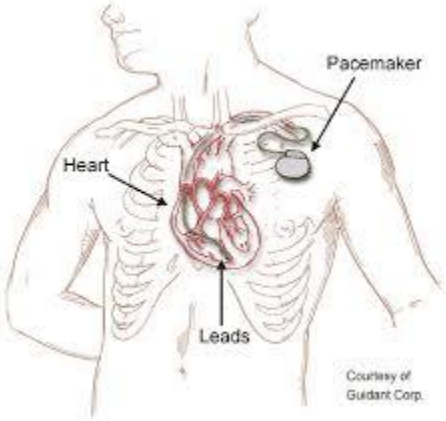
Good Enough Dependability: A Unified Paradigm for Dependable Systems Design

Karthik Pattabiraman

http://blogs.ubc.ca/karthik

THE UNIVERSITY
OF BRITISH COLUMBIA

Computer Systems are Everywhere



Dependability of computer systems is paramount

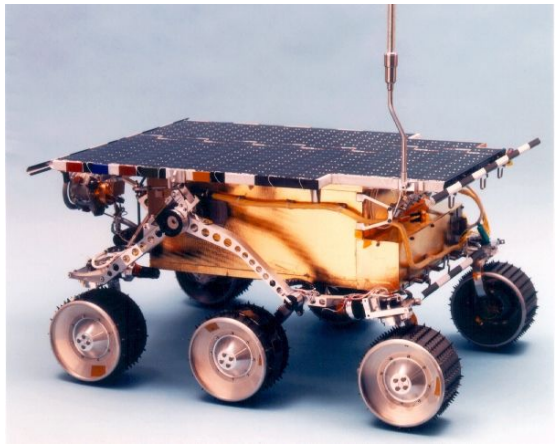
Traditional Dependability Approaches

Hardware Redundancy

- IBM Mainframes, Tandem Non-stop – full duplication
- Huge energy and performance overheads

Formal Verification

- Space exploration (e.g., NASA Mars rover)
- Requires significant time and resources, as well as expertise



The “Good Enough” Revolution

Source: WIRED Magazine (Sep 2009) – Robert Kapps
http://www.wired.com/gadgets/miscellaneous/magazine/17-09/ff_goodenough

People prefer “cheap and good-enough” over “costly and near-perfect”

Can we build dependable systems with this principle ?

“Good Enough” Dependable Systems

- **Just reliable enough to get the job done**
  - Do not provide the illusion of perfection to end user
  - But do not fail catastrophically or cause severe errors
  - Depends on the application and its context of use

Low Reliability:
Entertainment Applications

Bank Reconciliation — ABC Company — Ctrl + M

Ledger: HDFC Bank — 1-Apr-2010 to 5-Dec-2010

(Reconciliation)

Date	Particulars	Favouring Name / Received From	Vch Type	Transaction Type	Instrument No	Instrument Date	Bank Date	Debit	Credit
25-3-2010	Universal Suppliers		Opening BRS	Cheque/DD	123487	25-3-2010	[redacted]		93,354.00
26-3-2010	Transtronics Limited		Opening BRS	Cheque/DD	123495	26-3-2010			80,000.00
31-3-2010	Q-Base Technologies		Opening BRS	Cheque	009654	31-3-2010		21,000.00	
5-7-2010	Other Incomes		Receipt	Cheque/DD	837433	5-7-2010		10,000.00	
5-8-2010	Rent	Ramlal Nikhanj	Payment	Cheque	A/c Payee	5-8-2010			15,000.00
5-8-2010	Other Incomes		Receipt	Cheque/DD	564647	5-8-2010		10,000.00	
25-8-2010	A-One Traders		Receipt	Cheque/DD	423428	25-8-2010		25,000.00	
25-8-2010	A-One Traders		Receipt	Inter Bank Transfer	234235333433	25-8-2010		25,000.00	
24-9-2010	Bangalore Chemicals Fertilizers		Payment	Inter Bank Transfer	123456789012	24-9-2010			20,000.00
25-9-2010	Bangalore Chemicals Fertilizers		Payment	Cheque	676460	25-9-2010			10,000.00
26-9-2010	Hindustan Suppliers		Payment	Cheque	100006	26-9-2010			8,650.00
26-9-2010	State Bank of India	ABC Company	Contra	Inter Bank Transfer	001000098983	26-9-2010		10,000.00	
27-9-2010	Virupaksha Traders		Payment	Cheque	453452	27-9-2010			30,000.00
27-9-2010	Virupaksha Traders		Payment	Cheque	453453	30-9-2010			10,000.00
28-9-2010	Computer Kraft	Computer Zone	Receipt	Cheque/DD	234211	28-9-2010		5,000.00	
28-9-2010	Computer Kraft	Computer Zone	Receipt	Cheque/DD	435778	28-9-2010		45,000.00	
28-9-2010	Computer Kraft	Computer Zone	Receipt	Inter Bank Transfer	3424675676766	28-9-2010		25,000.00	
29-9-2010	Hindustan Suppliers		Payment	Cheque	787877	29-9-2010			35,600.00
29-9-2010	Hindustan Suppliers		Payment	Inter Bank Transfer	78787784544544	29-9-2010			10,000.00
29-9-2010	Bhavish Trading Co.,	Courier	Receipt	Cheque/DD	786555	29-9-2010		30,000.00	
29-9-2010	Unique Traders		Receipt	Cheque/DD	983222	29-9-2010		25,000.00	
29-9-2010	Manba Finance Limited		Receipt	Cheque/DD	900099	29-9-2010		15,000.00	

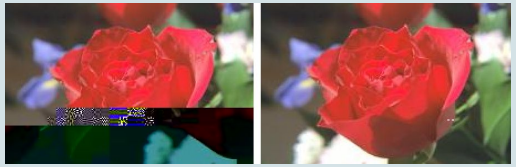
6 more ...

Balance as per Company Books	1,85,004.00	
Amounts not reflected in Bank	2,76,000.00	3,57,604.00
Balance as per Bank	**2,66,608.00**	

High Reliability:
Financial Services

Good Enough Dependability

Hardware Error Resilience

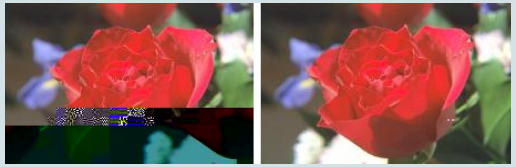


Web Application Reliability

Selective Security Protection

Good Enough Dependability

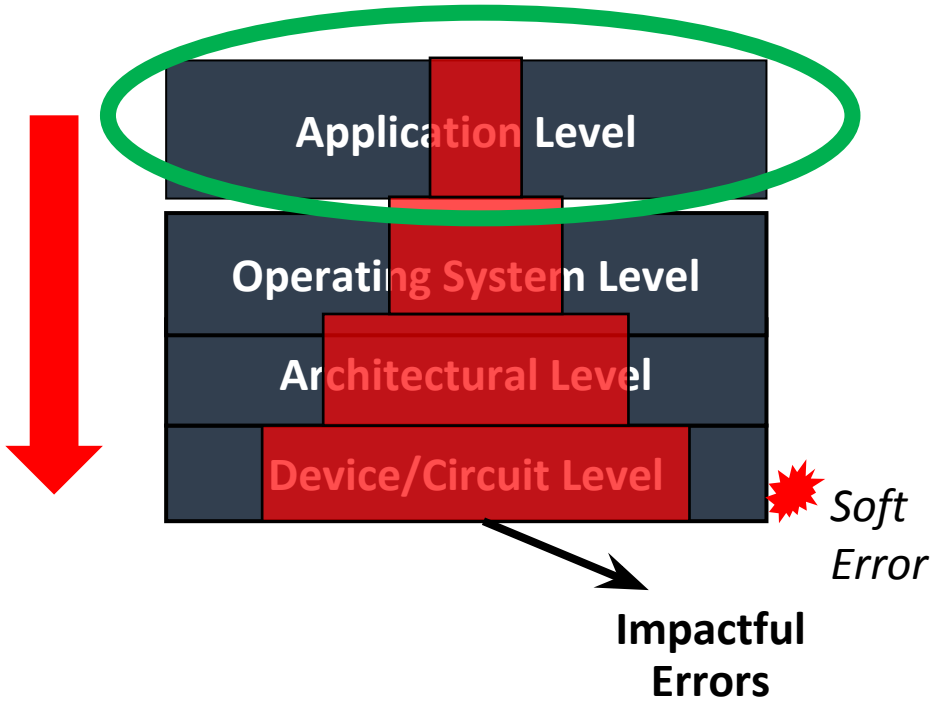
Hardware Error Resilience

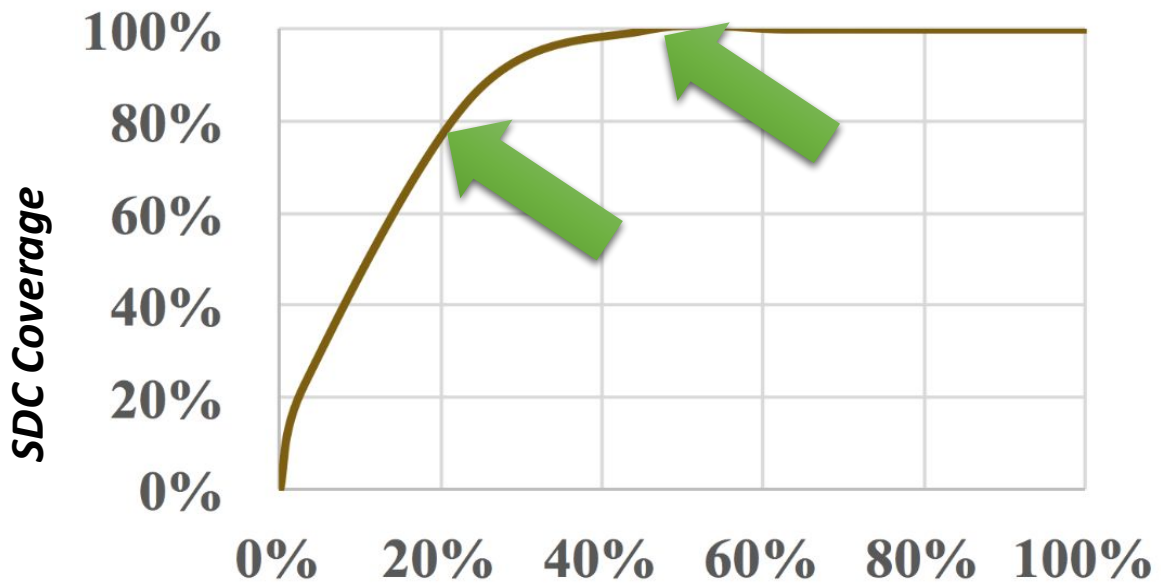


Web Application Reliability

Selective Security Protection

Why does this approach work ?



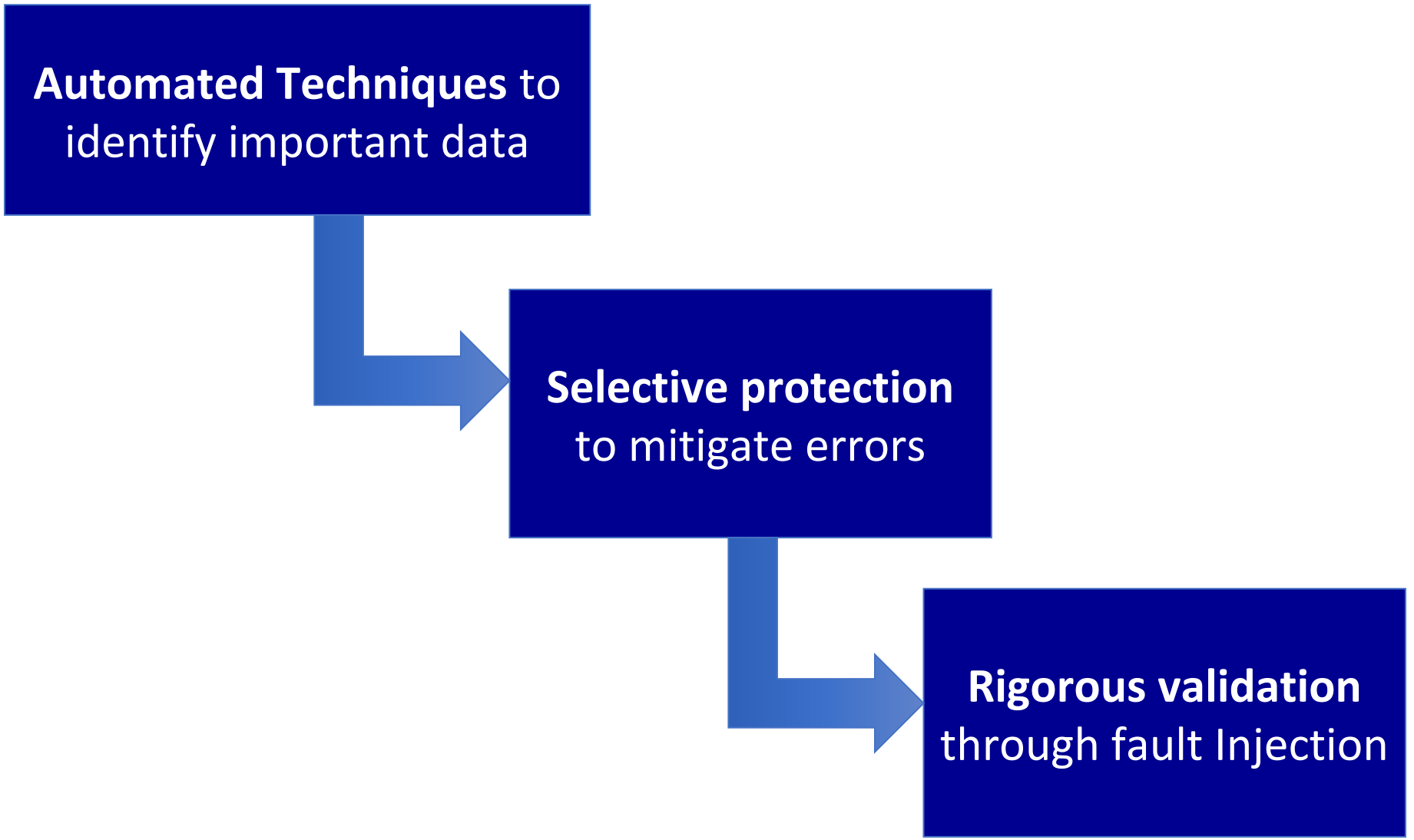


The Cost-Benefit Curve of Selective Duplication (Liquantum)

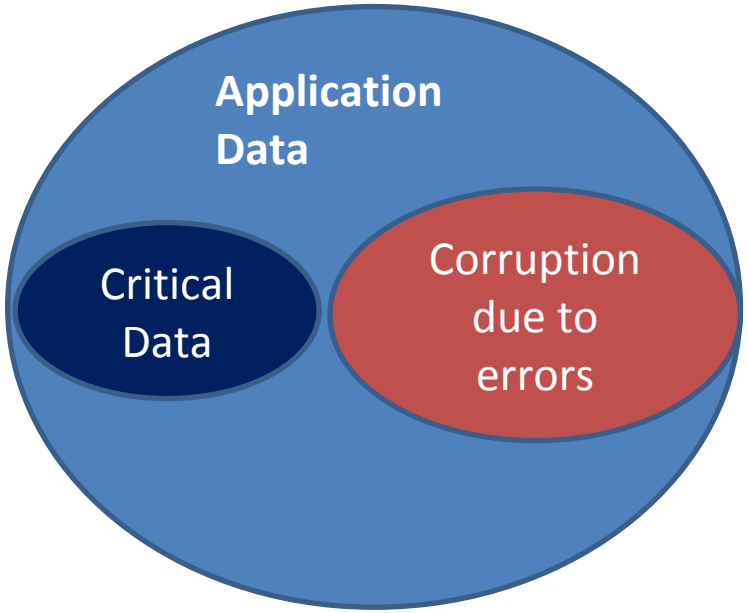
Software protection techniques are more flexible and cost-effective!

About 80% of SDCs can be mitigated by 20% overhead (80-20 rule)

Good Enough Dependability: Approach



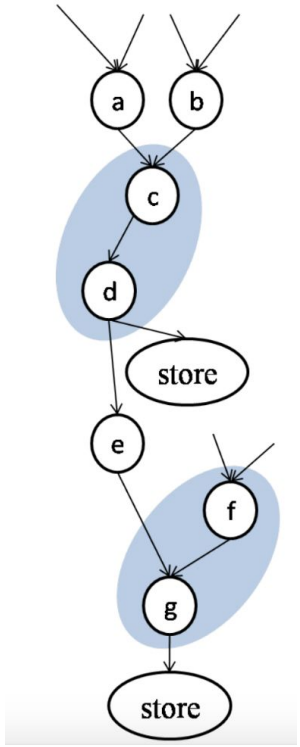
Step 1: Automated Identification



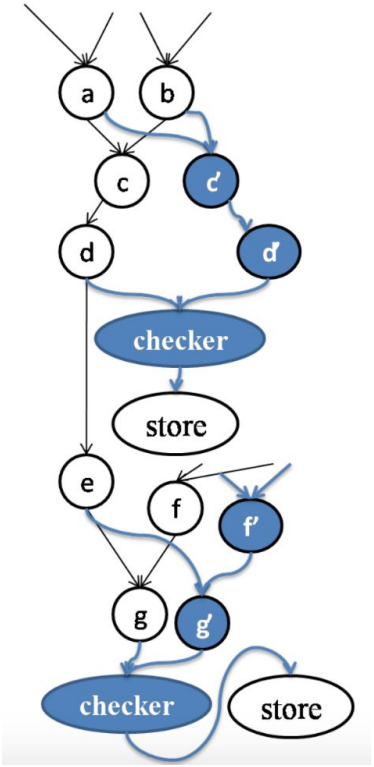
Critical Data is correlated with high-level static program characteristics

- Type System [ASPLOS'11][CSF'11]
- Heuristics [DSN'13][TECS][DSN'15]
- Machine Learning [CASES'14][TECS]
- Analytical Models [DSN'16][DSN'18]

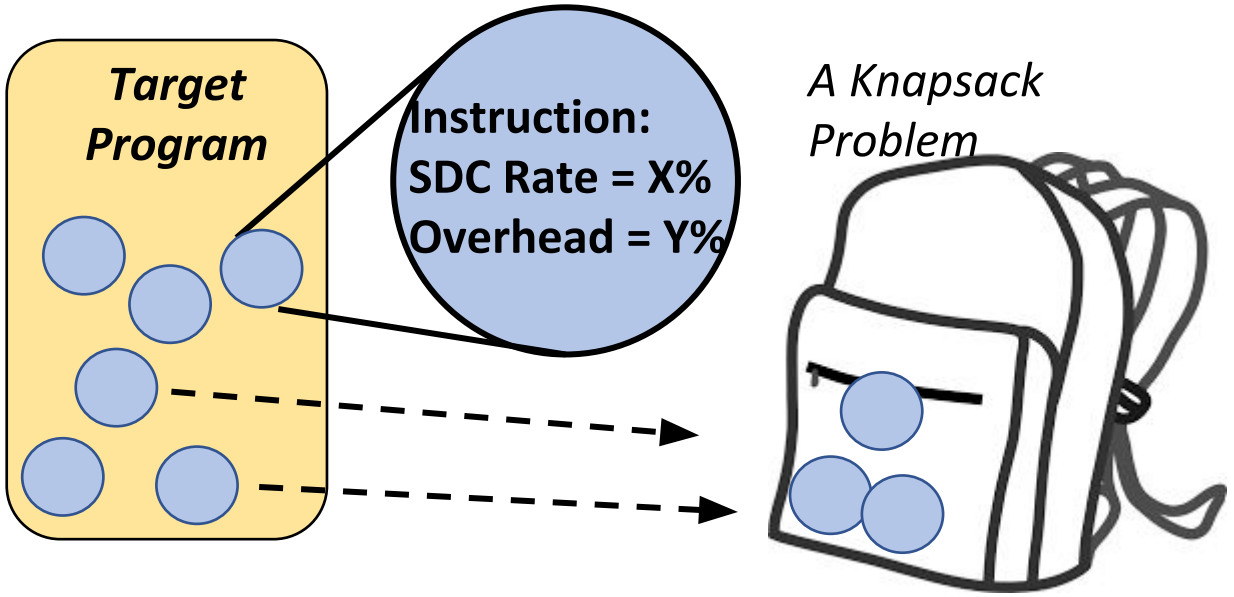
Step 2: Selective Protection



Original Program

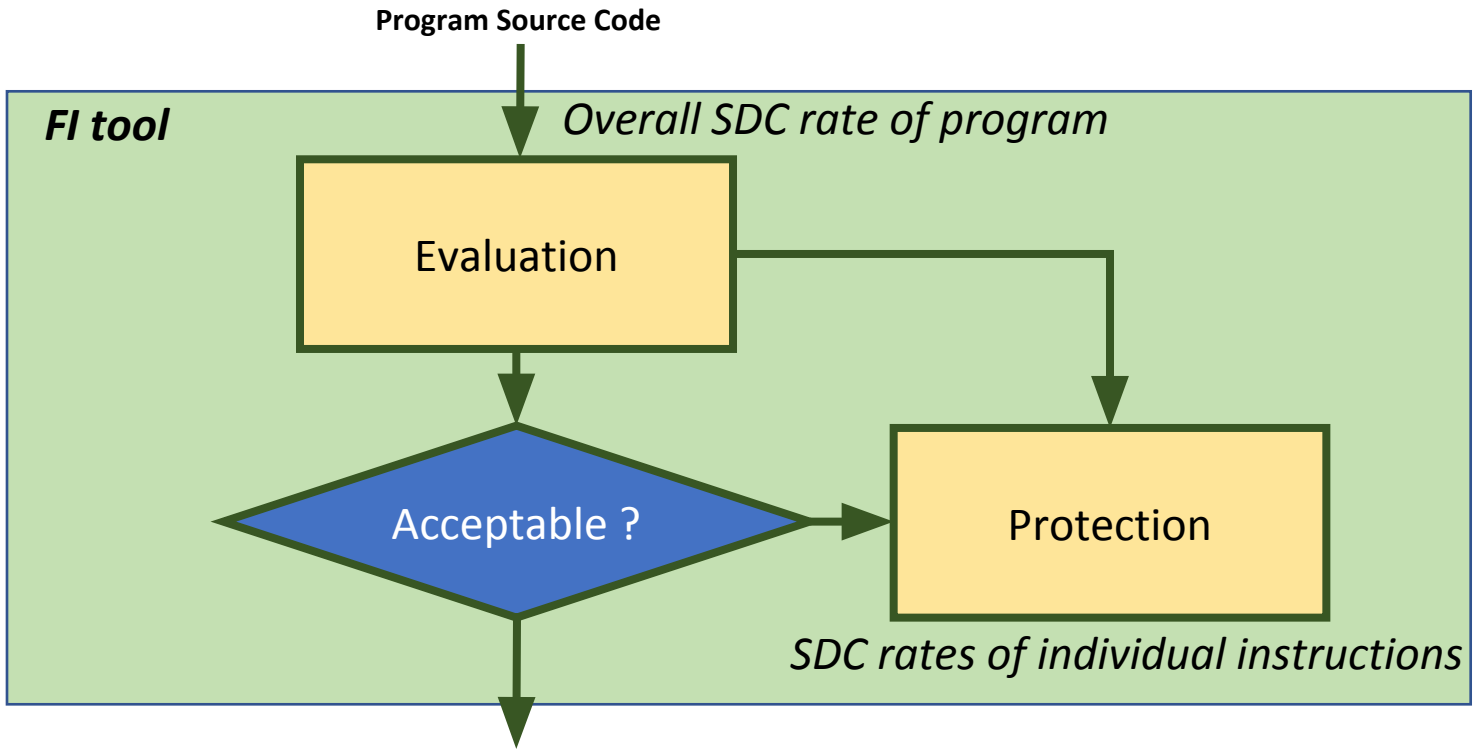


Selective Duplication

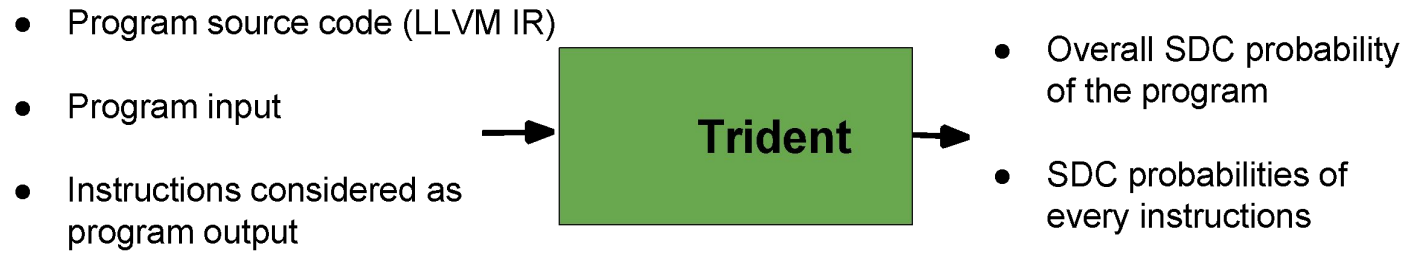


Step 3: Fault Injection Validation

- LLFI [DSN'14][QRS'15]
- PINFI [DSN'14]
- GPU-Qin [ISPASS'14]
- LLFI-GPU [SC'16]

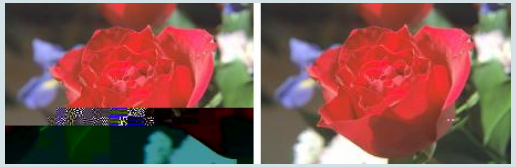


Trident, vTrident [DSN'18A][DSN'18B]



Good Enough Dependability

Hardware Error Resilience

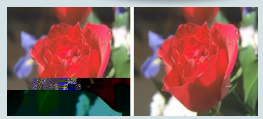


Web Application Reliability

Selective Security Protection

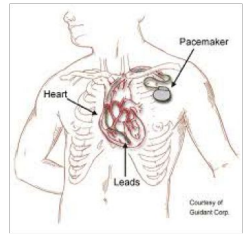
Good Enough Dependability

Hardware Error Resilience



Web Application Reliability

Selective Security Protection



Programming Models

Resilient Operation

Adaptive Security

Internet of Things (IoT) Dependability

Good Enough Dependability: Takeaways

- **Errors and attacks are becoming common in commodity systems**
  - **Cost is the all important factor in these systems**

- **But, most errors (attacks) don't matter much, in many cases !**

- **Important to focus on the few errors (attacks) that matter**
  - Provide targeted protection for the important errors (attacks)
  - Goal is not to achieve near 100% coverage, but keep costs low
  - Automated techniques to trade-off coverage for cost

Thanks …

Students (Current and Past) - 12 PhD, 20 MS, 30 Undergrad

http://blogs.ubc.ca/karthik