ECEN 3753: Real-Time Operating Systems

Risks

Illustrative Risk Types

- Risks are not just technical in nature (development unknowns, component failures), though they *often* are in our context
  - Head Assisted Magnetic Recording Heads for HDD
    - 5+ years from Demo to "Commercial Production"
    - 11 years from materials science doctorate to Demo, with lots of ablation!
- Human Factors (illness, accidents, major life events, burnout, size of currently-available talent pool)
- Business Flow (Supply Chains, drug/trade/political wars)
- "Acts of God"

Human Factor Risk Examples

- c.2001: Telecomm: Fastest routing product on market by significant margin
  - Fewer than 10 engineers who could write/adapt custom processor's assembly code fast enough to meet customer's schedules
  - Could trade off training-prep, tool expansion, coding
- c.2012: HDD project (Avg 100 engineers, 2 years)
  - 1 to prison
  - 2 deaths
  - a few retirements
  - multiple multi-month leaves-of-absence
  - half dozen left company
  - organization restructured once

Business Issues/Flow Risk Examples

- 1992: Presidential Political Party Flip: Aerospace imploded.
- 1994: Conner Peripherals: horizontal integration (6 months competitive lead)
- 1998: Seagate acquired Conner (vertical integration saved costs)
- 2000: 1" ~1GB Microdrive (vs. Flash)-cheapest per-device flip around 2003
- 2000+: cheap labor & market access v. IP (China)
- 2002: $1B Palladium (Ford,Russia. Futures v. Engineering)
- 2018+: Cobalt for batteries (DR Congo: 60%)
- 2019+: Rare Earth Metals for HDDs (China: 80%)
- 1990+: Carbon Taxes
- Always: Energy costs

Expand your Horizons: read **The Innovator's Dilemma**, by Clayton Christensen

Playing Field is NOT level, nor linear

- Laws change with opinion ("artificial markets")
  - Carbon Taxes (who pays?)
  - Renewable energy (rivers vs. CO2: Columbia River)
- Historical agreements
  - Western States water (Lakes Powell, Mead)
  - Hydro-power pricing (Niagara Falls)
- International agreements try to be "fair" (for some measures of fair), but rarely are seen that way by all countries.

"Acts-of-God" Risks

These are (nominally) the once-in-a-lifetime-or-rarer risks.

- Often discounted by businesses (quarters-to-decade vision)
- When they happen, either adapt or get out of the way
  - WDC, 2001 Thailand Floods (technical involvement, governmental mitigation). Stock fell 95%.
  - GM/Ford in 2006 Financial Crisis (governmental save vs. force to energy efficiency)
- Occasional mitigations by governments/companies/people
  - US/Russia: MAD policy: "Reduce chance of enemy first strike"
  - US, India Crop Insurance (for 1%, 43% of populations)
    - Beware of **Moral Hazard**
  - Elon Musk
    - Neuralink to counter AI takeover
    - SpaceX-to-Mars: to mitigate WW3. Side-benefit: counter Death of Solar life by asteroid?
    - Tesla (Cars-to-Batteries): Carbon/GlobalWarming mitigation

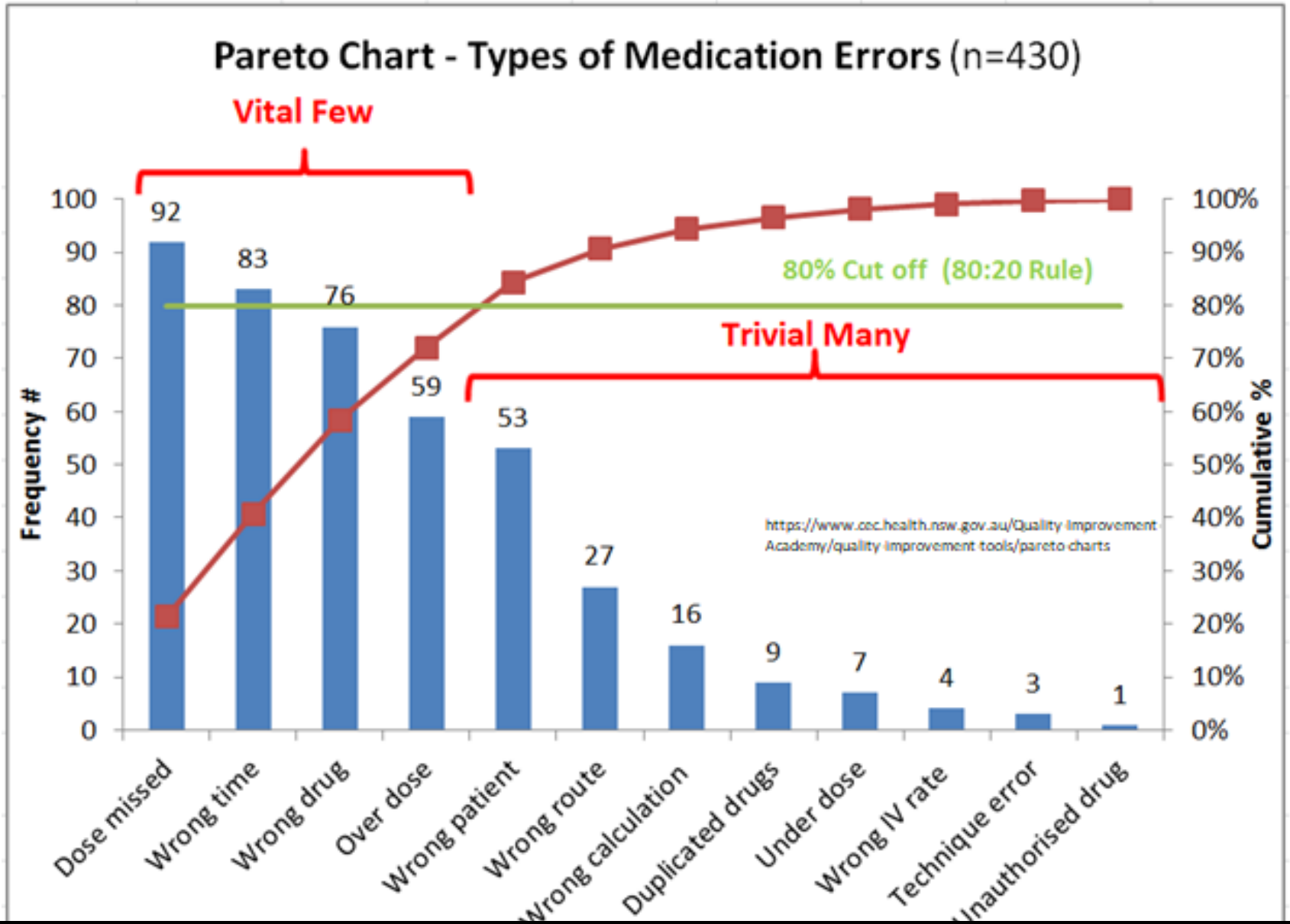
Risks: What to do, when?

Risk Analysis:

- How bad is it?
  - What's the probability of the risk manifesting as an actual problem?
  - What's the likely impact if the risk manifests as an actual problem
- What's being done about it?

Multiple methods are used to quantify risks. Most treat the risk's "size" as the product of the probability and the impact IF it happens.

Pareto Chart (80/20 rule)



Agile Numbering

Conveniently an agile method of using a modified Fibonacci sequence, can be used for both probability and impact scales:

- 1, 2, 3, 5, 8, 13, 20, 40, 100 (can be %, and impact-out-of-100)
- E.g. Risk is of other coursework delaying you from Lab7 submission for a day
  - prior data suggests that about 5% of the labs will be submitted late
  - impact to your grade is about a 1 or 2 on this scale Is everyone going to agree on the probability and impact?

Always sort risks by their Risk value (product of the probabilty and impact), either with "Resolved" and "Mitigated" risks in a separate "completed" list, or not.

Risk Status: ROAM your risks

R esolved Truly, these are no longer risks. They may have occurred or not, but there is no remaining risk.

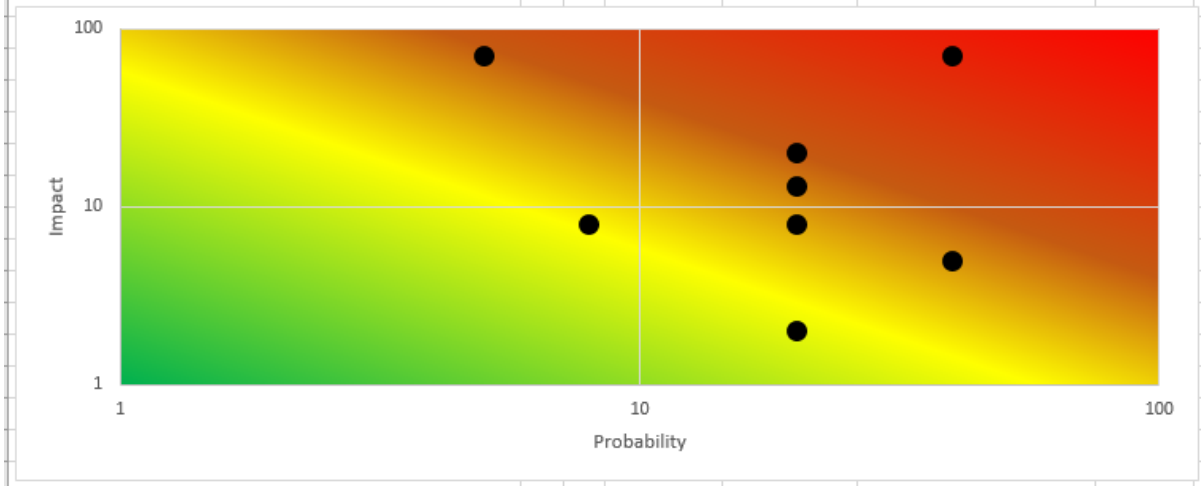
O wned These might happen, but we've got no plan yet. Whoever Owns a risk is seeking a mitigation or positive resolution.

A ccepted These are going to hurt if they occur, but no further mitigation is deemed worth the price.

M itigated You've used your trained optimization skills to find ways to either reduce the P or I scores to the point that the remainder is another, lesser-valued risk.

Risk Register

Item			Risk (P*	Recognize	Mitigated/ Resolved	ROAM	How
Registration snafu kills class	40	70	2800	4-Nov-19	12-Nov-19	R	Daily emails with supervisor, advisors
Too much lecture prep needed by 1st day	20	20	400	28-May-19	27-Aug-19	R	Enlisted volunteers at work (was M: JIT prep)
Insufficient student interest for CU funding	5	70	350	12-Nov-19	29-Jan-20	R	32 registered. (was M: gen compelling into)
Jon's day job interrupts too much for this	20	13	260	1-Nov-19	16-Nov-19	R	Jon's VP agreed to priority-swap
PPT fatigue for volunteers	40	5	200	27-Aug-19	3-Sep-19	R	Isaac set up markdown template, turnkey install
uC-Probe&Mac/Linux incompatibilities kill profiling	20	8	160	14-Jan-20	1-Feb-20	M	Supervisor installed uC-probe on lab Win boxes
Lab developer unable to finish lab development	8	8	64	3-Oct-19		A	If it happens, we'll react.
uC-Probe not licensed in time	20	2	40	4-Dec-19	7-Jan-20	R	(was O by Jon: if not in time, can use Segger only)



Here's an example from when this class was being developed.

Note that the items are things outside of my personal control–not "it might take me longer than I plan". A valid risk is "I don't know how long XYZ will take", and you can mitigate that with "spike" activities (learning/analyzing/prototyping to gain better understanding).

Control Loop Risks

Very often, the HARD RT task in a RT system is a control loop, and we **need** to ensure sufficient performance.

Pre-"reading" for this lecture:

- https://www.youtube.com/watch?v=wouhREkqZa0
- Causes: Synch and Slack Time
- Effect: Delay Margin

Common Chain of Causes to Variable Latency

- Source of the readiness of some external thing is not exactly periodic
- Desire to share the CPU among many tasks leads to variable response time to the thingy (Interrupts, task switching latencies)

Approximately: a normal RV added to a couple of small uniform RVs.

- Usually, a pretty small range of latencies
- Rarely, a significant outlier

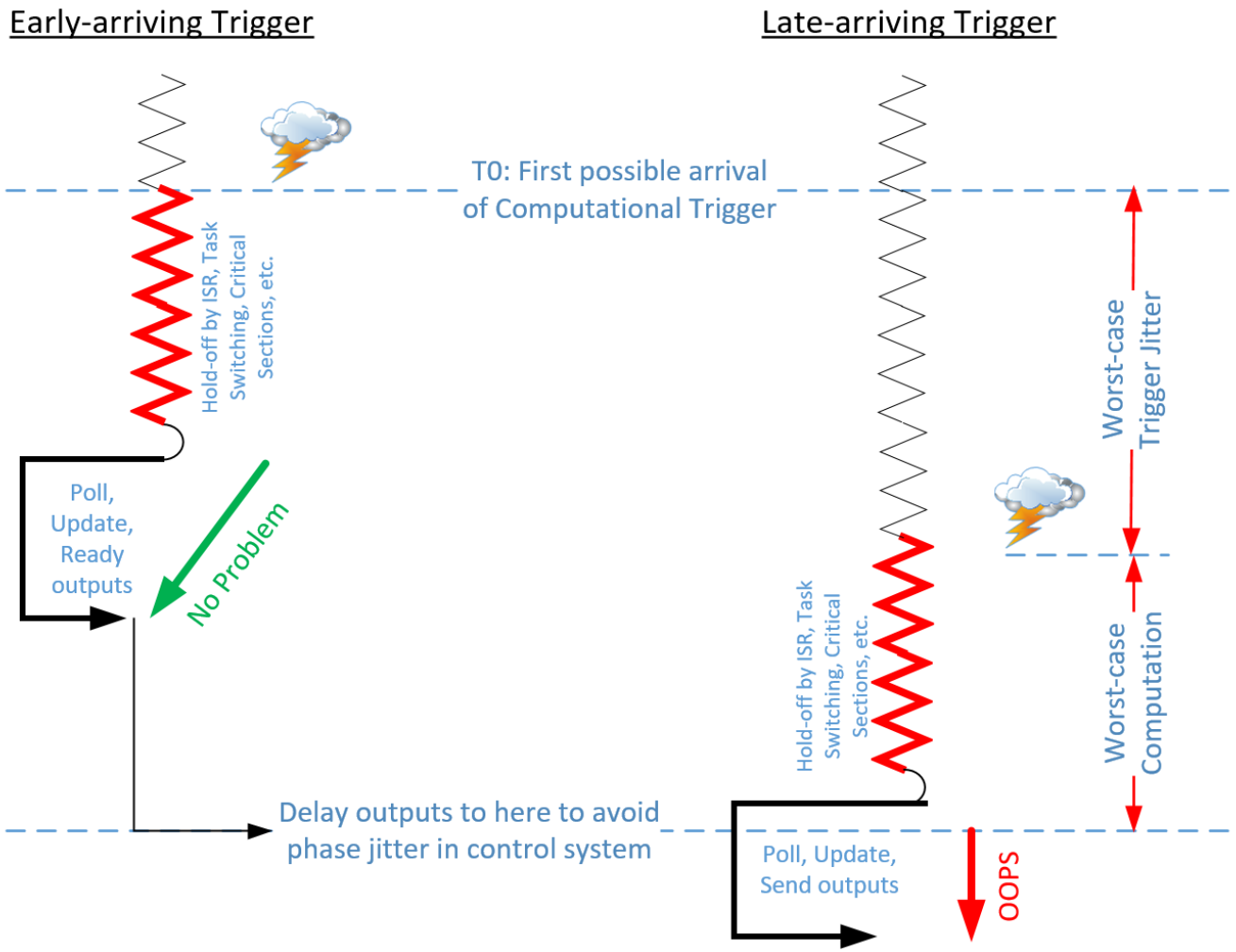
$\rightarrow$ Mitigate with variable slack time that re-synchs everything

Control-Loop Latency Mitigation

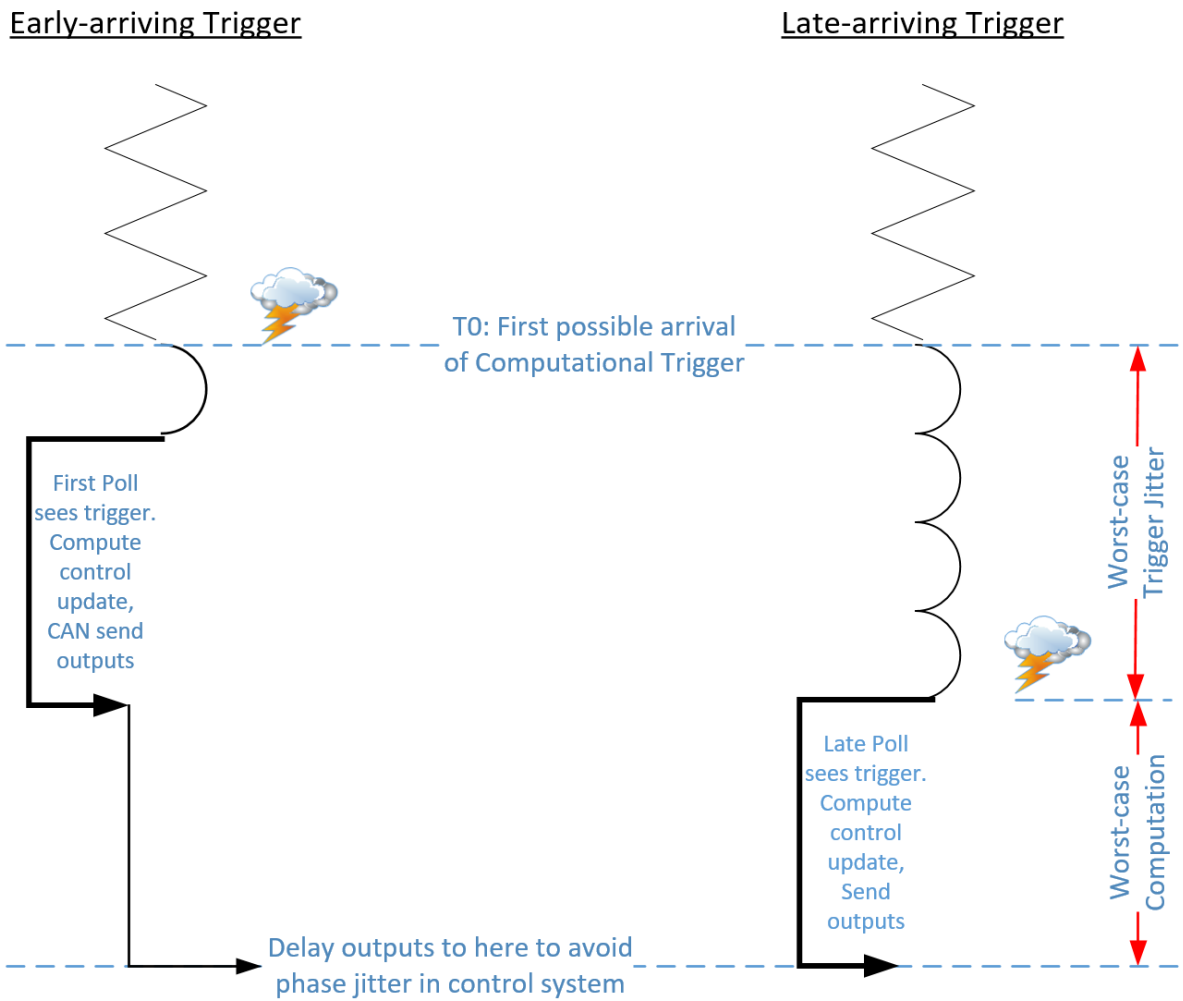
Ideas that are relevant in most RT systems, particularly to help ensure the Hard RT task gets the service it needs:

- Use timer to wake up before computation trigger, and poll for its arrival (see next pages)
  - E.g. Start-of-packet + Shortest-packet to begin polling, rather than end-of-packet interrupt
  - Subtract off the longest possible holdoff (longest critical section plus longest ISR/TaskSwitch, above HardRT priority)
- Pre-computation
  - Apply math ahead of time to get intermediate results
  - Compute estimated/expected values for nominal usage
- Use of Interrupts that have register banking or other accelerations

Why not just use Interrupt Triggering?

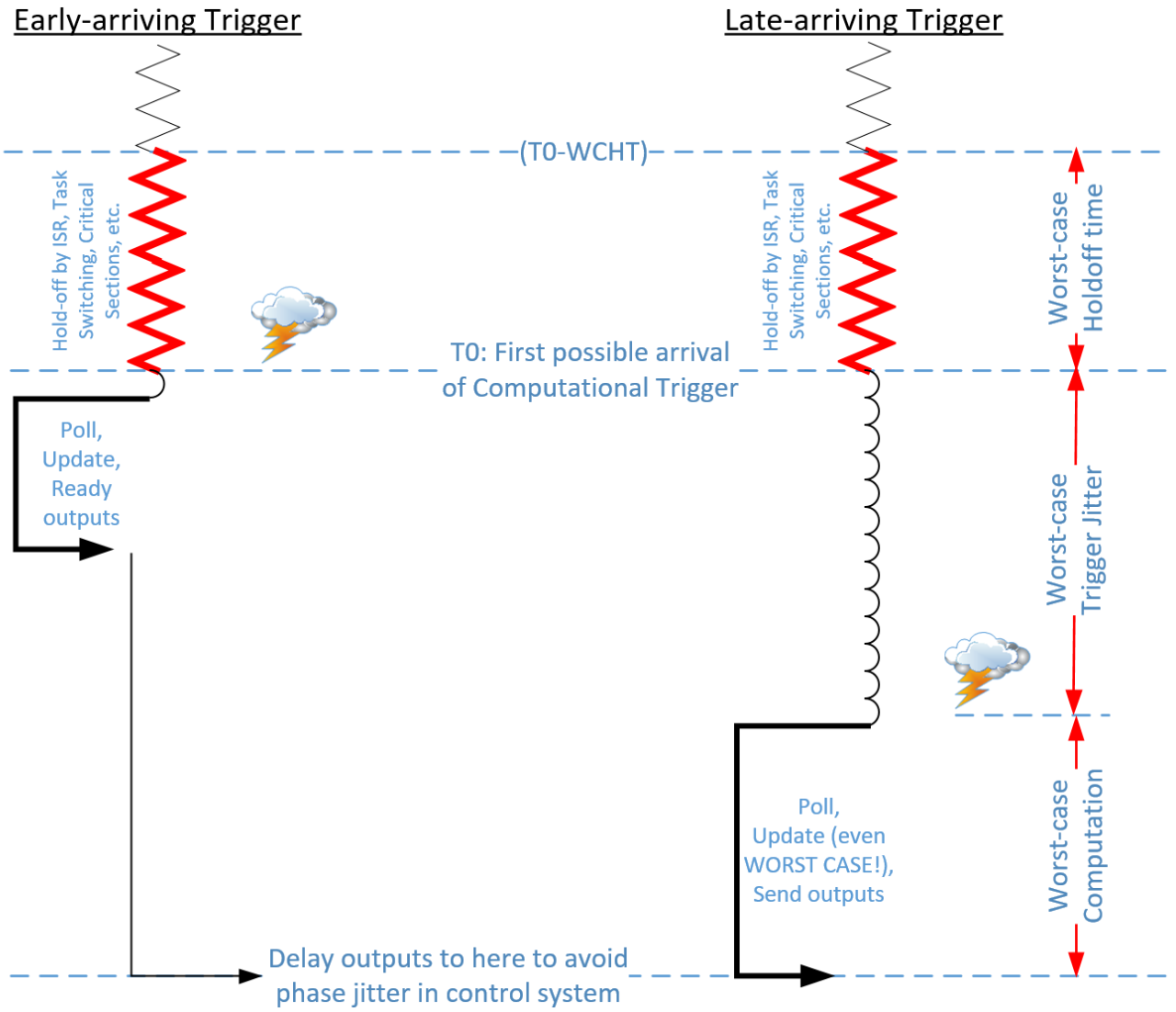


Begin Polling at Earliest Possible Trigger



What's this back to assuming?

Polling, with Compensation for CPU Holdoff



How does a cache miss on a low priority task's code factor into this?