Formal Methods at Scale

Workshop 2019-09-25

The FM@Scale Workshop

- 0900: Welcome: Brad Martin
- 0915: One Minute of Fame for each participant
- 0945: Goals of meeting: Pat Lincoln and Bill Scherlis
- 1015: Tom Ball and Jonathan Protzenko
- 1045: break
- 1100: Case introduction: Darren Cofer
- 1130: Panel: Formal Methods for systems: Janos Sztipanovits, Ray Richards, Sandeep Neema
- 1230: gather lunch
- 1300: Lunch talk: Nina Amia
- 1400: Case Introduction: Marjin Huele
- 1430: Andrew Appel and Ben Pierce
- 1500: break
- 1515: Panel: Formal + Informal: Stephen Magill, Arlen Cox, Paul Miner
- 1615: Jeannette Wing
- 1645: Take aways: one minute each participant
- 1715: adjourn

One Minute of Fame

- Introduce yourself to the group
  - Name
  - Institution
  - One of:
    - Favorite Flavor of Formal Method
    - Favorite Application Domain
    - Favorite fact from last decade that indicates to you that formal methods is ready to scale

Welcome to SRI, Rosslyn Facility, Logistics

- SRI: not-for-profit, ~1,500 staff, ~1,000 projects a year (.gov & .com)
  - Founded as Stanford Research Institute 70+ years ago, now independent (not FFRDC)
  - We invent stuff: SMT solving (Yices), Virtual Personal Assistants (Siri), Telepresence Surgery (DaVinci), Ultrasound Imaging, Intrusion Detection, Speech-to-text (Nuance)
  - We are hiring in computer security and privacy, formal methods, and machine learning

- Caffeine and food behind you, in the corner of the building with the best view
- Restrooms behind the elevators
- In case of emergency, follow the crowd to the two stairways near the elevators
  - Down to Mezzanine, out main entrance,
    or up to roof deck if you have a parachute and do base jumping

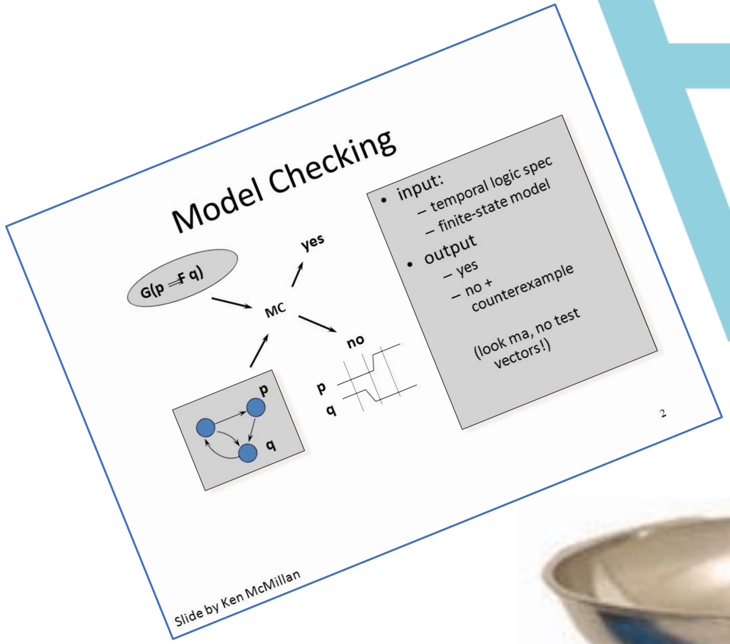
At Least Two Dimensions To Discuss Today

Scale

- (1) the range of properties and qualities that are modeled and reasoned about, such as relating to security, safety, performance, fault tolerance, real-time, etc.
- (2) complexity and the size of systems and their supply chains, including issues related to composability
- (3) efficiency of FM-related modeling, tooling, and engineering practices, including integration into mainstream tooling and practices
- (4) ability to rapidly co-evolve systems and associated evidence
- (5) ease of use for non-expert developers and evaluators

Experience

- (1) applications to specific major systems in government and industry
- (2) tour-de-force results, such as proofs of significant mathematical results or reasoning about modern processors
- (3) the advancement of formal methods ecosystems surrounding the various provers and stacks
- (4) integration of more limited capabilities into broader communities of practice, such as has been happening in major tech firms.



Model Checking

G(p ⇒ F q)
MC
yes
no
p
q
p
q

- input:
  - temporal logic spec
  - finite-state model
- output
  - yes
  - no + counterexample

(look ma, no test vectors!)

2

Slide by Ken McMillan

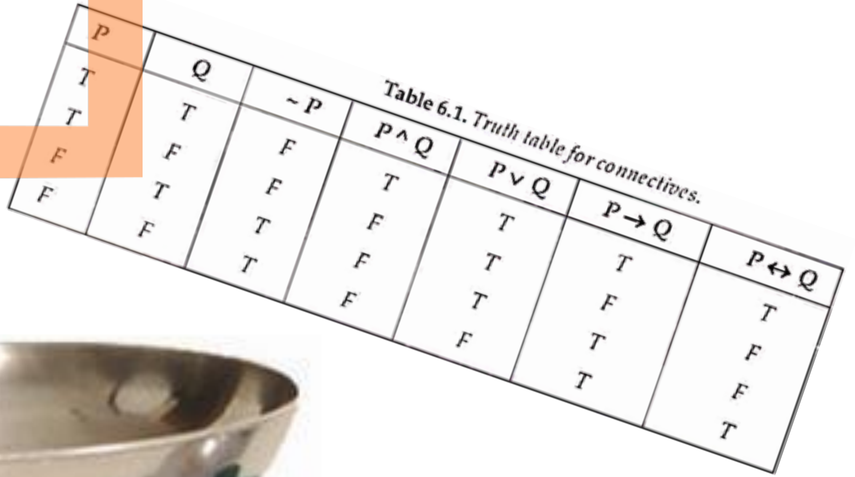


Table 6.1. Truth table for connectives.

P	Q	~ P	P ∧ Q	P ∨ Q	P → Q	P ↔ Q
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

Questions?

Patrick Lincoln
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025-3493
650.859.4105
patrick.lincoln@sri.com

www.sri.com

Headquarters: Silicon Valley

SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025-3493
650.859.2000

Washington, D.C.

SRI International
1100 Wilson Blvd., Suite 2800
Arlington, VA 22209-3915
703.524.2053

Princeton, New Jersey

SRI International Sarnoff
201 Washington Road
Princeton, NJ 08540
609.734.2553

Additional U.S. and
international locations

www.sri.com

Workstations
NO IP
Basic Data
Main Data
RISE OF THE HACKERS
NOVA
SRI
International
WORM
THE FIRST DIGITAL WORLD WAR
MARK BOWDEN

SRI

Independent, non-profit research institute founded by Stanford University in 1946

- 2,000+ staff members; 2/3 advanced degrees
- $500M in annual revenues
- Locations:
  - Menlo Park, CA
  - Princeton, NJ
  - Arlington, VA
  - Ann Arbor, MI
  - San Antonio, TX

- 1,000 R&D projects per year
- 4,000 patents
- 60+ spin-off companies & 100+ licenses

San Francisco
SRI
Sand Hill Road
Stanford University
NASA Ames
San Jose

SRI's Mission: **Promote peace, prosperity, and the public good**

SRI creates **WORLD-CHANGING SOLUTIONS** making people safer, healthier, and more productive

SRI is an Independent Non-Profit Research Institute

(SRI is not a university, not an FFRDC, not a UARC)

Independent
mission-driven
non-profit

Connected to commercial, US
government, and international
partners for innovation

Culture fostering innovation,
client-focus, and entrepreneurial
research and development

A Legacy of SRI service to US government

High-impact research, open-source community contributions, close-held proprietary advantages, and commercial spinoff companies

Non-profit founded over
70
years ago

Partnered with nearly
EVERY
federal agency with an R&D mission

$4B+
of federal research contracts the past **10 years**

60+
spin-off companies generating **billions** in marketplace value

Historical Highlights

of innovation with the Government and other partners

First autonomous robot

Computer mouse

ARPANET

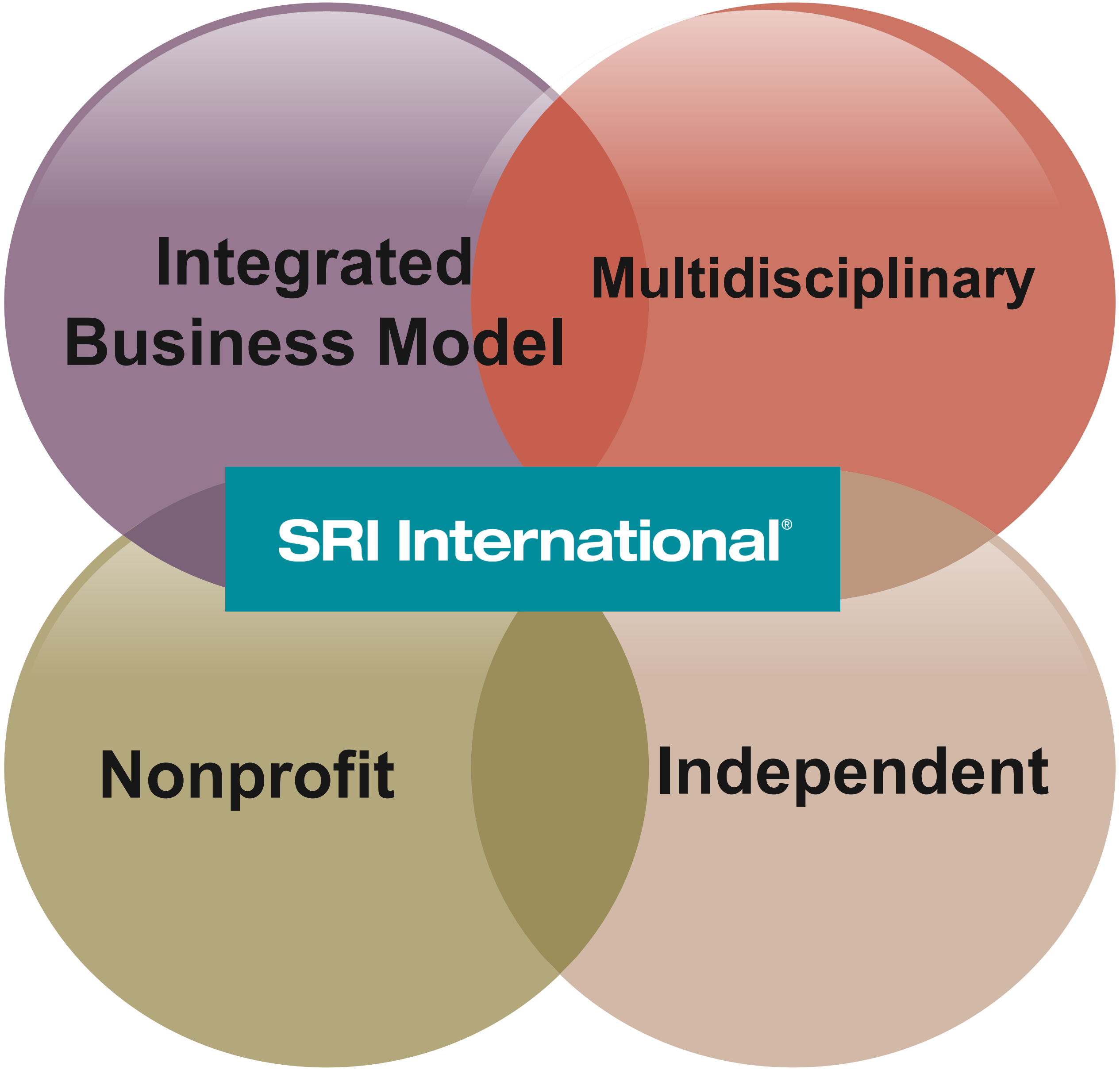
Stealth technology

Anti-Malaria drugs

National Education Policies

What is SRI?

From basic science to customer transitions



Breadth and depth to solve the hardest problems

ROI measured by impact

Focused on customers needs, and helping them see “beyond the headlights”

SRI’s engine delivers innovation and results

1,500
Staff Members

60%
hold advanced degrees

1,000
R&D Projects a Year

200
Patent Applications Year

>20%
Patent Utilization Rate Compared to 1-3% Corporate Rates

~5
Spinoffs a Year
fueled by innovations funded and utilized by the
FEDERAL GOVERNMENT

SRI Has Delivered Breakthrough Innovations to the Government…

SRI invented
Computer Mouse

SRI received the first
packet on ARPA-Net

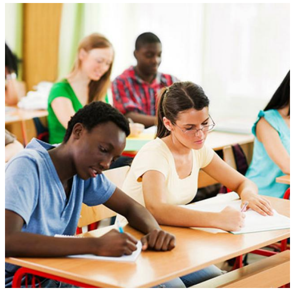
DARPA PAL Command
Post of the Future

SRI Managed NIC from
1970-91

GPS Tracking

Medical Robotics

Shakey, the first
mobile robot, 1966



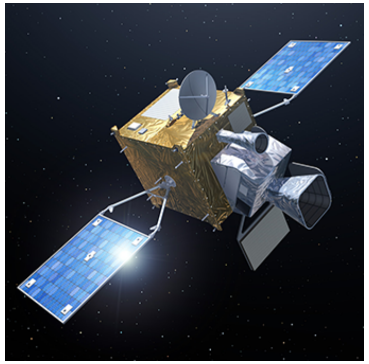
National Education
Strategy

Anti-Cancer
Drugs

Desert Owl
Saving soldier's lives

Formal Reasoning
Systems for Assurance

…And Spin-Out Companies from government research

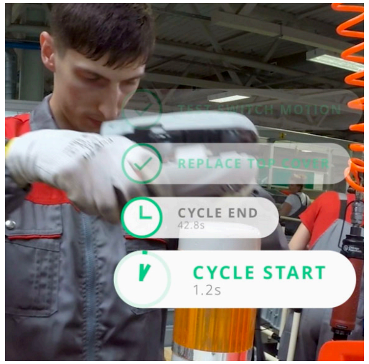


Leo Labs
Where are my
satellites?

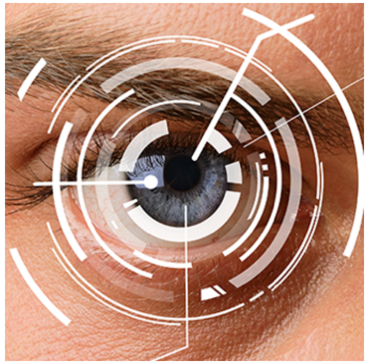
Intuitive Surgical
Where are the
surgeon's hands?

"Set reminder to buy gazpacho when I leave"
tap to edit
Here's your reminder for when you leave here:
Reminder
Buy gazpacho
Cancel
Confirm

Siri
What can a virtual
personal assistant
do for us?



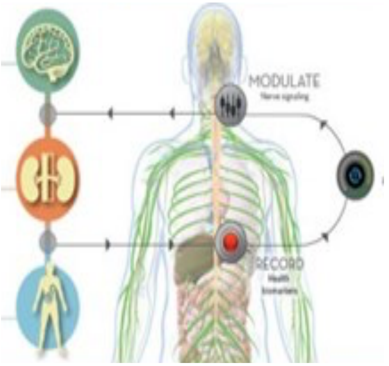
Drishti
What do we do next
in this assembly or
maintenance job?



Princeton Identity
Who is that at the
other end of our
transaction?

Seismic
How to augment
our physical ability:
Exo-muscle?

Nuance
Who is talking?
What are they saying?

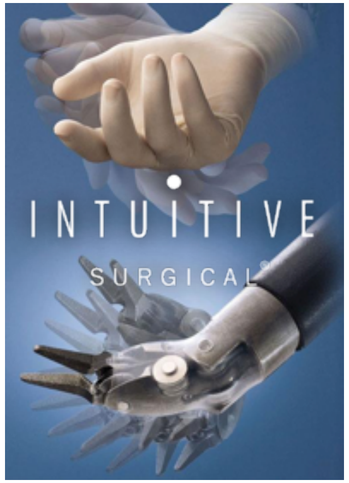


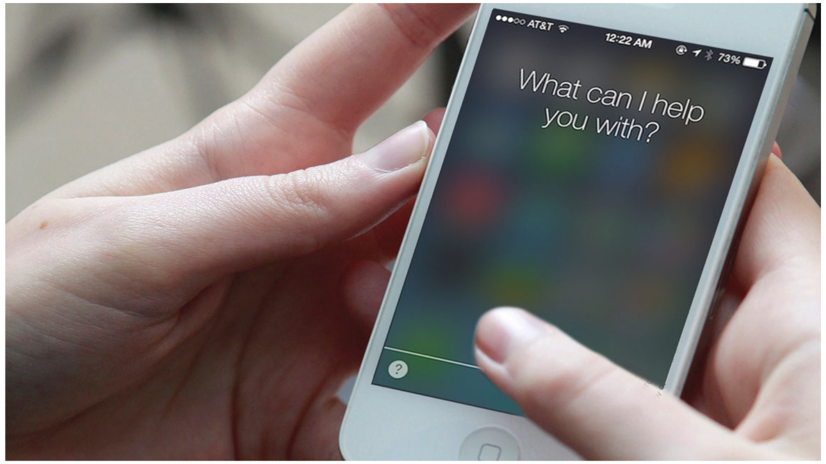
Neurome
Can we control our
internal organs?

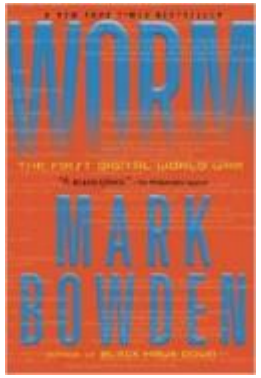
SRI History and Press

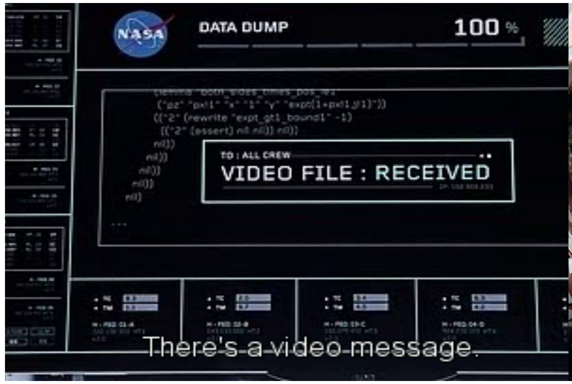
Electronic banking

Mother of All Demos








DATA DUMP 100 %

TO : ALL CREW

VIDEO FILE : RECEIVED

There's a video message.