENERGY (MeV): 25

                                     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       SYSTEM   : BEAM READY     OP. MODE  : TREAT    AUTO
TIME    : 12:55: 8        TREAT    : TREAT PAUSE                X-RAY    173777
OPR ID  : T25V02-R03      REASON   : OPERATOR       COMMAND:
```

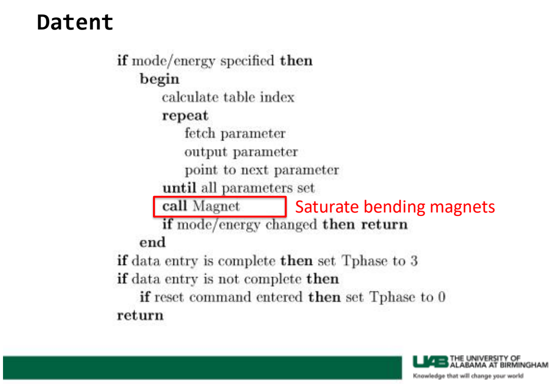




## Datent

```
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
```

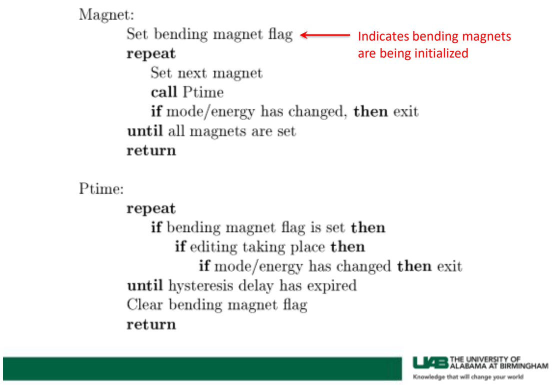
East Texas therapist had set parameters for 25 MV x-rays



## 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 reset command entered then set Tphase to 0
return
```

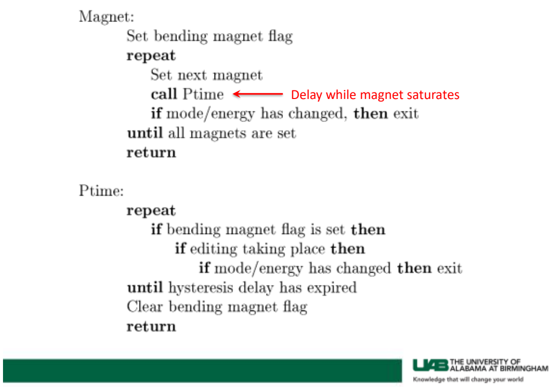
Saturate bending magnets



```
Magnet:
    Set bending magnet flag
    repeat
        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
```

Indicates bending magnets are being initialized

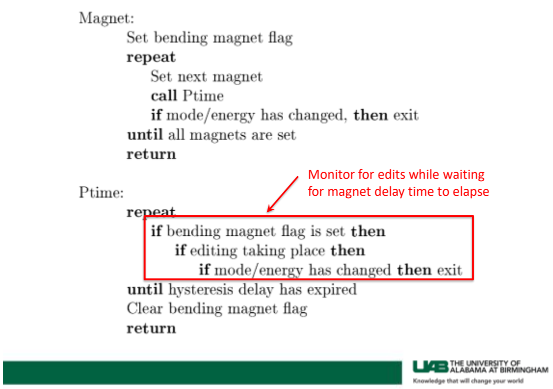


```
Magnet:
        Set bending magnet flag
        repeat
            Set next magnet
            call Ptime
            if mode/energy has changed, then exit
        until all magnets are set
        return

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
```

Delay while magnet saturates

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

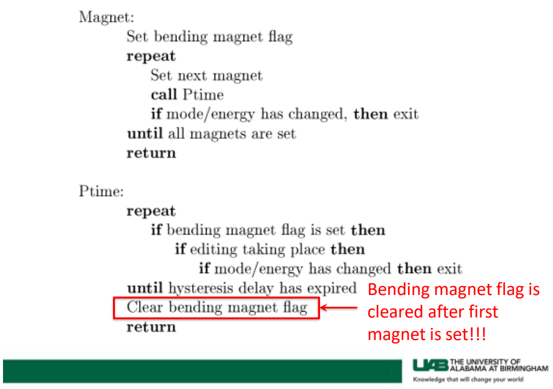


```
Magnet:
        Set bending magnet flag
        repeat
            Set next magnet
            call Ptime
            if mode/energy has changed, then exit
        until all magnets are set
        return

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
```

Monitor for edits while waiting for magnet delay time to elapse

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

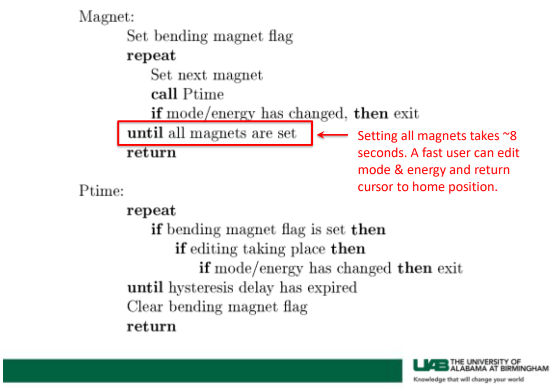


```
Magnet:
        Set bending magnet flag
        repeat
            Set next magnet
            call Ptime
            if mode/energy has changed, then exit
        until all magnets are set
        return

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
```

Bending magnet flag is cleared after first magnet is set!!!

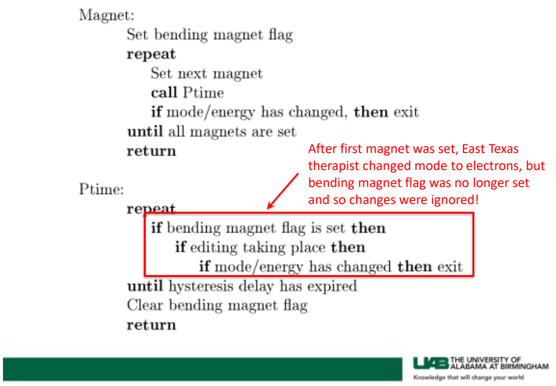
THE UNIVERSITY OF ALABAMA AT BIRMINGHAM
Knowledge that will change your world



```
Magnet:
        Set bending magnet flag
        repeat
            Set next magnet
            call Ptime
            if mode/energy has changed, then exit
        until all magnets are set
        return

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
```

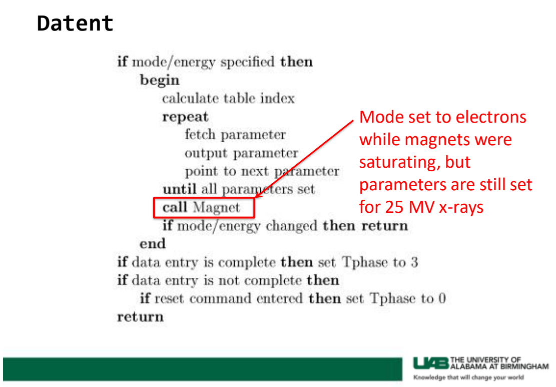
Setting all magnets takes ~8 seconds. A fast user can edit mode & energy and return cursor to home position.



```
Magnet:
        Set bending magnet flag
        repeat
            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
```

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!



## 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
```

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 reset command entered then set Tphase to 0
return
```

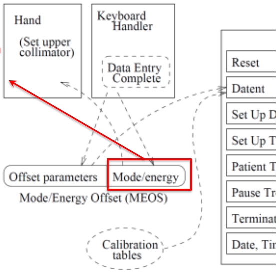
Mode/energy changed flag is no longer set, so edits are ignored.

## Datent

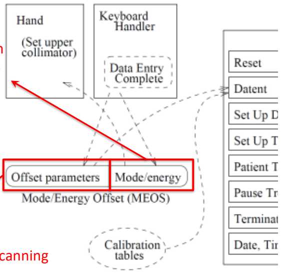
```
if mode/energy specified then
    begin
        calculate table index
        repeat
            fetch parameter
            output parameter
            point to next parameter
        until all parameters set
        call Magnet
        if mode/energy changed then return
    end
if data entry is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

Cursor back at home position, indicating data entry complete

Electron mode → turntable set to open position (no x-ray target)



Electron mode → turntable set to open position (no x-ray target)



25MV x-ray parameters → high beam current, no scanning

### 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

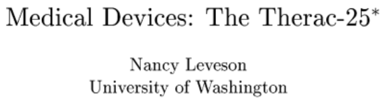
### Causal factors: Software reuse

- 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

http://sunnyday.mit.edu/papers/therac.pdf