Towards Automated Safety Vetting of PLC Code in Real-World Plants

Mu Zhang∗, Chien-Ying Chen†, Bin-Chou Kao‡, Yassine Qamsane§, Yuru Shao¶, Yikai Lin¶, Elaine Shi∗, Sibin Mohan†, Kira Barton§, James Moyne§ and Z. Morley Mao¶

∗CS, Cornell; †CS, UIUC; ‡ITI, UIUC; §ME, UMich; ¶EECS, UMich

∗mz496@cornell.edu, ∗elaine@cs.cornell.edu, †{cchen140,sibin}@illinois.edu, ‡ bkao2@illinois.edu, §{yqamsane,bartonkl,moyne}@umich.edu, ¶{yurushao,yklin,zmao}@umich.edu

Safety Hazards are Unique Threats in ICS

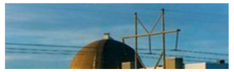
HOME SEARCH The New York Times

Cyberattacks on Iran — Stuxnet and Flame

News about Cyberattacks on Iran — Stuxnet and Flame, including commentary and archival articles published in The New York Times.

Latest | Search

July 6, 2017 Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say



CBS NEWS / *June 23, 2017, 12:48 PM*

Was Russian hacking of Ukraine's power grid a test run for U.S. attack?

Comments / Share / Tweet / Stumble / Email

The Russian attacks on Ukraine's power grid were extensive. In 2015, electricity was cut to nearly a quarter-million Ukrainians, and about a year later a transmission station was taken down, revealing the attacks were becoming more sophisticated.

BBC Sign in News Sport Weather Shop Earth Travel

NEWS

Home Video World US & Canada UK Business Tech Science Magazine E

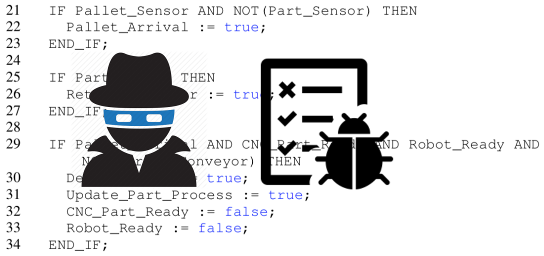
Hack attack causes 'massive damage' at steel works

22 December 2014 Technology Share

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

PLC being a Major Attack Vector



Controller Code w/ Safety Violations

Insider Attacks or Bugs

Programmable Logic Controller (PLC)

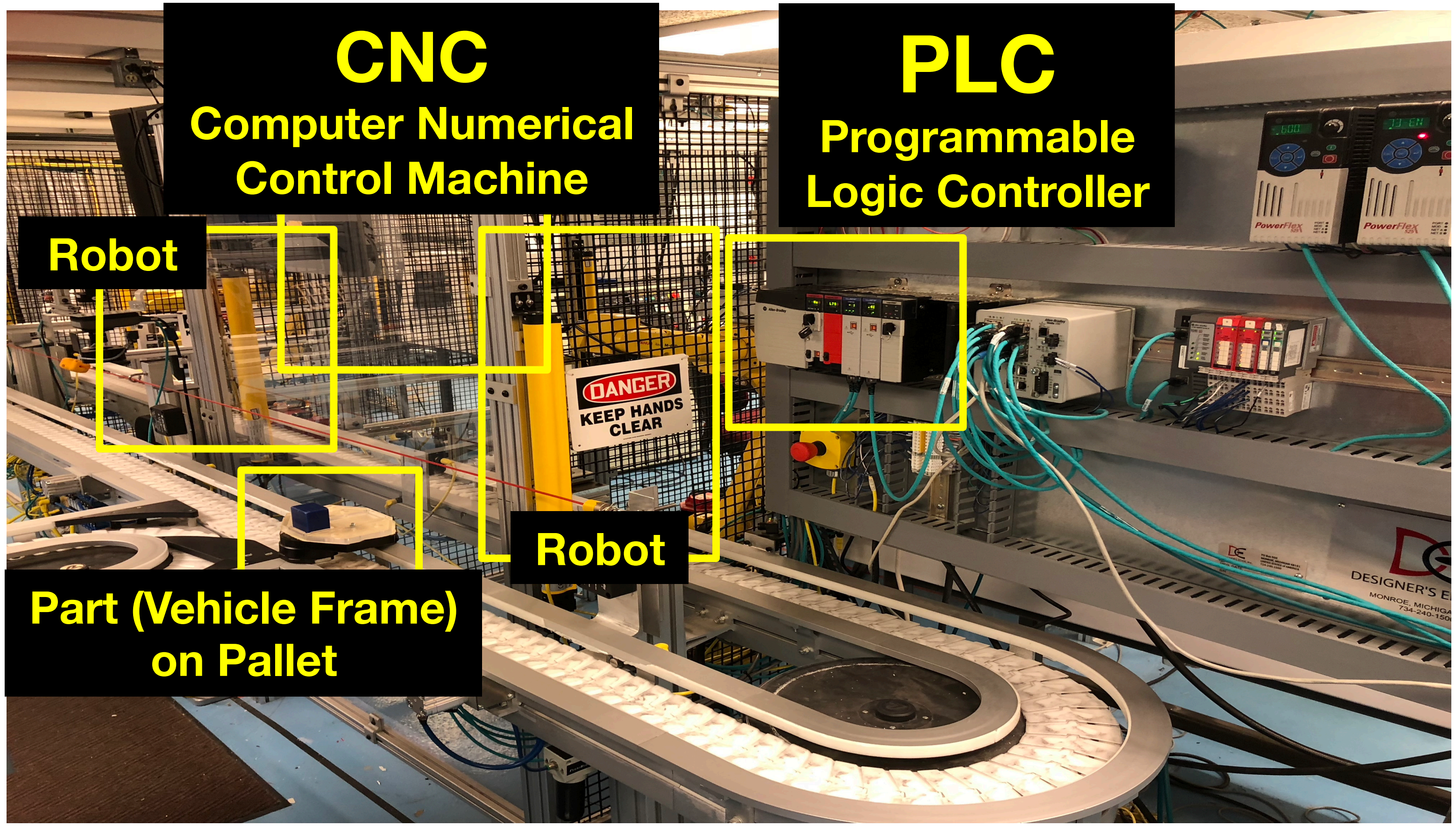
Core Control Unit on the Factory Floor

Physical Damage

Different from Financial Loss Often Seen in Attacks in Consumer Systems

A great many of prior work: *e.g.,* TSV (NDSS'14), SYMPLC (FSE'17)

Overlooked Fact: ICS is Complex; PLC is NOT Working Alone



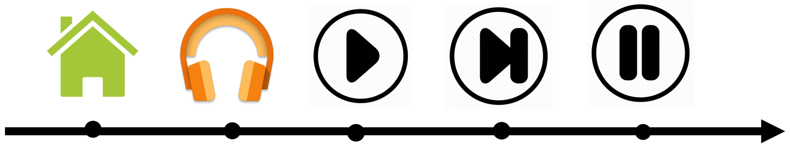
- Real-world Automotive Manufacturing Testbed
- Developed by **No.1 Vendor** (Rockwell Automation)
- PLCs are **driven by events** from other machines

Testing PLC code requires external event inputs

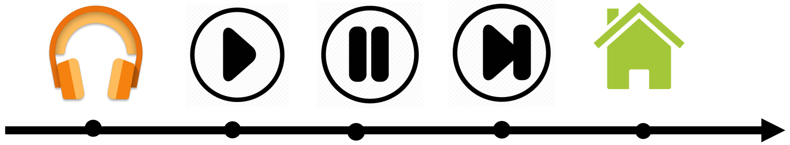
Testing Event-driven Code in Other Domains – Simulating and Rearranging Events

Android App: Anand *FSE'12*, Jensen *ISSTA'13*, Mirzaei *Softw. Eng. Notes'12*, Yang *CCS'13*

Web Program: SymJS *FSE'14*, Saxena *Oakland'10*



Simulated Event Sequence



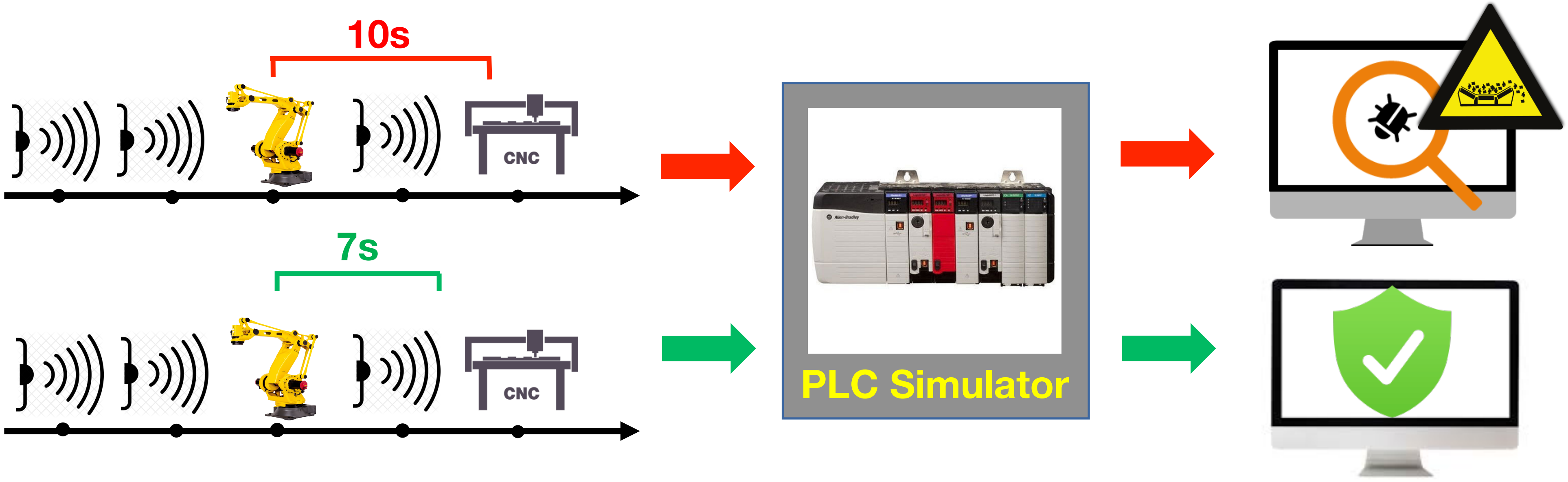
Rearrange Event Order

⋮

App Testing in Emulator

Crash

Rearranging Event Order to Test PLC Code is NOT Sufficient

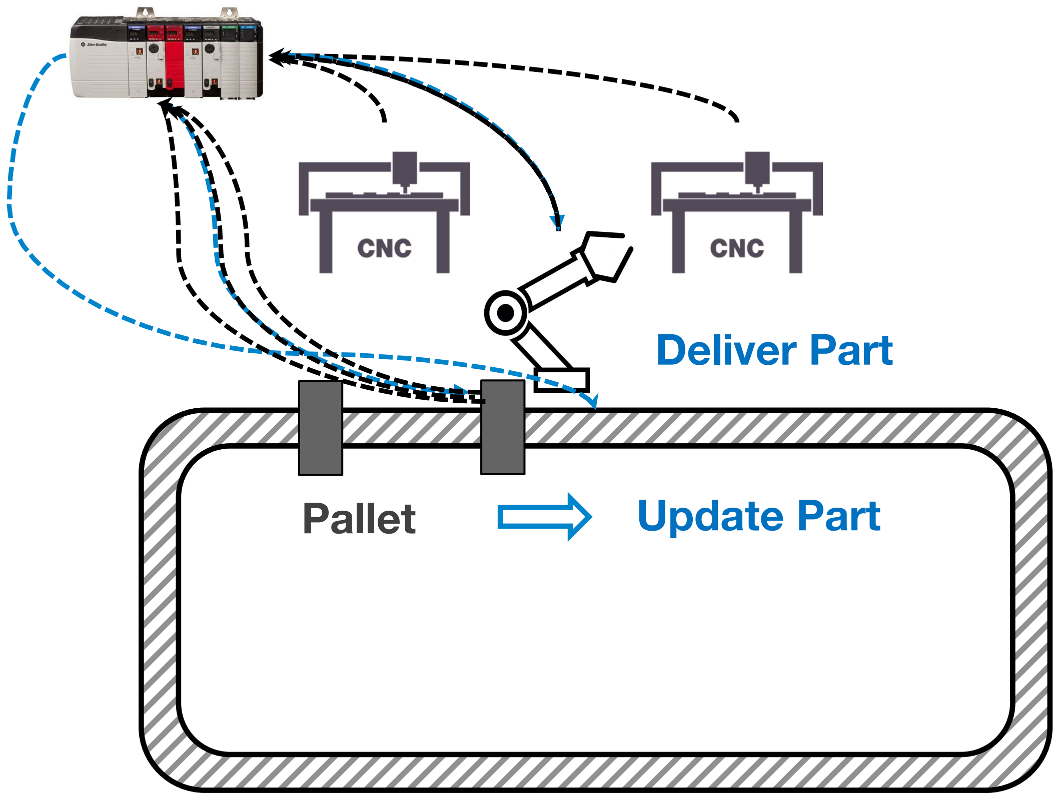


Event Sequences of Same Ordering But Different Timings

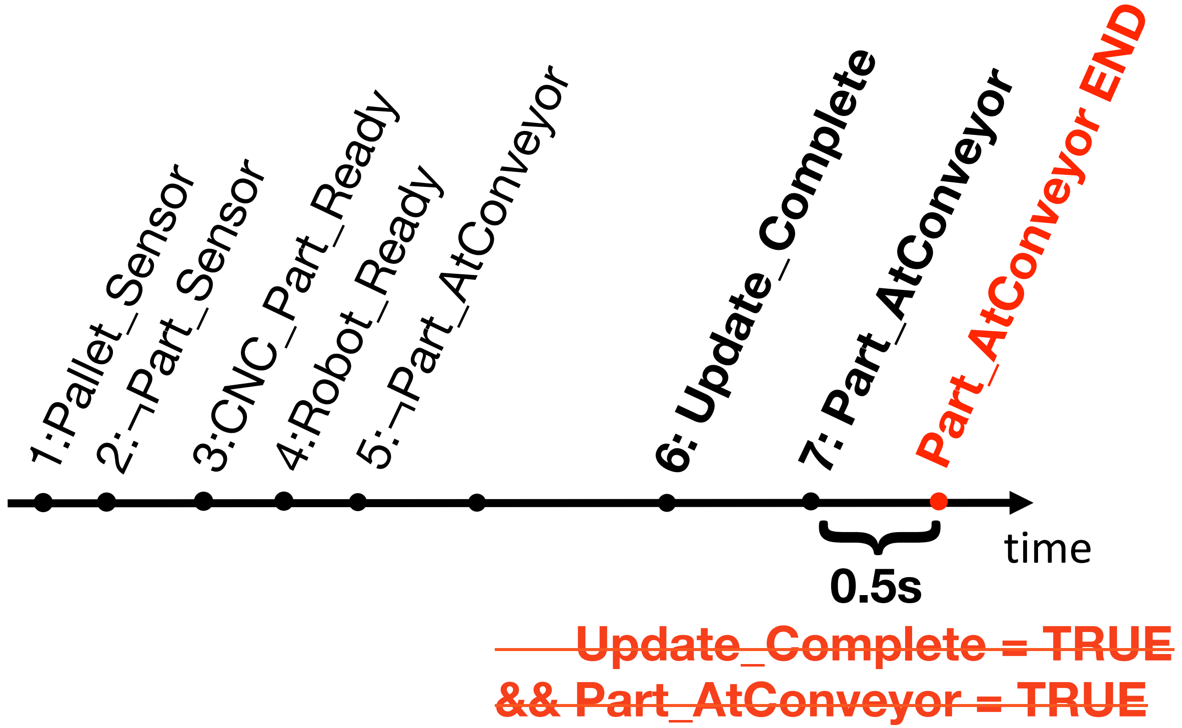
Timing factor: Nature of ICS

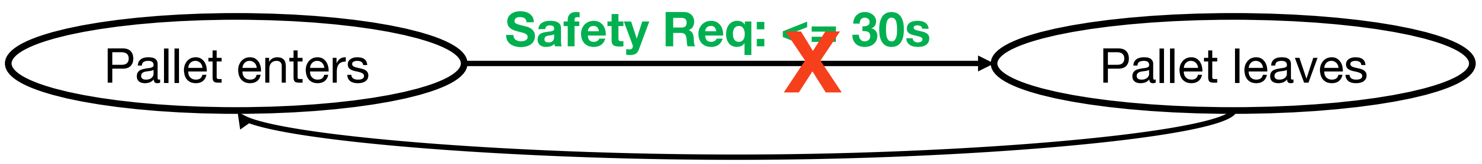
Timeliness, Throughput → Internal Timeouts
Machine Speed Limits → External Timing Constraints

A Running Example



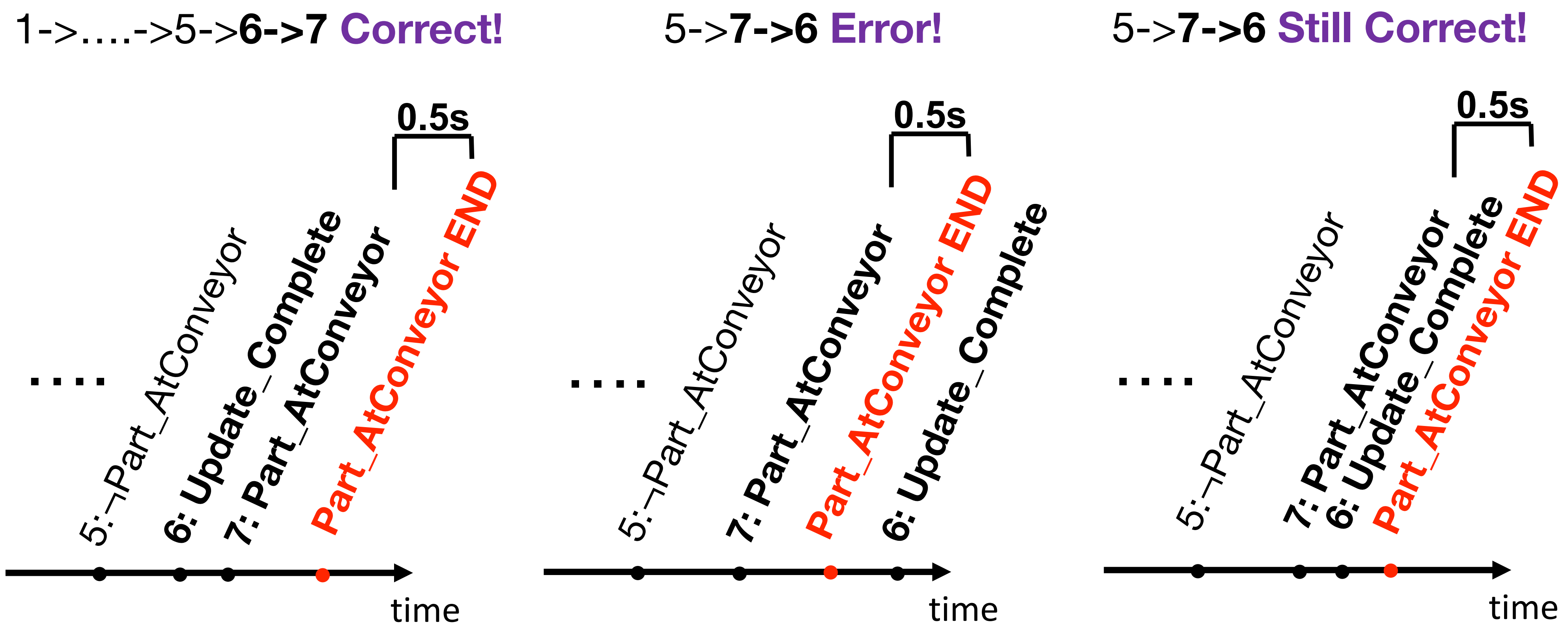
Events Received by PLC



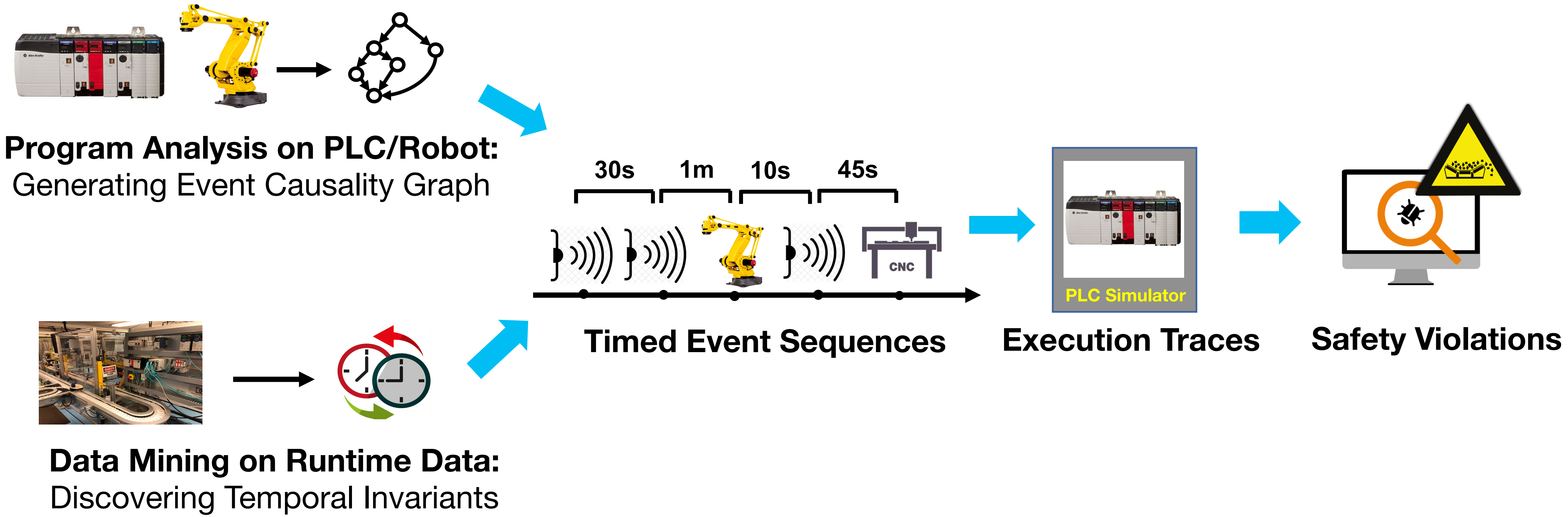


Violated ***TPTL Spec:*** $\Box t_x.(\texttt{Pallet} \rightarrow \Diamond t_y.(\texttt{Retract} \wedge t_y - t_x \leq 30\texttt{s}))$

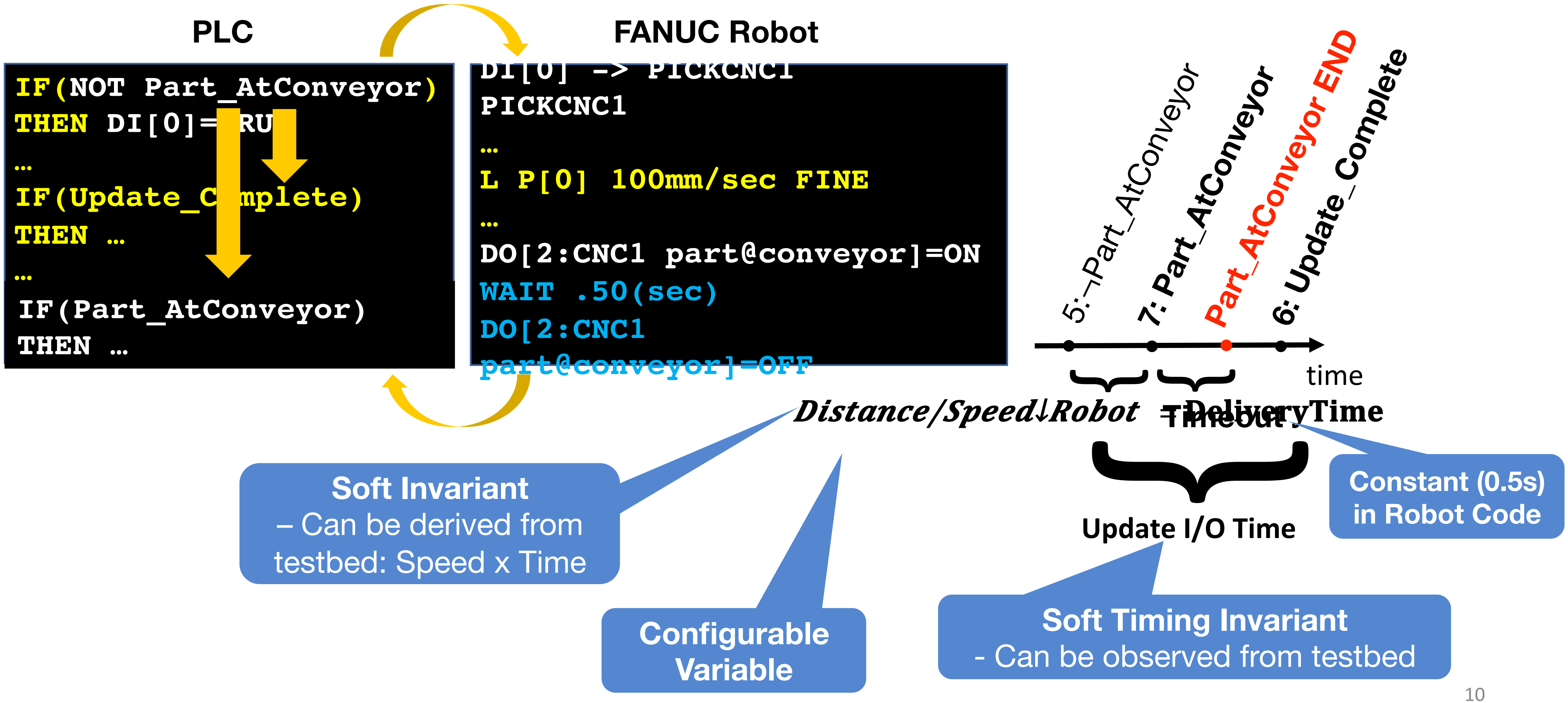
Traditional Event Permutation Doesn’t Solve the Problem



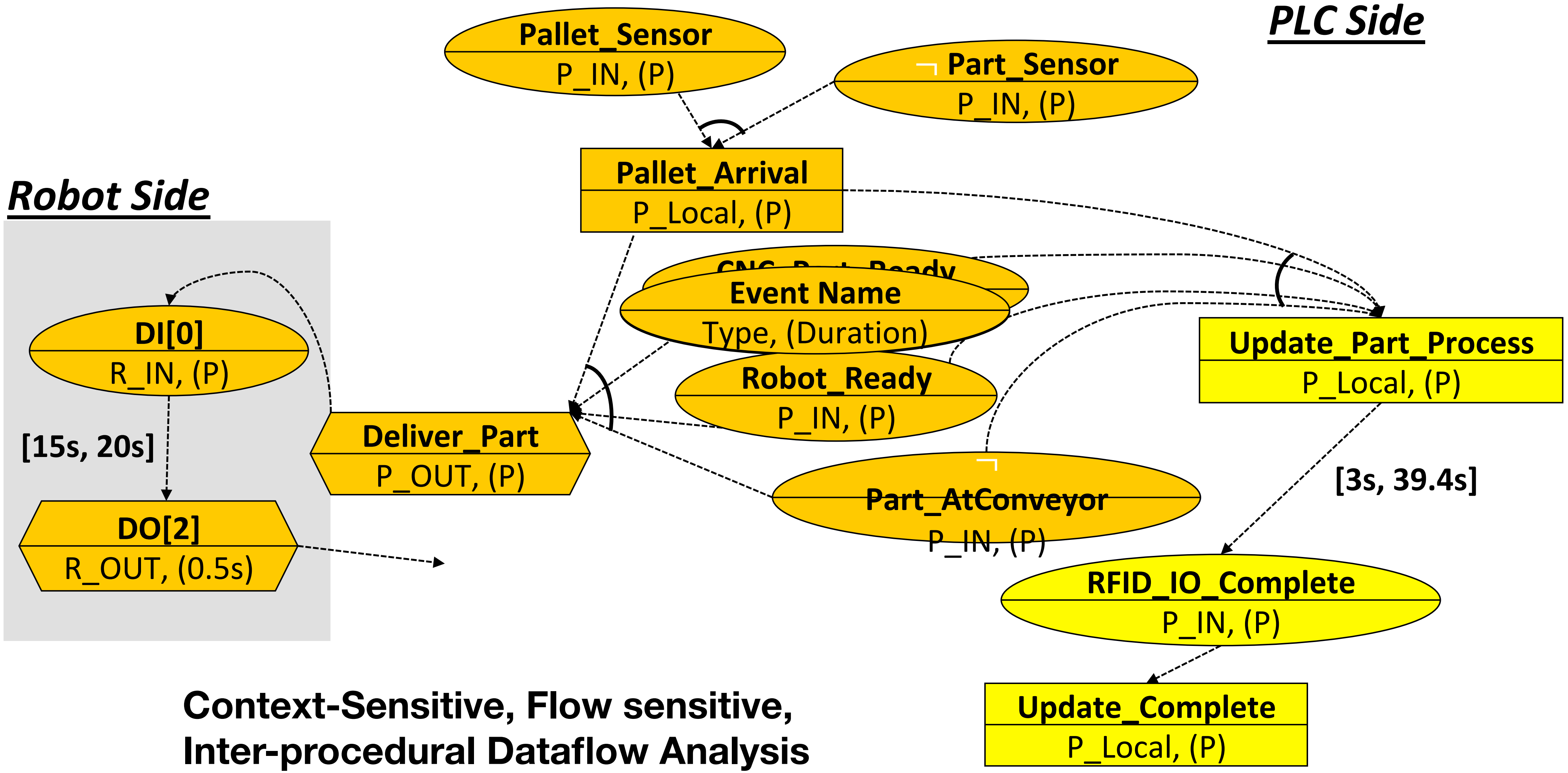
VetPLC: Generating **Timed Event Sequences** to enable Automated Safety Vetting of PLC Code



VetPLC on Running Example



Timed Event Causality Graph (TECG): Find Valid Event Orders



Context-Sensitive, Flow sensitive, Inter-procedural Dataflow Analysis

Mining Temporal Invariants for Events: 2 Steps

Step 1: Qualitative "followed-by":

– Synoptic (*FSE'11*)

Follows[ε_a][ε_b] = Occurrence[ε_a]

Step 2: Quantitative "with-in":

– Perfume (*ASE'14*)

$$\square\, t_x.(\varepsilon_a \rightarrow \Diamond\, t_y.(\varepsilon_b \wedge t_y - t_x \geq \tau_{lower}))$$

$$\square\, t_x.(\varepsilon_a \rightarrow \Diamond\, t_y.(\varepsilon_b \wedge t_y - t_x \leq \tau_{upper}))$$

Results for Motivating Example (1.2 GB data for 10 hours):

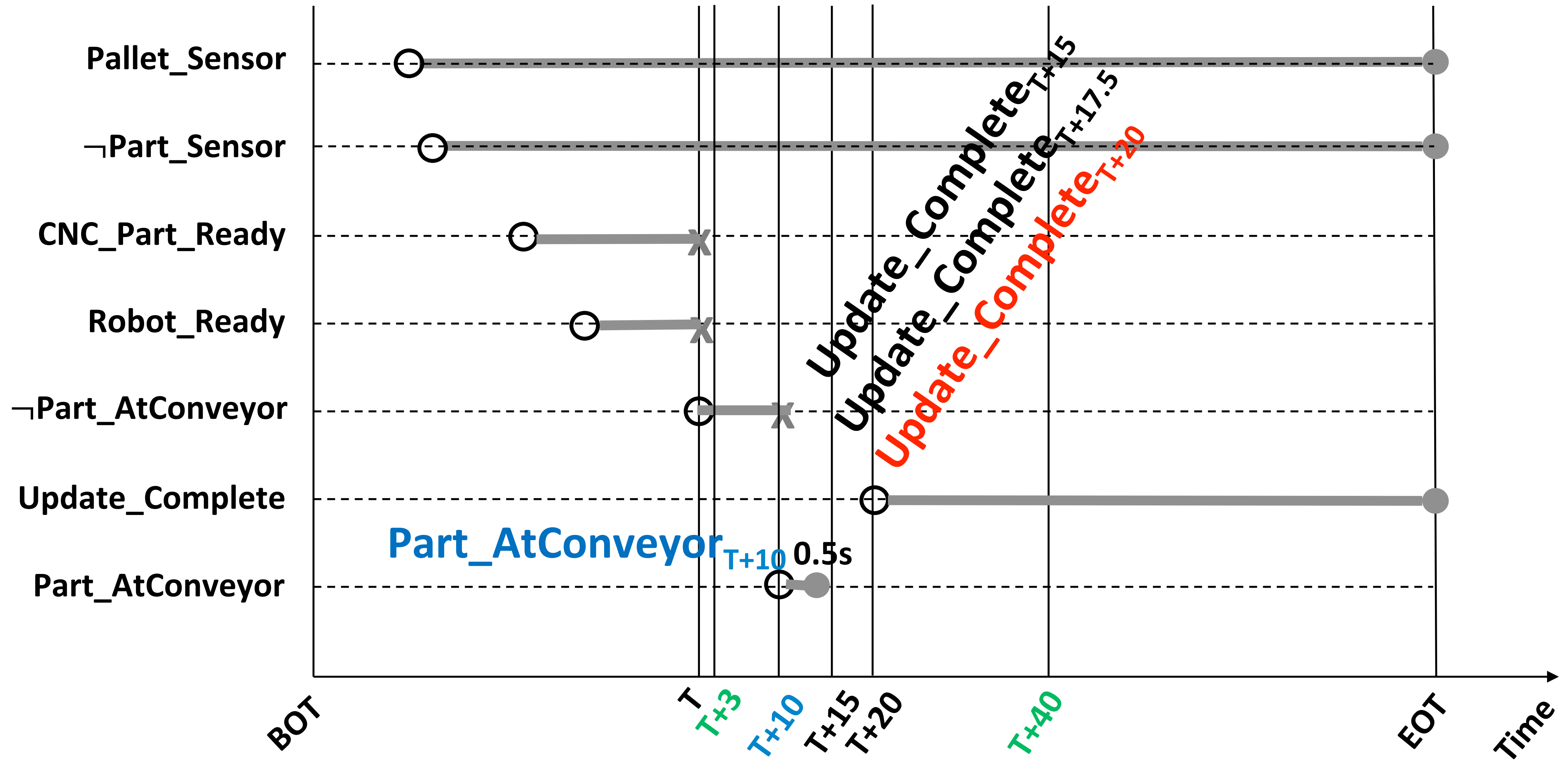
TABLE I: Mined Invariants

Event Pair	Invariant
$\square$(Deliver_Part → $\Diamond$Part_AtConveyor)	[24.4s, 24.6s]
$\square$(Update_Part_Process → $\Diamond$RFID_IO_Complete)	[15s, 20s]
$\square$(Update_Part_Process → $\Diamond$Update_Complete)	[15s, 20s]

Advantage of TECG: Only need to mine relations that do not contradict TECG

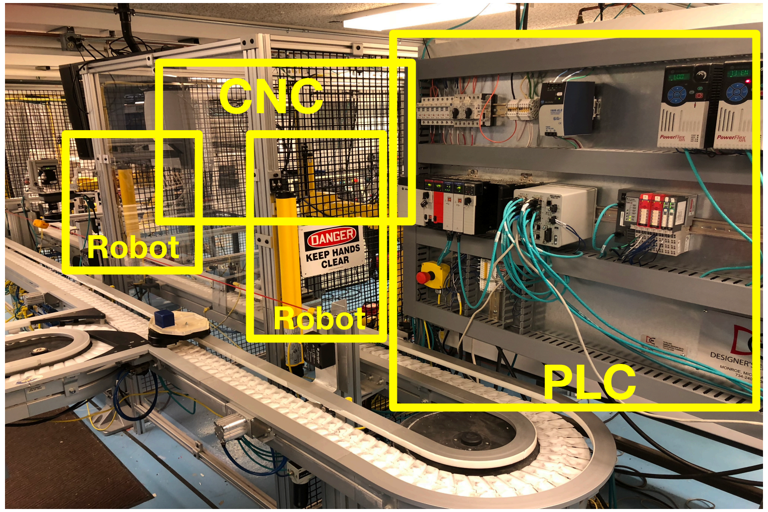
Creating Timed Event Sequences

Safety Violation Triggered
How to discretize durations?

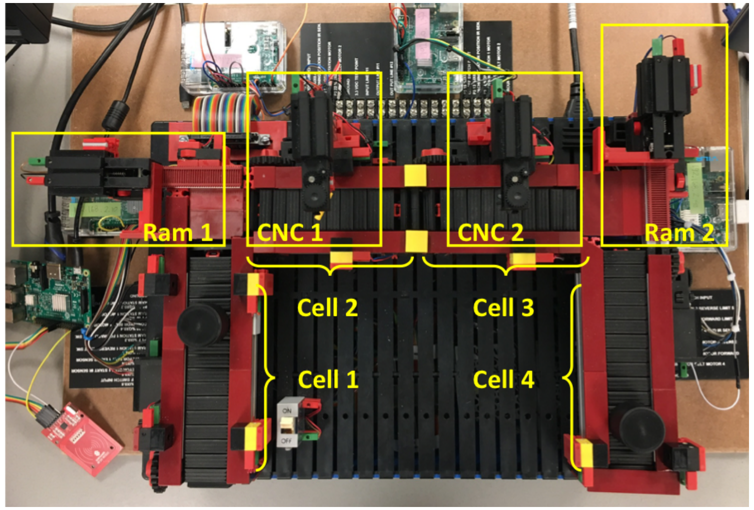


Evaluation on Real Testbeds for Different Scenarios

2 Different Testbeds



***SMART*: Automotive Production Line**



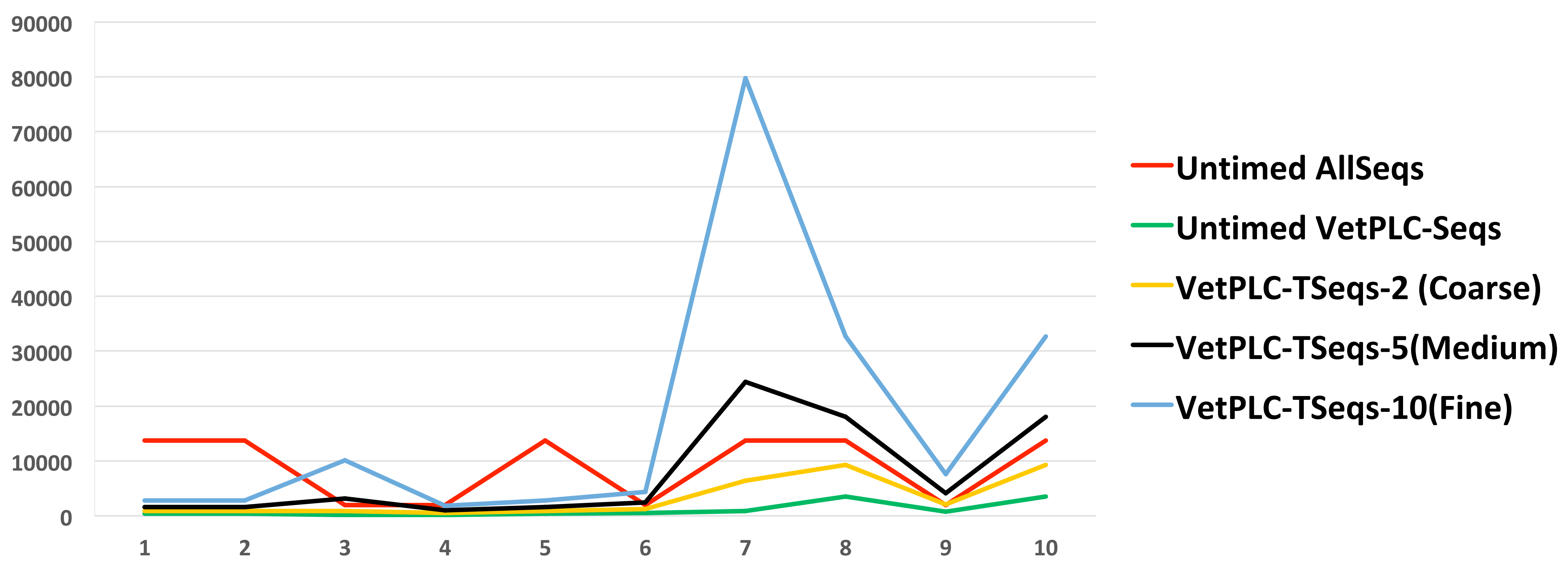
***Fischertechnik*: Part Processing w/ 4 PLCs**

10 Safety-critical Scenarios

S1: Conveyor Overflow #1
S2: Robot in Danger Zone
S3: Conveyor Overflow #2
S4: Part-Gate Collision
S5: CNC Overflow

S6: Ram-Part Collision
S7: CNC-Part Collision
S8: Conveyor Overflow #3
S9: Conveyor Underflow
S10: Ram-Part Collision #2

Evaluation: How many sequences are created?



Red → Green: Program analysis reduces amount of event sequences

Green → Orange → Black → Blue: Time discretization can significantly increases that

Bug Detected? State-of-the-Art vs. VetPLC

#	State-of-the-art	VetPLC
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

More Time Slices -> More Precise Error-Triggering Range

VetPLC Outperforms State-of-the-art!

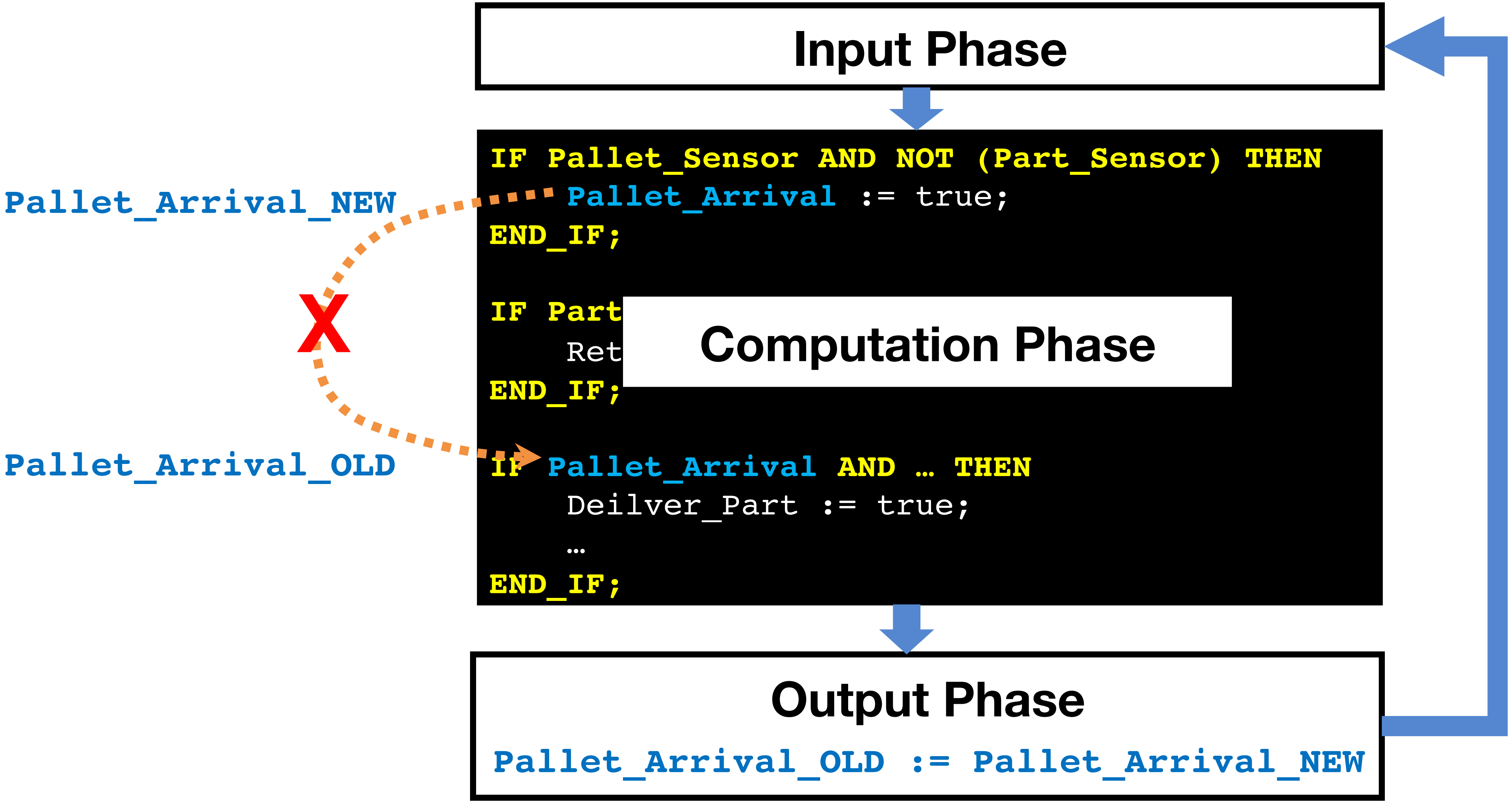
Empirically, 5 slices works better.

Conclusion

- **Insight:** real-world PLC code is *event-driven* and *timing-sensitive*
- **Solution:** VetPLC *automatically constructs timed event sequences* via analyzing event causalities in PLC/robot code plus mining runtime data from physical testbeds
- **Effectiveness:** VetPLC outperforms state-of-the-art and has found “organic” vulnerabilities in two different types of real-world ICS testbeds.

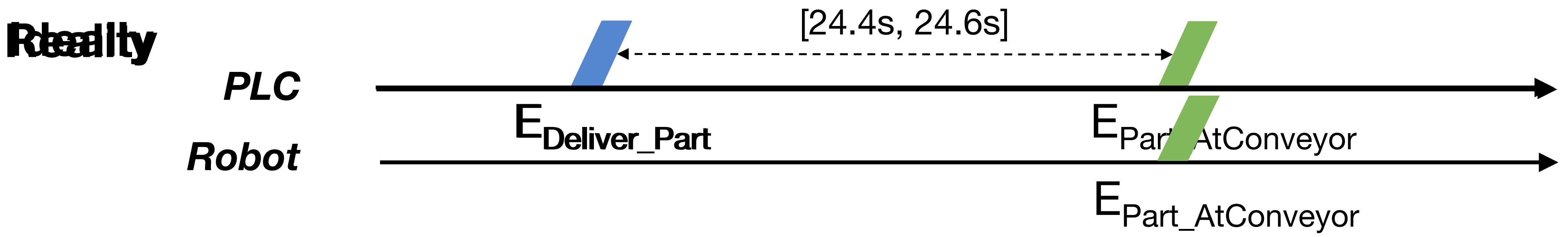
Thank you!

PLC Programming Paradigm: Scan Cycle

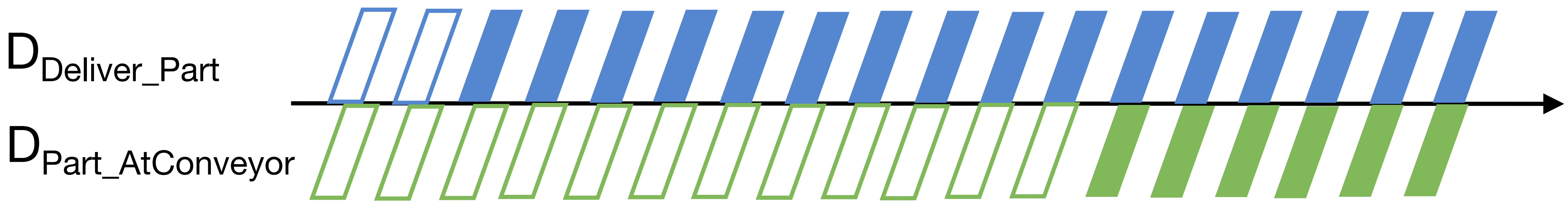


- No dataflow in one cycle
- Dataflow across cycles
- Any “Define” in a cycle may affect “Use” in the next

Technical Challenge: Distributed Event Sources



Solution: Inferring Events from State Variables



Speed Reconfiguration

$\because$

$$\tau_{lower} \leq \boldsymbol{T_{job}} = job/speed_{conf} \leq \tau_{upper}$$

Time variation caused by physical operations or program execution paths

$$\boldsymbol{speed_{min}} \leq speed_{conf} \leq \boldsymbol{speed_{max}}$$

Time variation caused by reconfiguring machine speeds

$\therefore$

$$\tau_{lower} \times speed_{conf} / \boldsymbol{speed_{max}} \leq \boldsymbol{T_{job}} \leq \tau_{upper} \times speed_{conf} / \boldsymbol{speed_{min}}$$

$Speed_{rated}$ $\quad$ $Speed_{high\text{-}throughput\text{-}and\text{-}safe}$

resulting in unpredictable robot motion and velocities.

3.41 slow speed control: A mode of **robot** motion control where the speed is limited to 250 mm/sec (10 in/sec) to allow persons sufficient time to either withdraw from **hazardous motion** or stop the robot.

3.42 space: The three dimensional volume encompassing the movements of all **robot** parts

Scenario-Specific Safety Specs

#	Description of Hazard	Safety Specification to Avoid Hazard
1	Motivating Example. See Section III	$\Box t_x.(\texttt{Pallet} \rightarrow \Diamond t_y.(\texttt{Retract\_Stopper} \wedge t_y - t_x \leq \texttt{30s}))$
2	Robot fails to return its safe zone.	$\Box t_x.(\neg\texttt{Safe\_Zone} \rightarrow \Diamond t_y.(\texttt{Safe\_Zone} \wedge t_y - t_x \leq \texttt{60s}))$
3	Robot stops processing parts from conveyor due to signal conflicts.	$\Box t_x.(\texttt{Pallet} \rightarrow \Diamond t_y.(\texttt{Retract\_Stopper} \wedge t_y - t_x \leq \texttt{30s}))$
4	A pallet collides with a closed gate.	$\Box(\texttt{Pallet\_AtGate} \rightarrow \Box\texttt{Gate\_Open})$
5	CNC stops processing parts from gantry due to missing signals.	$\Box t_x.(\texttt{Part\_In} \rightarrow \Diamond t_y.(\texttt{Part\_Out} \wedge t_y - t_x \leq \texttt{5m}))$
6	A ram starts pushing when a part has not fully entered the ram.	$\Box(\texttt{Part\_Entering} \rightarrow \neg\Diamond\texttt{Ram\_Push})$
7	A part is passed to CNC when a preceding part is not fully discharged.	$\Box(\texttt{CNC\_Busy} \rightarrow \neg\Diamond\texttt{Part\_Arrival})$
8	Parts are pushed to conveyor prematurely.	$\Box t_x.(\texttt{Part\_Arrival} \rightarrow \Diamond t_y.(\texttt{Part\_Arrival} \wedge t_y - t_x \leq \texttt{6s}))$
9	A conveyor belt halts operation.	$\Box t_x.(\texttt{Part\_Arrival} \rightarrow \Diamond t_y.(\texttt{Part\_Arrival} \wedge t_y - t_x \geq \texttt{8.5s}))$
10	Ram1 pushes a part to unprepared Ram2.	$\Box(\texttt{Part\_Entering} \rightarrow \Box\texttt{Ram\_Ready})$