Inference Engine applied to School Security for Robot-Man Teaming

Sponsor: US Army ARDEC SED

By
Mr. Jorge R. Buenfil
6th Annual SERC Doctoral Students Forum
November 7, 2018
FHI 360 CONFERENCE CENTER
1825 Connecticut Avenue NW
8th Floor
Washington, DC 20009

www.sercuarc.org

SYSTEMS ENGINEERING RESEARCH CENTER

Presentation Plan

RDECOM ARDEC

1. Motivation
2. Approach
3. Architecture
4. Design
5. V&V
6. Future Work
7. Q & A

Academic Committee

- **Ph.D. advisor:**

  Jose Ramirez-Marquez, Ph.D.
  SIT Enterprise Science and Engineering

- **Committee:**

  Jon Wade, Ph.D.
  SIT Systems and Software Engineering

  Mo Mansouri, Ph.D.
  SIT Systems and Software Engineering

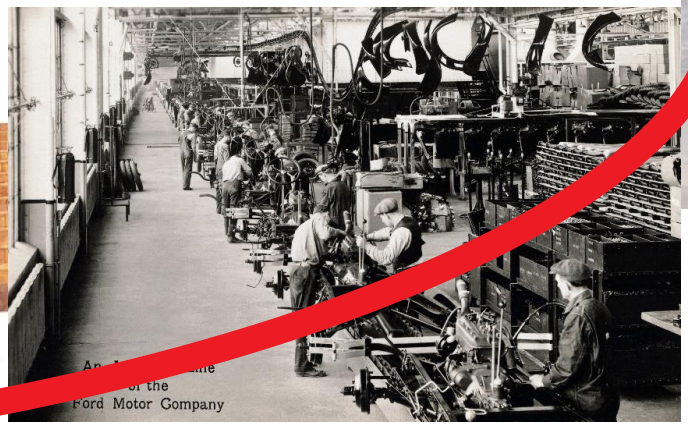
  Jason Cook, Ph.D.
  US Army RDECOM ARDEC

Dissertation Topic

Systems Engineering Architectural Framework for Decision Support Systems based on an Inference Engine and Deep Learning.

SE Challenges

We are witnessing the 3rd revolution of systems to enhance human labor. We have gone from all labor being human and animal muscle, to mechanized labor, to mechatronics and now narrow artificial intelligence on the way to general AI and fully autonomous systems.



SYSTEMS ENGINEERING RESEARCH CENTER

Research Interest

RDECOM ARDEC

Advance the state of the art in systems engineering to better grapple with 21st century engineering problems where robotics and automation drive both the solutions and challenges we face to create and control intelligent systems capable not only of reprogramming themselves but also of creating other intelligent systems on their own without human intervention.

SYSTEMS ENGINEERING RESEARCH CENTER

Why It Matters

RDECOM ARDEC

This research matters because rapid advances in robotics and neural networks make it possible to create a whole new category of complex systems that vastly outpace the traditional systems engineering cycles or creating concepts of operations, requirements, architecture, design, prototyping, testing, validation, etc.

To control artificial intelligence it will be necessary to use artificial intelligence.

State of the Art

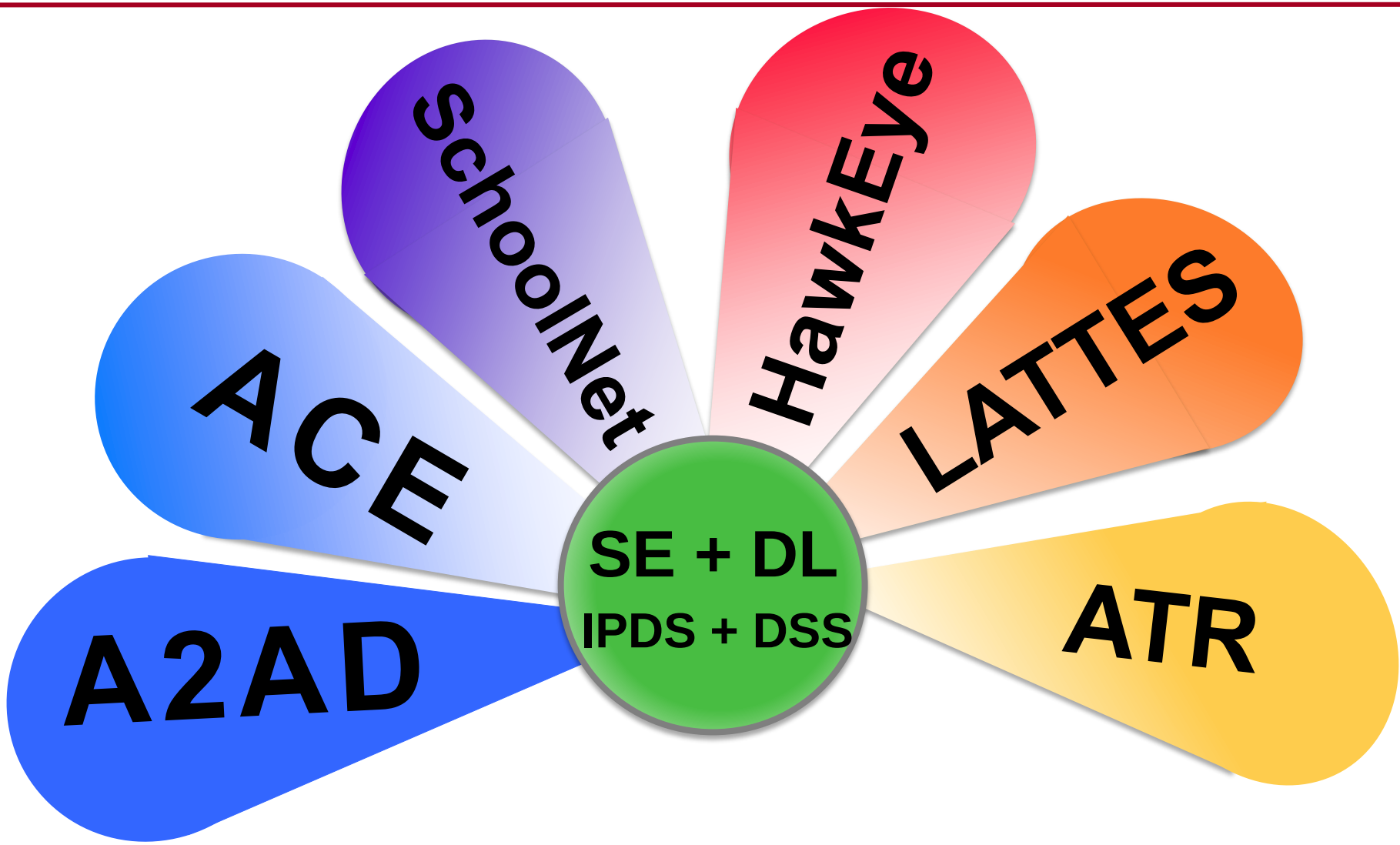
Earlier research provides a conceptual framework to develop intelligent systems mostly from the perspective of computer science and electronics engineering, but little research has gone into advancing systems engineering to cope with this new kind of systems development.

This research fills a gap in the field of convolutional neural networks by adding a purely temporal dimension to the inputs via a system dynamics model as opposed to a spatio-temporal dimension as it is currently the state of the art.

Validation

Validation is accomplished by the creation of a test prototype and demonstrating its ability to solve security problems in multiple domains (C-IED, School Protection, Industrial and Commercial Physical Security, Cybersecurity, etc.)

Systems Engineering + Deep Learning
A Powerful Combination



School Security Problem

High predictability = Ease of Automation

Stochastic events = Need for A.I.

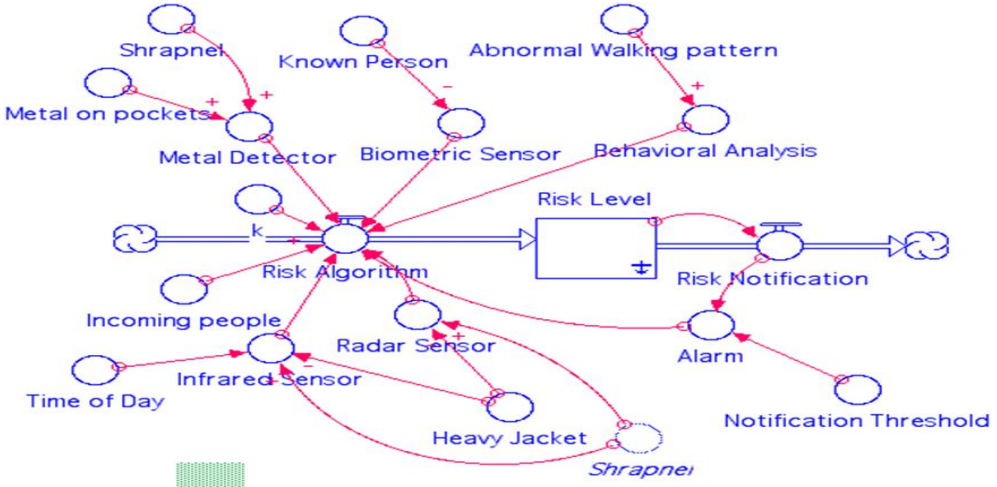
Humans: best at rapid grasp of situations + intuition

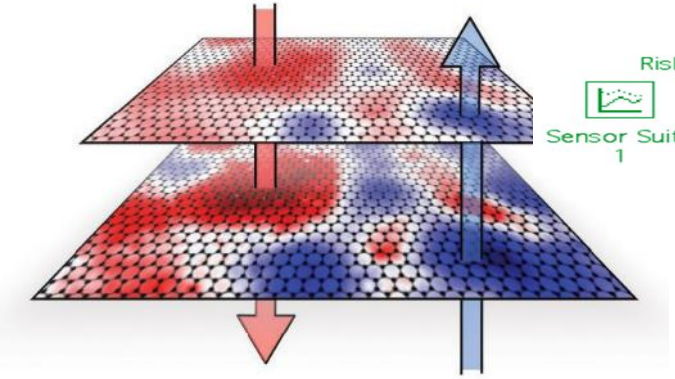
Robots: tireless execution of the same tasks with no loss of attention

Research Scope

Aspects that are part of the problem scope:

- System obsolescence
- Trustworthy systems
- Data fusion
- Systems architecture
- Spoofing prevention

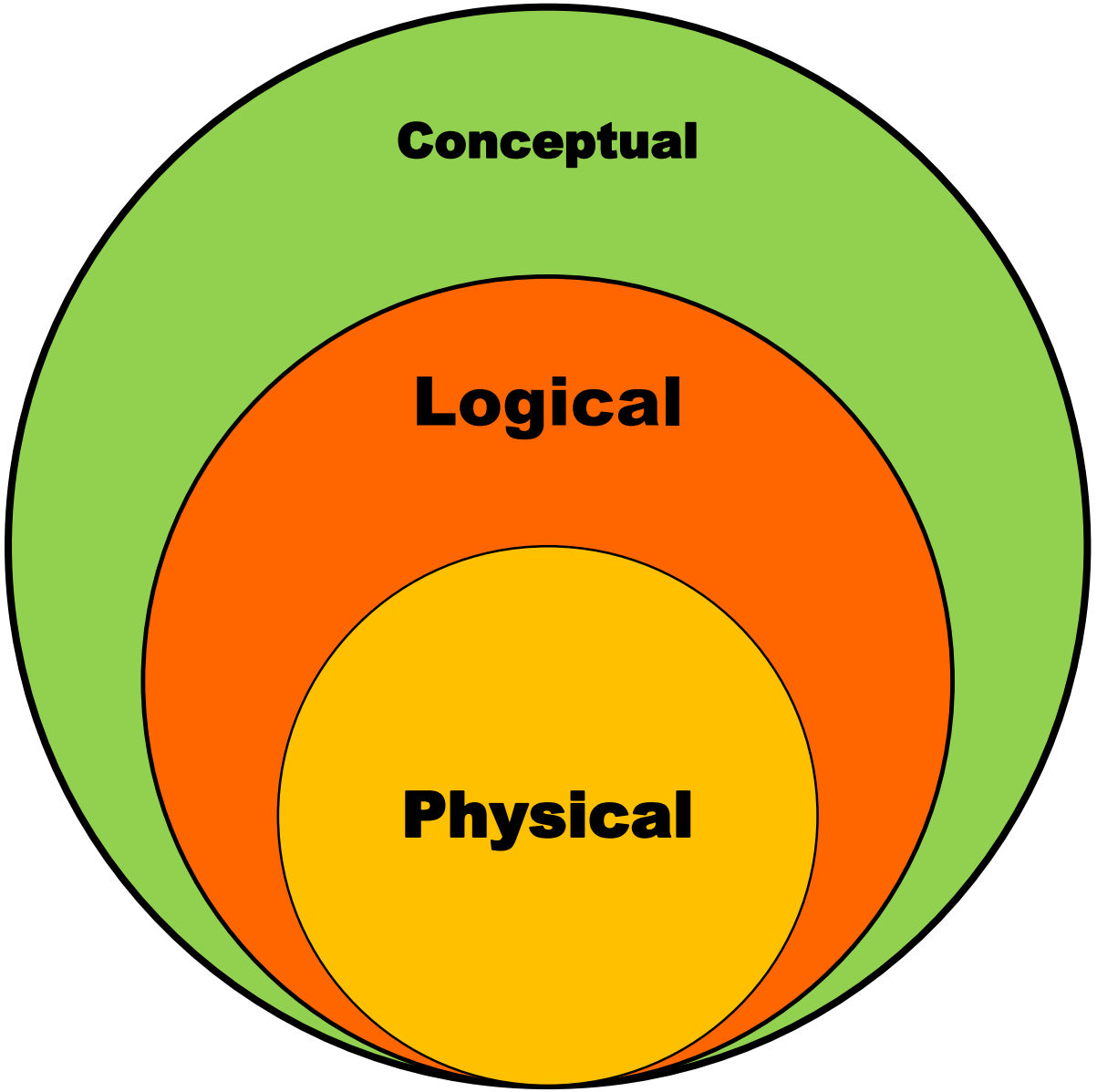




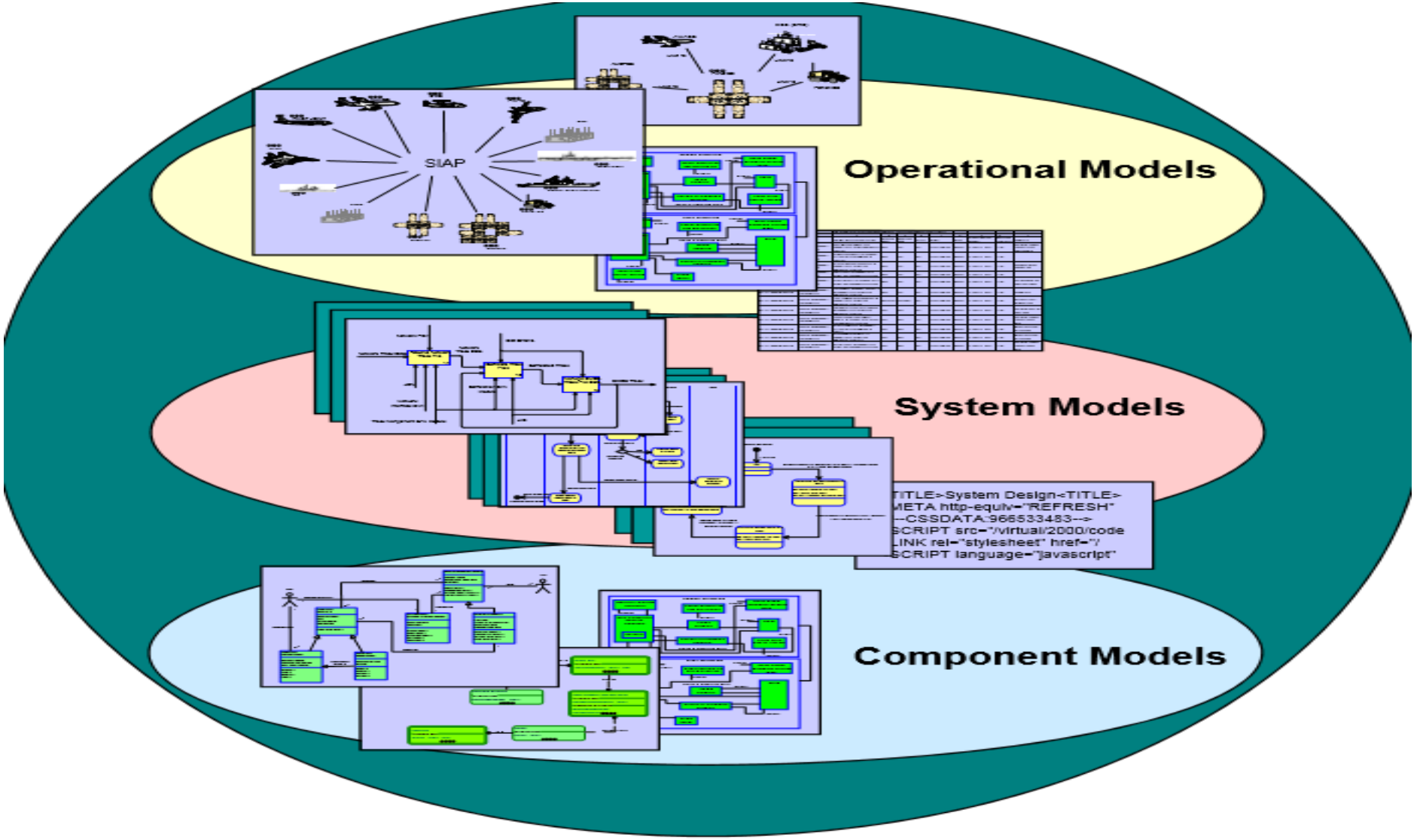
SYSTEMS ENGINEERING RESEARCH CENTER

Levels of Abstraction

RDECOM ARDEC



Architectural Concept



** Ref. Digital Engineering Strategy, OSD June 2018*

SYSTEMS ENGINEERING RESEARCH CENTER

Concept of Operations

RDECOM ARDEC

SYSTEMS ENGINEERING RESEARCH CENTER

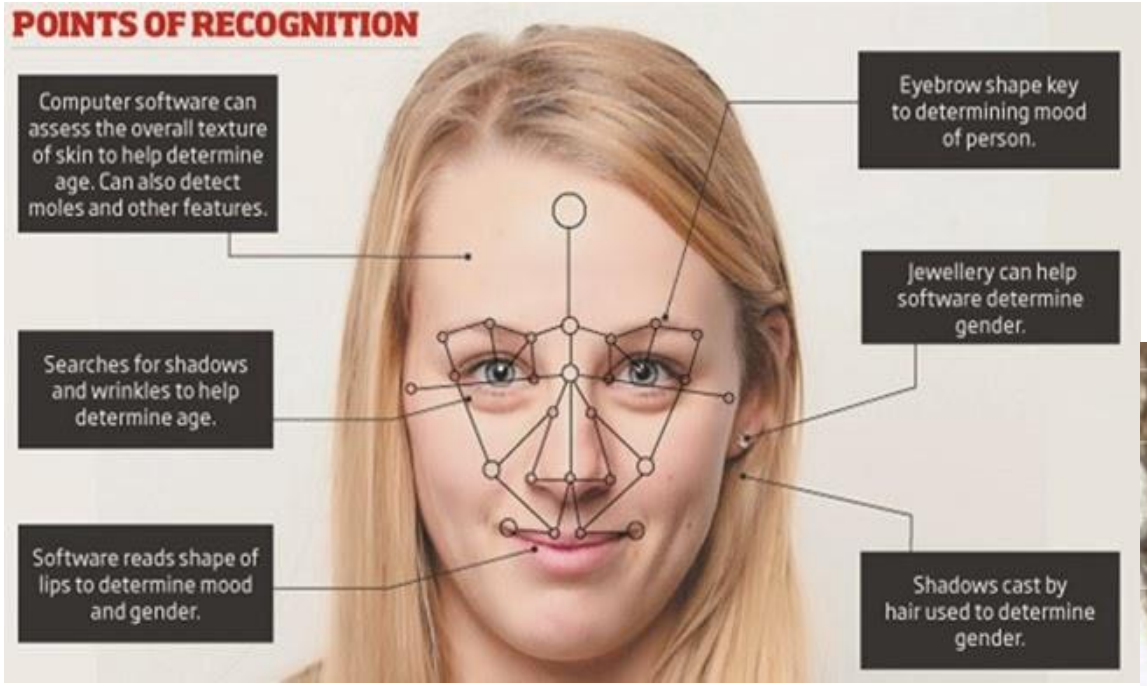
Methodology

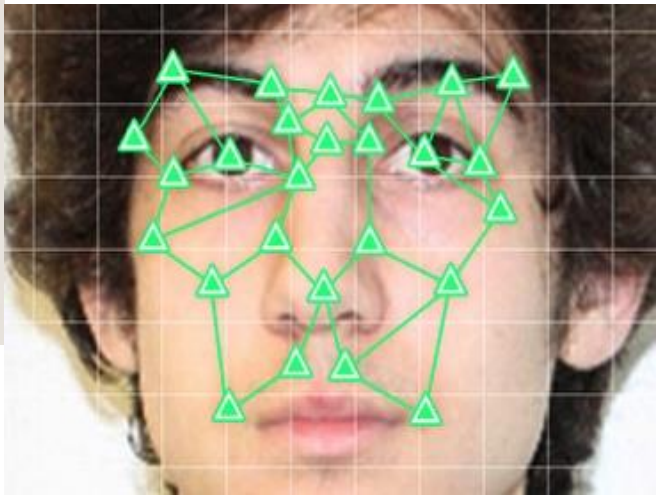
RDECOM ARDEC

- Application of computer vision in the visible, thermal and radar energy bands to find weapons, even concealed.
- Application of transfer learning to convolutional neural networks to recognize desired categories of contraband.
- Exploration of multiple architecture frameworks to determine which one is more likely to provide more compatibility with other systems, modularity, flexibility, and scalability.
- Data fusion of dissimilar sensor technologies.
- Separation of concerns between sensor management and decision support system.

Facial Recognition

Facial recognition software could also be used to identify people in black lists who are not allowed to be in the surveillance area and to identify known personnel such as guards and other support staff.

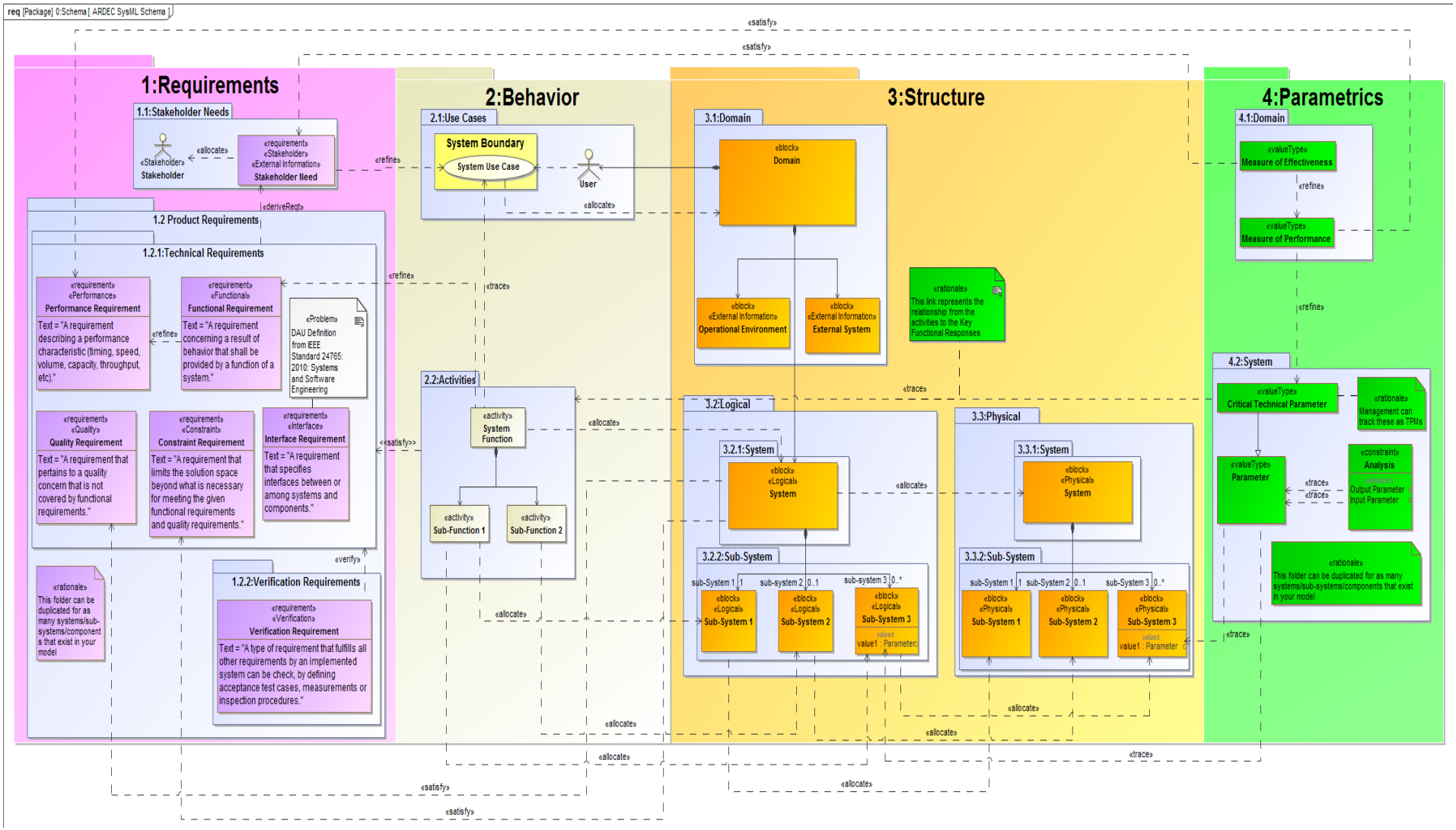




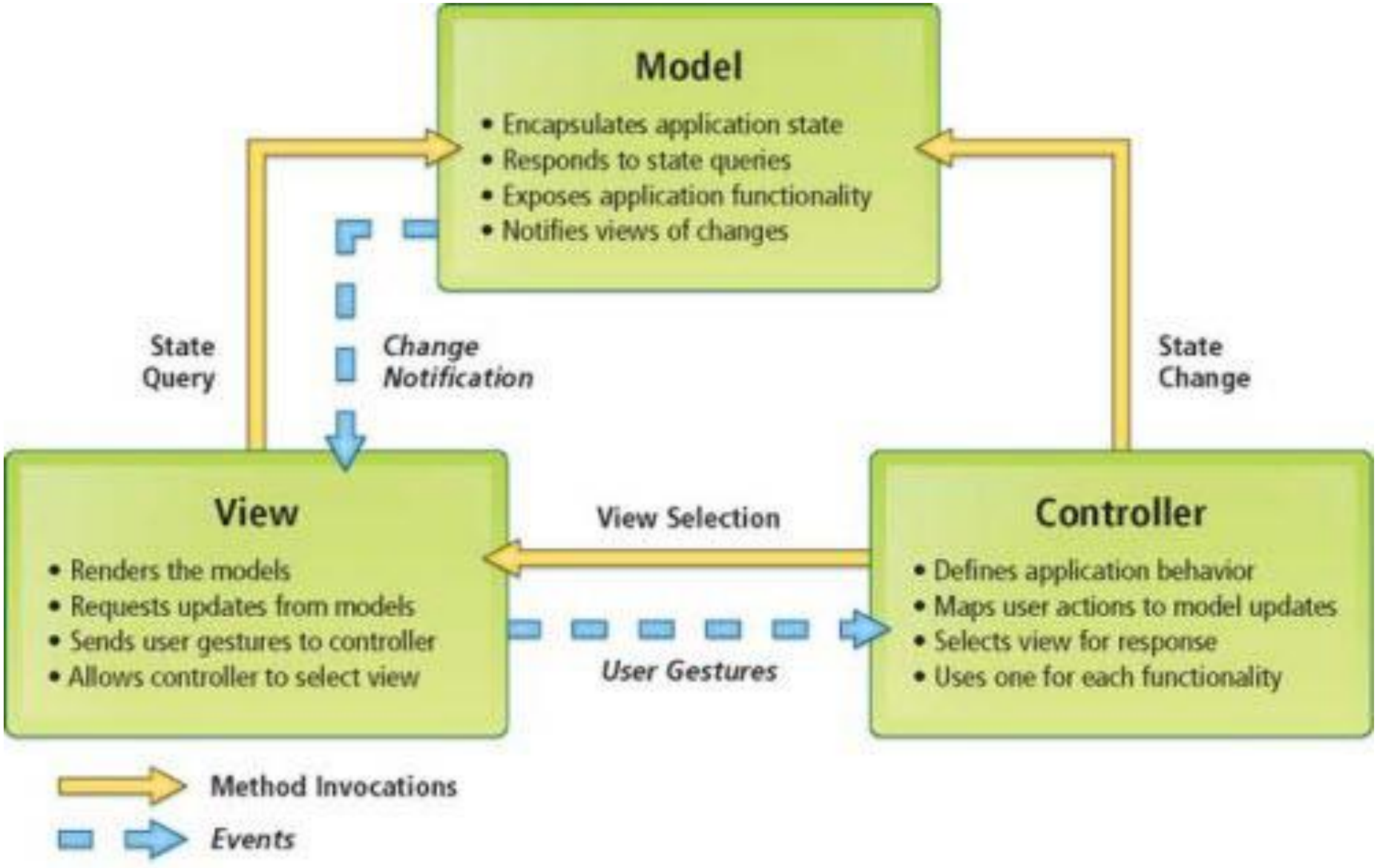
SYSTEMS ENGINEERING RESEARCH CENTER

Architectural Schema

RDECOM ARDEC

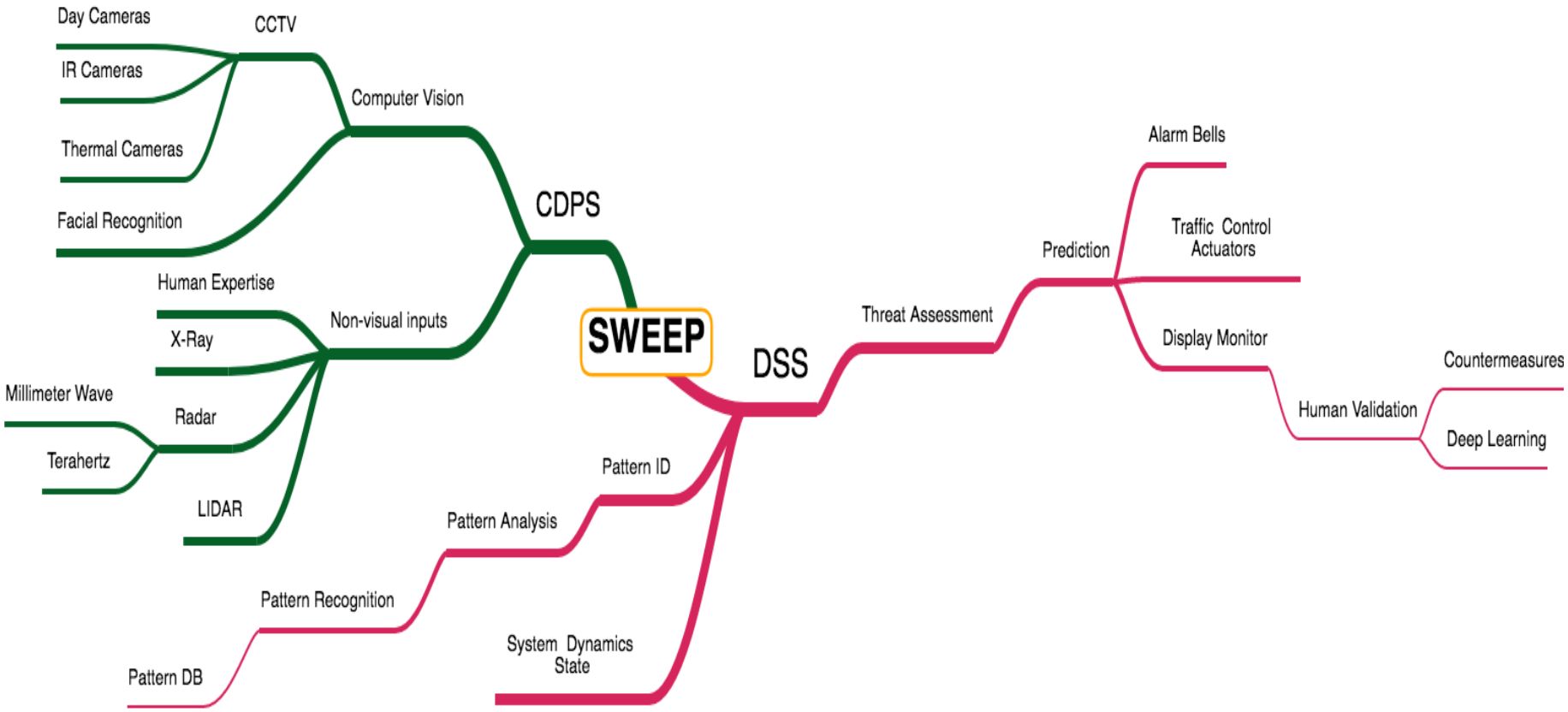


SE Design Patterns

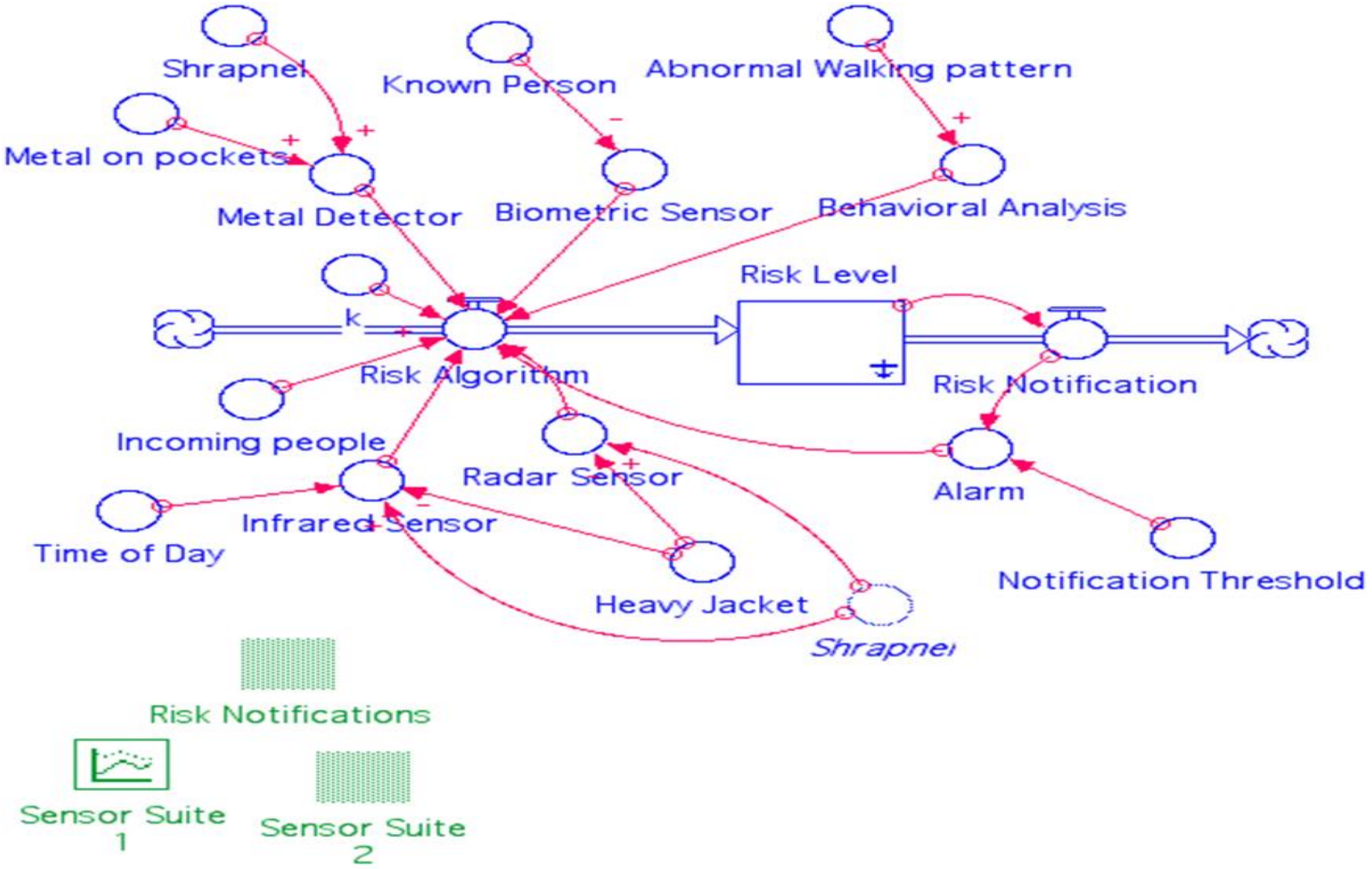


Architecture

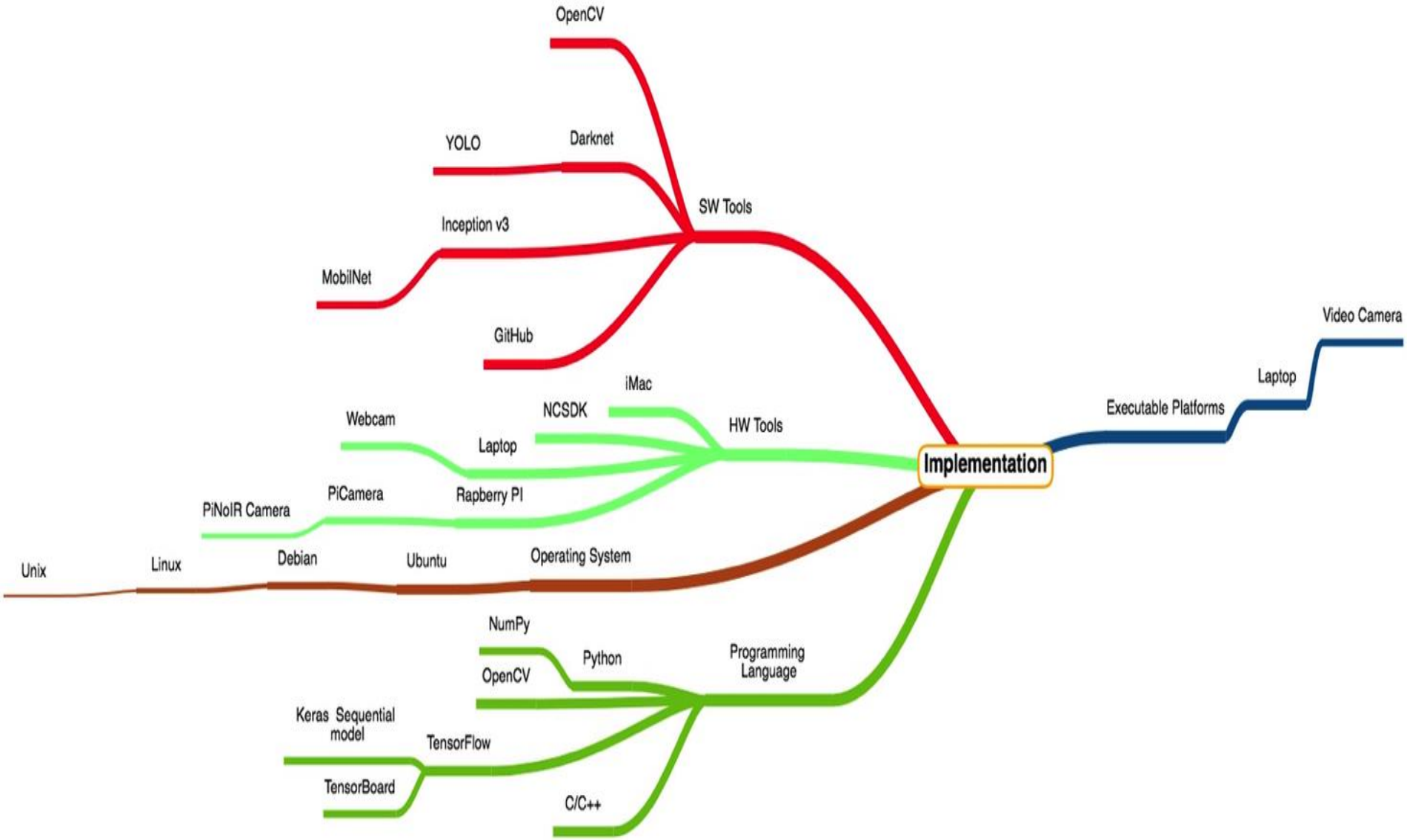
SWEEP: School Weapon Entry Elimination Program.



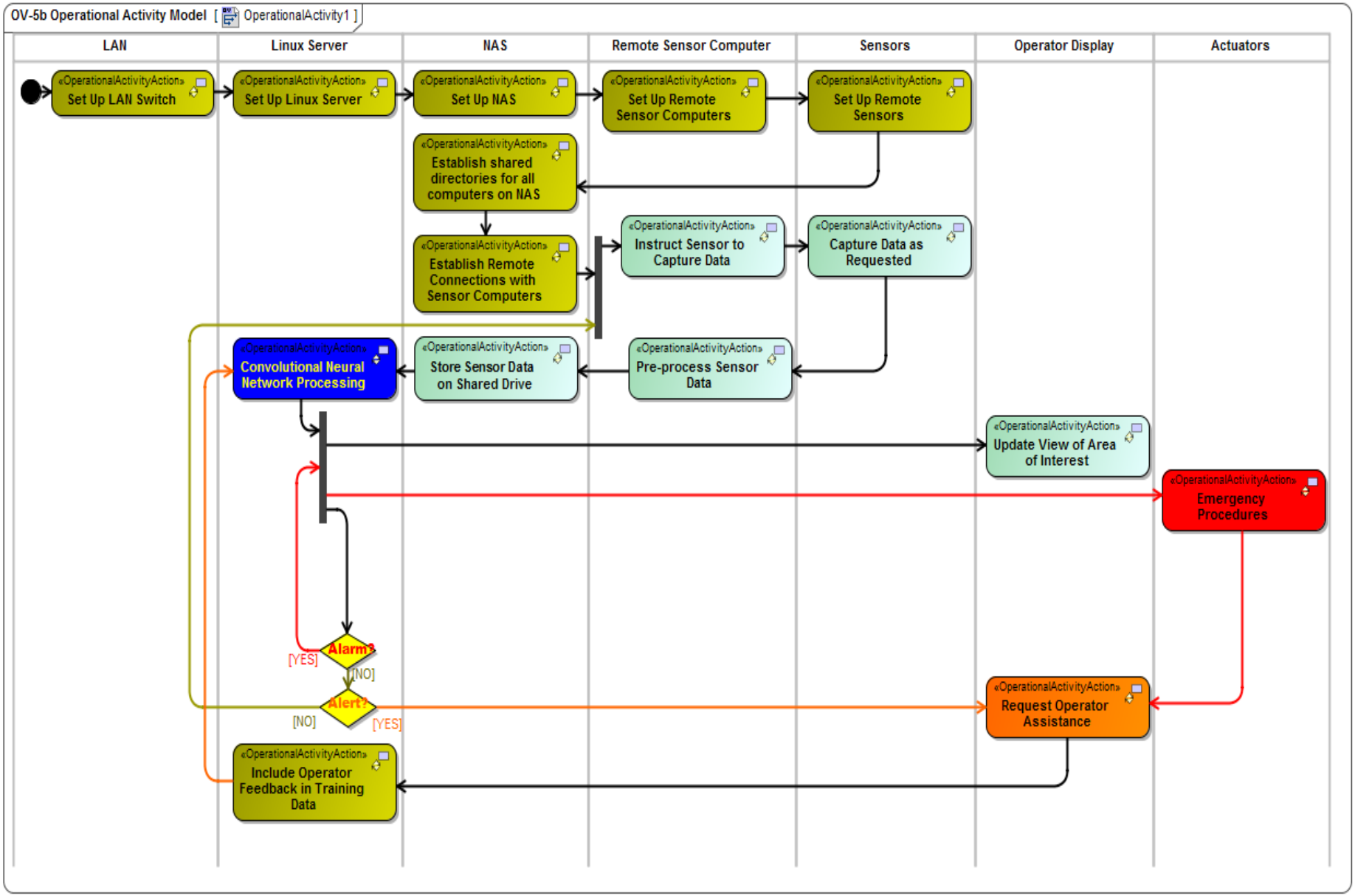
System Dynamics + NN



Prototype Implementation



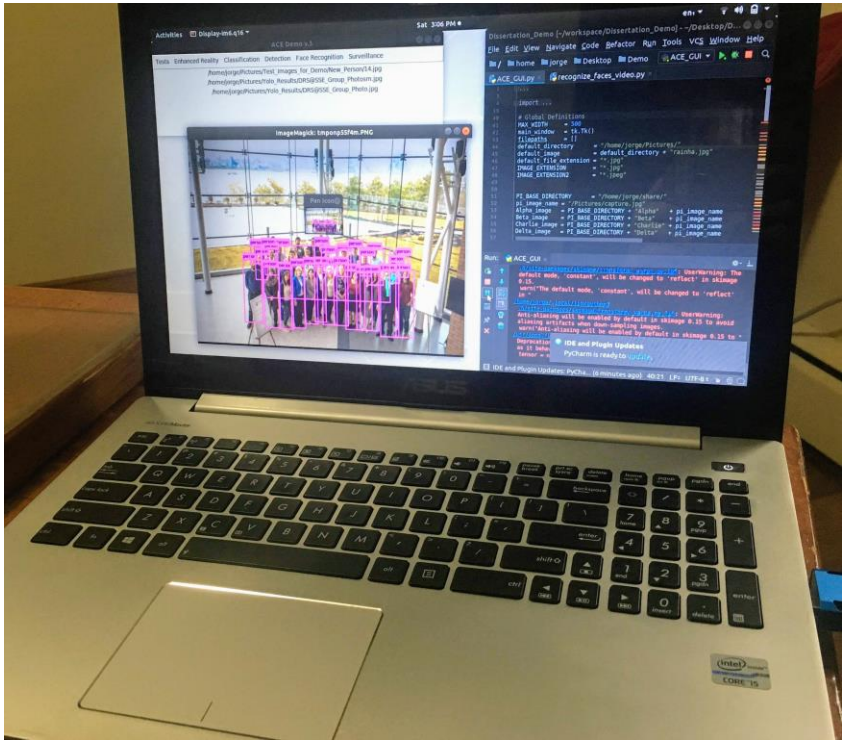
Sequence of Operations



SYSTEMS ENGINEERING RESEARCH CENTER

Validation Prototype

RDECOM ARDEC



Validation Goals

- ✓ Ability to train a convolutional neural network with ~100 training images for each category it needs to recognize.
- ✓ High precision with low rate of false positives for recognition of contraband under different light conditions, picture size, and angle of view.
- ✓ Ability to recognize faces with ~10 training images per person.
- ✓ High precision with low rate of false positives for facial recognition from inexpensive videocameras at distances of over 20 ft.
- ✓ Ability to merge multiple wireless sensor feeds (4) onto a single monitor screen with near real-time image recognition.
- ✓ Ability to maintain secure encrypted communications between sensors and server.

SYSTEMS ENGINEERING RESEARCH CENTER

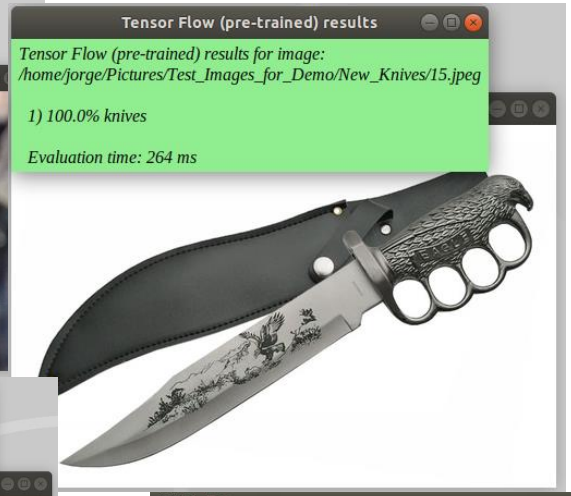
Anti-spoofing

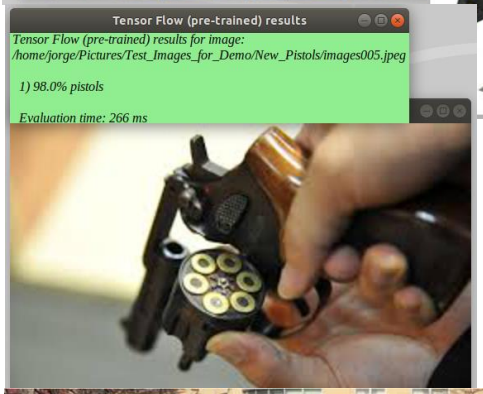
RDECOM ARDEC

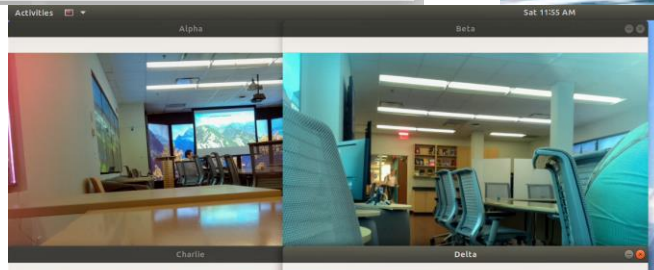
SYSTEMS ENGINEERING RESEARCH CENTER

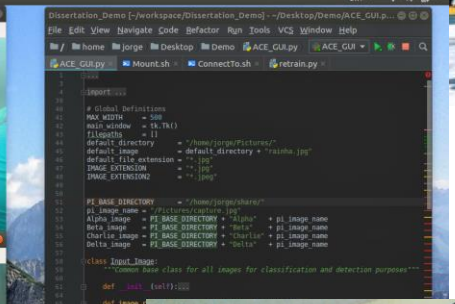
Test Examples

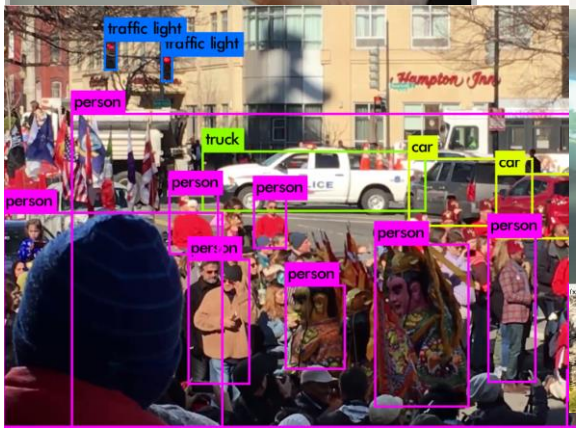
RDECOM ARDEC

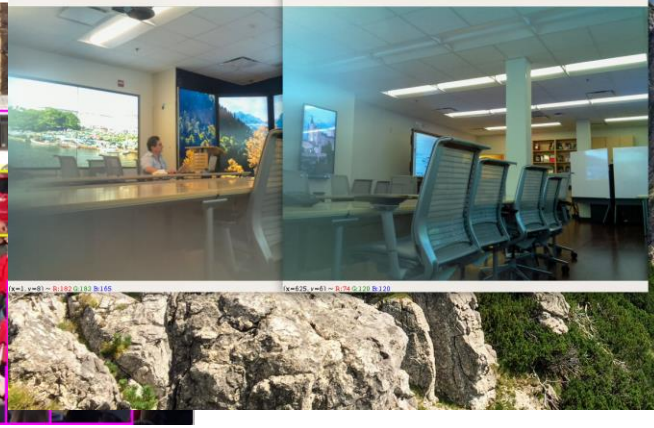


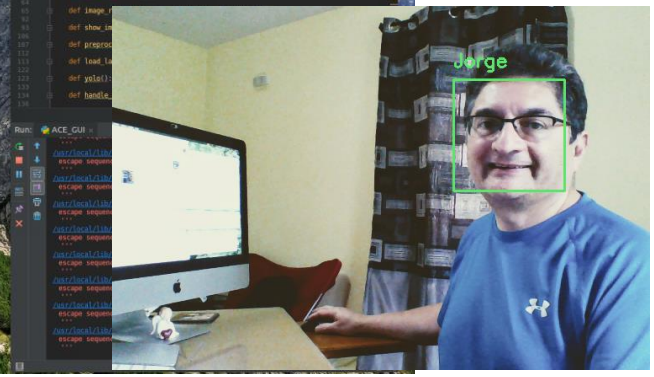




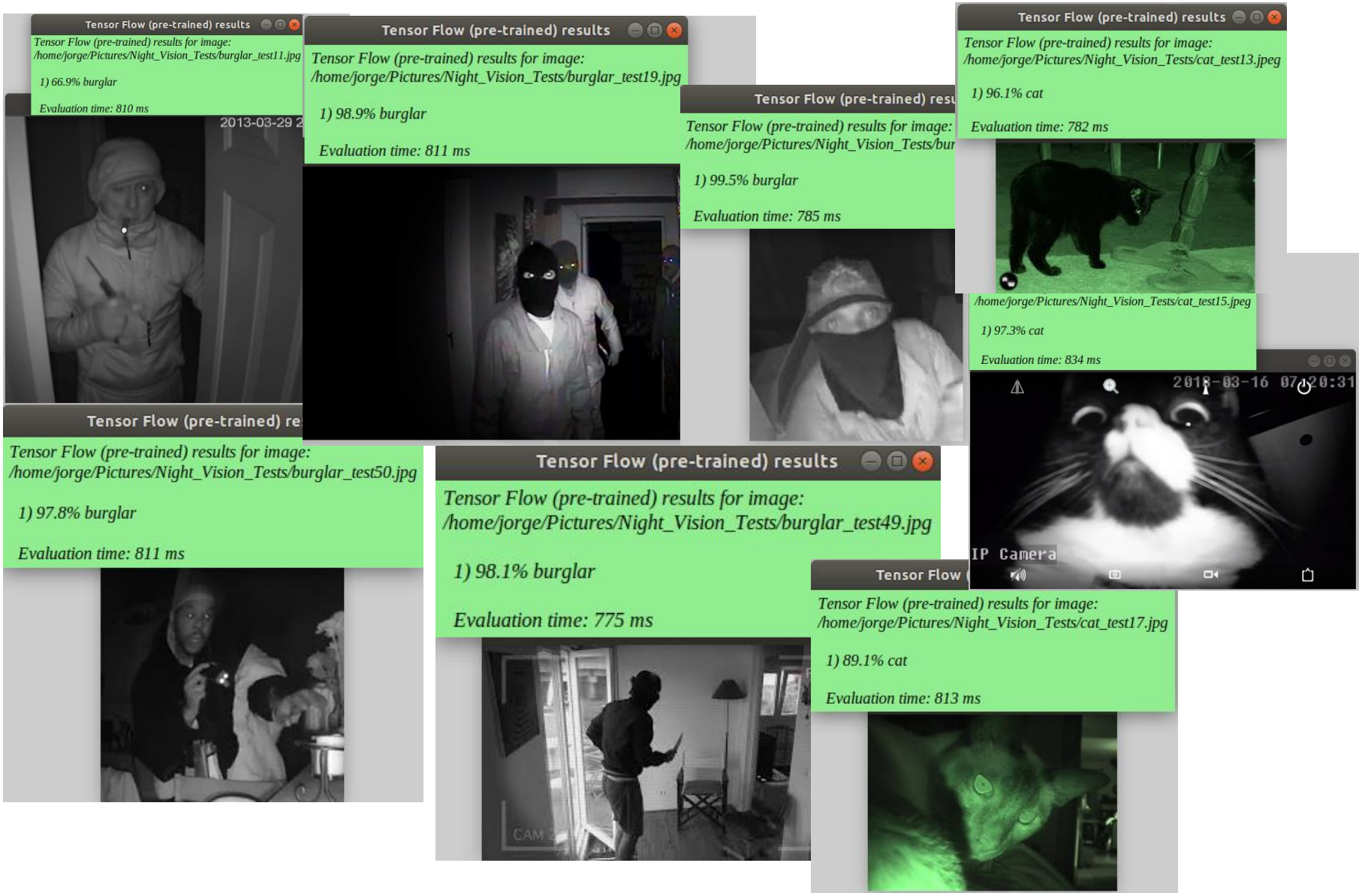








Night Vision Test Examples



Metrics

Precision

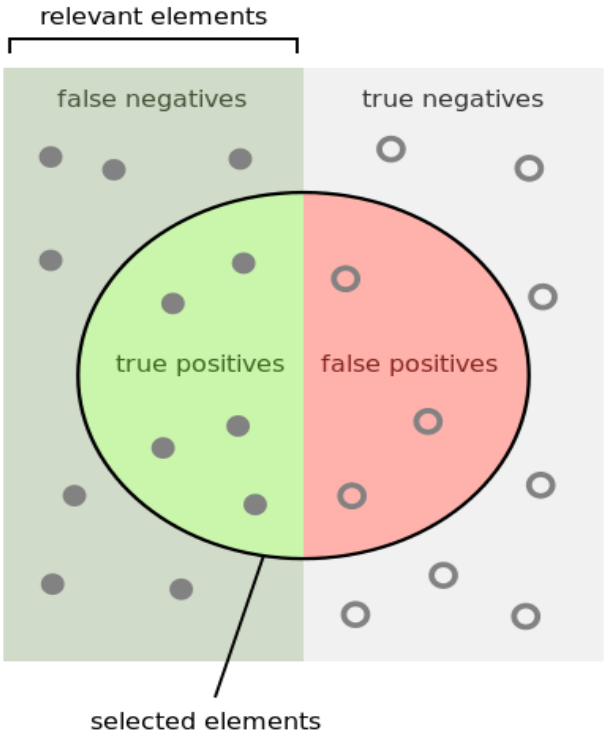
$$\frac{TP}{TP+FP}$$

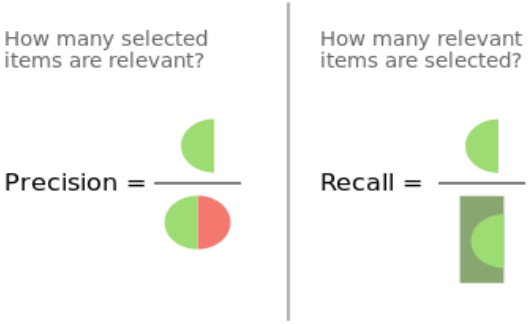
Recall

$$\frac{\mathrm{TP}}{\mathrm{TP+FN}}$$

F1 Score

$$\frac{2}{\frac{1}{Recall}+\frac{1}{Precision}}$$





SYSTEMS ENGINEERING RESEARCH CENTER

Validation Results

RDECOM ARDEC

		People	Knives	Pistols	Rifles	Bullets	Generic	Avg.
GoogLeNet p2	Top-1 Precision	100%	100%	100%	100%	100%	18%	86%
	Top-1 Recall	6%	22%	74%	86%	8%	18%	36%
	Top-1 F1	11%	36%	85%	92%	15%	18%	43%
	Top-1 Accuracy	53%	61%	87%	93%	55%	18%	61%
	Top-5 Precision	100%	100%	100%	100%	100%	41%	90%
	Top-5 Recall	24%	64%	98%	98%	38%	41%	61%
	Top-5 F1	39%	78%	99%	99%	55%	41%	69%
	Top-5 Accuracy	62%	83%	99%	99%	69%	41%	75%
SafetyNet 2	Top-1 Precision	98%	100%	100%	100%	91%	100%	98%
	Top-1 Recall	100%	98%	88%	90%	98%	94%	95%
	Top-1 F1	99%	99%	93%	95%	94%	97%	96%
	Top-1 Accuracy	99%	99%	94%	95%	94%	91%	95%
SafetyNet 3	Top-1 Precision	100%	100%	100%	100%	92%	100%	99%
	Top-1 Recall	100%	100%	94%	98%	100%	100%	99%
	Top-1 F1	100%	100%	97%	99%	98%	100%	99%
	Top-1 Accuracy	100%	100%	97%	99%	99%	100%	99%

SYSTEMS ENGINEERING RESEARCH CENTER

Validation Achievements

RDECOM ARDEC

- ✓Ability to react to a specified set of conditions and take immediate action.
- ✓Graphical user interface to show the security guard the situation in the area of observation from multiple cameras on the same screen.
- ✓Ability to request human assistance to resolve alerts and alarms.
- ✓Ability to run multiple convolutional neural networks and compare results to use a voting system to determine the most likely assessment of the presence of contraband.
- ✓Ability to recognize contraband, people, and different kinds of animal in near total darkness using IR illuminators.

SYSTEMS ENGINEERING RESEARCH CENTER

Contributions

RDECOM ARDEC

- ✓Man/Unmanned Team procedures that direct tasks to the best performer.
- ✓Solutions to systems engineering challenges to architect and design an inference engine with high performance, low cost, and rapid development.
- ✓Temporal context to neural network predictions
- ✓Leveraging supervised machine learning to delay system obsolescence

Conclusion

The statistical significance of demonstrating the capabilities of system core functionalities general enough to be instantiated into several different applications with minor changes equates to a general systems engineering framework to leverage artificial intelligence to rapidly create solutions to complex security challenges.

This research fills a gap in the discipline of systems engineering to leverage deep learning, in particular convolutional neural networks to solve problems that need to be solved to create affordable, scalable, safe systems in the shorter developing schedules demanded by the Government and Industry.

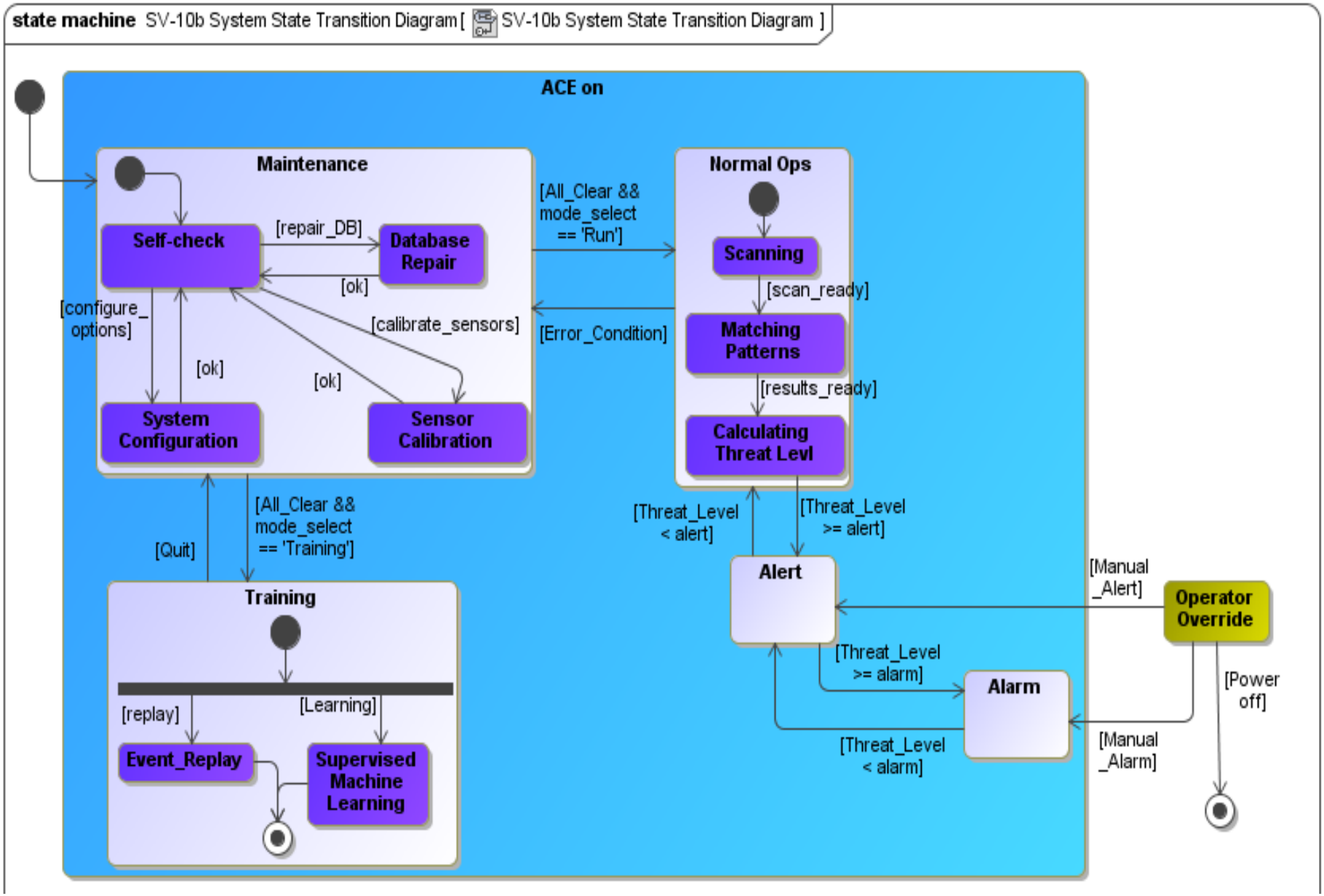

QUESTIONS
why
challenge
asking questions
who?
where?
how?
what?
clues
ask
who?
discover
knowing
how
investigation

APPENDIX

SYSTEMS ENGINEERING RESEARCH CENTER

System State Diagram

RDECOM ARDEC



SYSTEMS ENGINEERING RESEARCH CENTER

Technology Readiness

RDECOM ARDEC

TRL	Definition	Description	Supporting Information
1	Basic principles observed and reported	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development (R&D). Examples might include paper studies of a technology's basic properties.	Published research that identifies the principles that underlie this technology. References to who, where, when.
2	Technology concept and/or application formulated	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.	Publications or other references that outline the application being considered and that provide analysis to support the concept.
3	Analytical and experimental critical function and/or characteristic proof of concept	Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.	Results of laboratory tests performed to measure parameters of interest and comparison to analytical predictions for critical subsystems. References to who, where, and when these tests and comparisons were performed.
4	Component and/or breadboard validation in laboratory environment	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared with the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.	System concepts that have been considered and results from testing laboratory-scale breadboard(s). Reference to who did this work and when. Provide an estimate of how breadboard hardware and test results differ from the expected system goals.
5	Component and/or breadboard validation in relevant environment	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so they can be tested in a simulated environment. Examples include "high-fidelity" laboratory integration of components.	Results from testing laboratory breadboard system are integrated with other supporting elements in a simulated operational environment. How does the "relevant environment" differ from the expected operational environment? How do the test results compare with expectations? What problems, if any, were encountered? Was the breadboard system refined to more nearly match the expected system goals?
6	System/subsystem model or prototype demonstration in a relevant environment	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment.	Results from a laboratory testing of a prototype system that is near the desired configuration in terms of performance, weight, and volume. How did the test environment differ from the operational environment? Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
7	System prototype demonstration in an operational environment	Prototype near or at planned operational system. Represents a major step up from TRL 6 by requiring demonstration of an actual system prototype in an operational environment (e.g., in an aircraft, in a vehicle, or in space).	Results from testing a prototype system in an operational environment. Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
8	Actual system completed and qualified through test and demonstration	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation (DT&E) of the system in its intended weapon system to determine if it meets design specification.	Results of testing the system in its final configuration under the expected range of environmental conditions in which it will be expected to operate. Assessment of whether it will meet its operational requirements. What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before finalizing the design?
9	Actual system proven through successful mission operations	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation (OT&E). Examples include using the system under operational mission conditions.	OT&E reports.