Change is Coming… HERE

Evolving Systems Engineering Methods for Artificial Intelligence and Machine Learning

Rosa R. Heckle, PhD

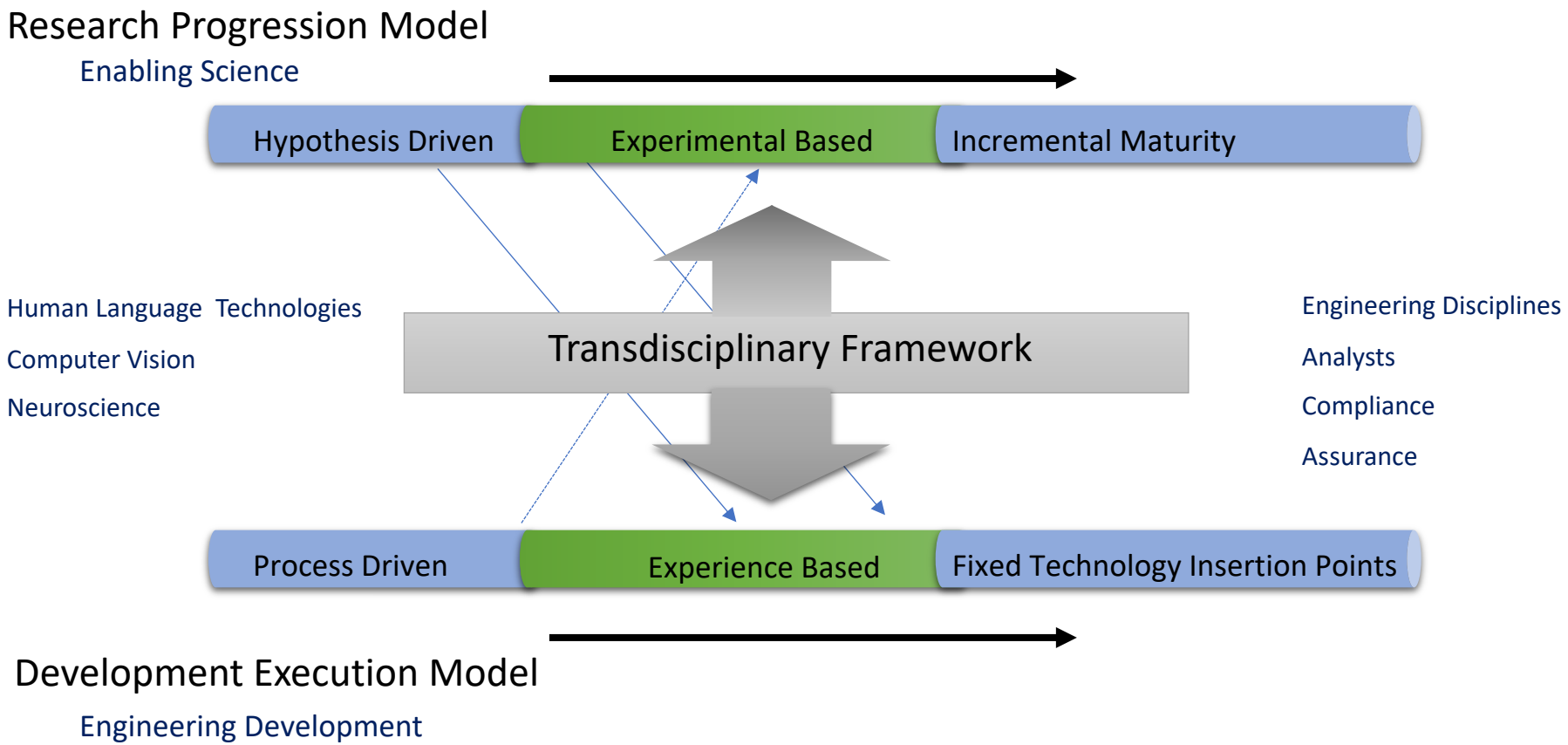
Stuart D. Harshbarger

October 29, 2020

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™

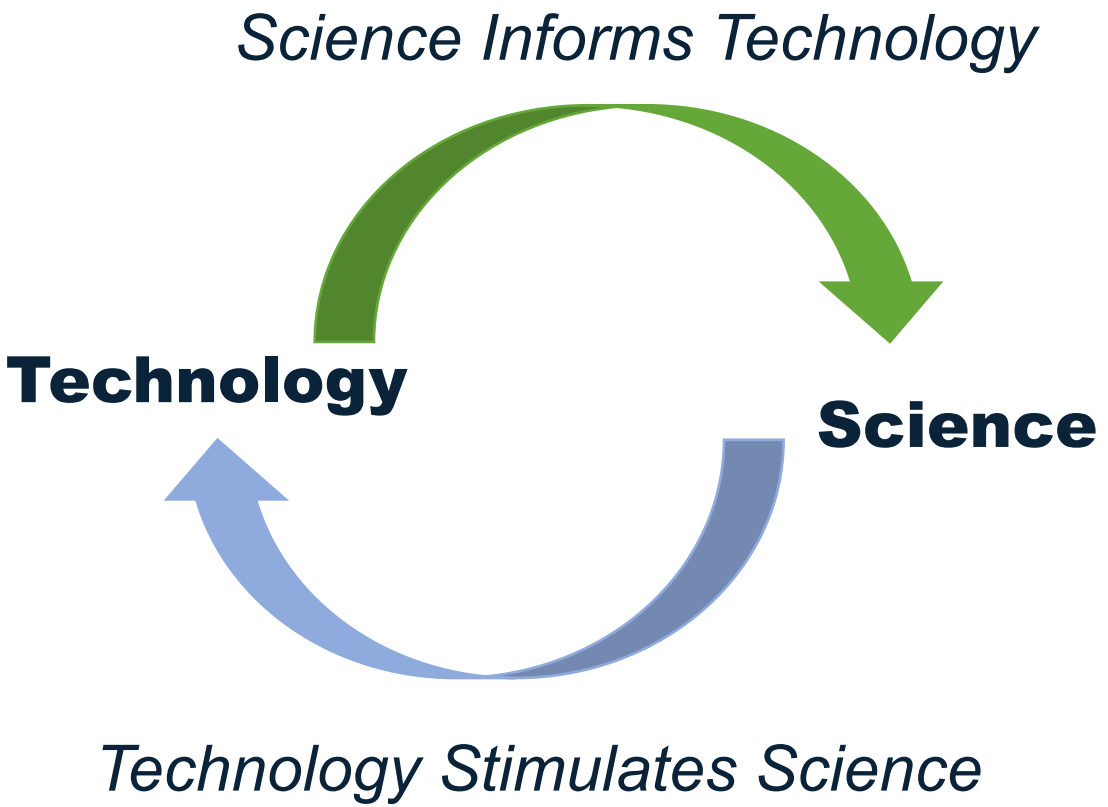
Approved for Public Release; Distribution Unlimited. Public Release Case Number 20-2639

Research Progression & Development Execution Differ



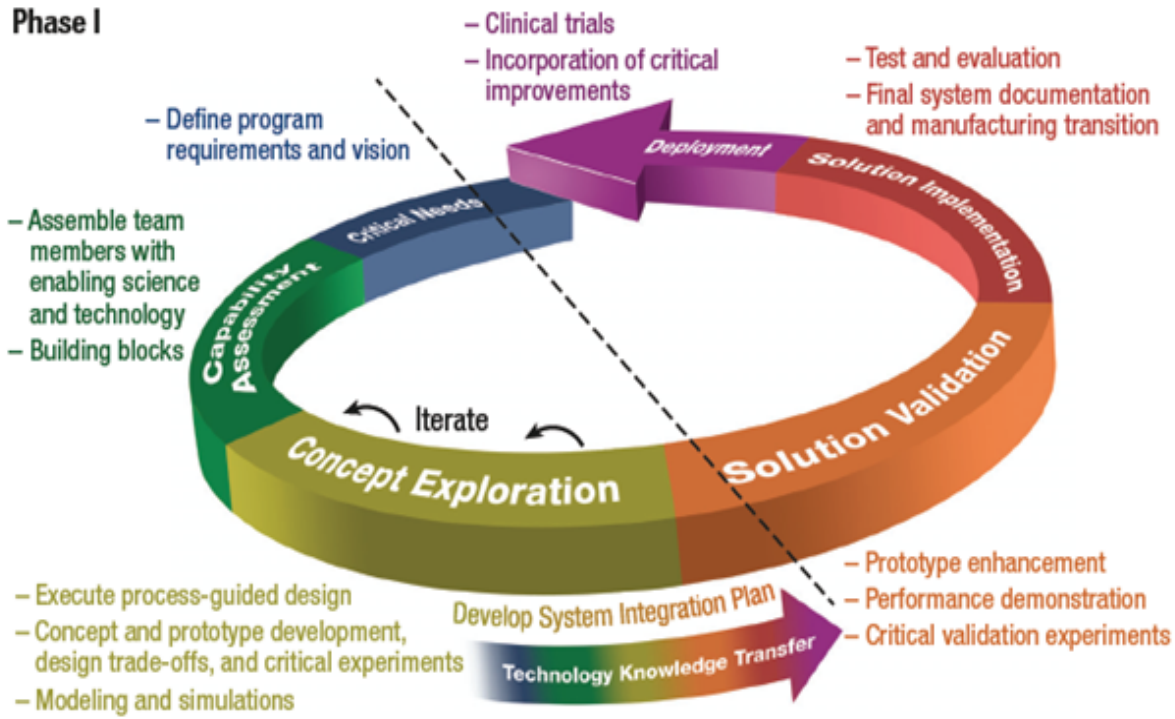
Building AI/ML systems requires a convergence of two fairly distinct approaches.

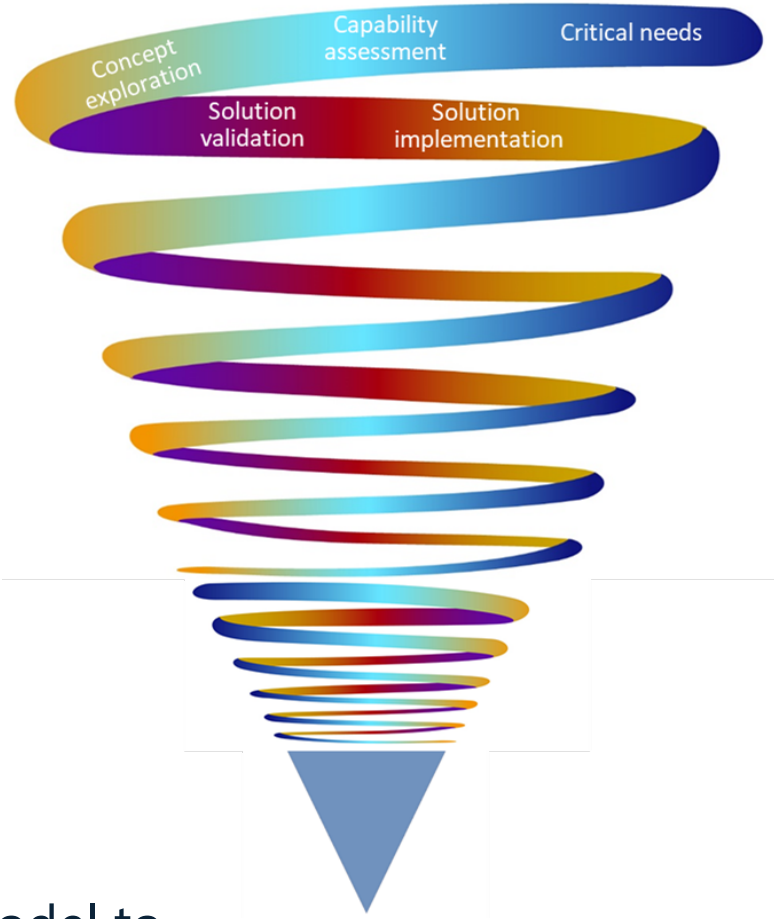
Need For Transdisciplinarity



Polanyi's Relationship Between Science and Technology

Vortical Development Model Concept





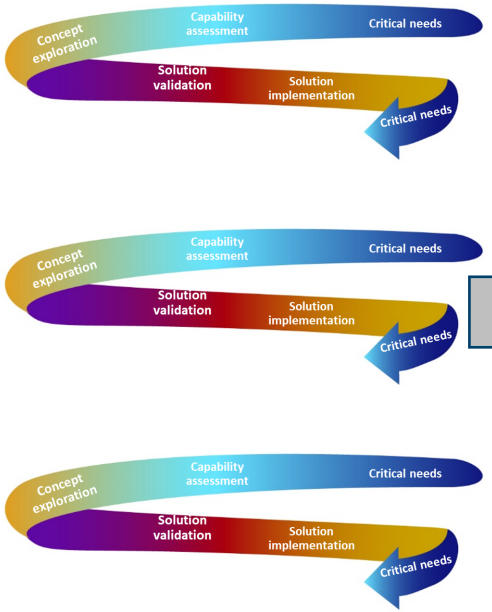
1. J. Burck, J. Bigelow, S. Harshbarger, "Systems Engineering Approach for Next Generation Prosthetic Limb", Johns Hopkins University Applied Physics Laboratory, Technical Digest, Vol 30, Special Edition – Revolutionizing Prosthetics, 2011

Vortical model evolves the traditional spiral development model to reflect the tightening of corresponding spirals as the model refinement/ progression continues.

Vortical Development Model Concept for Machine-Learning Systems

Major Discrete Building Blocks

Baseline system components at varying levels of maturity.



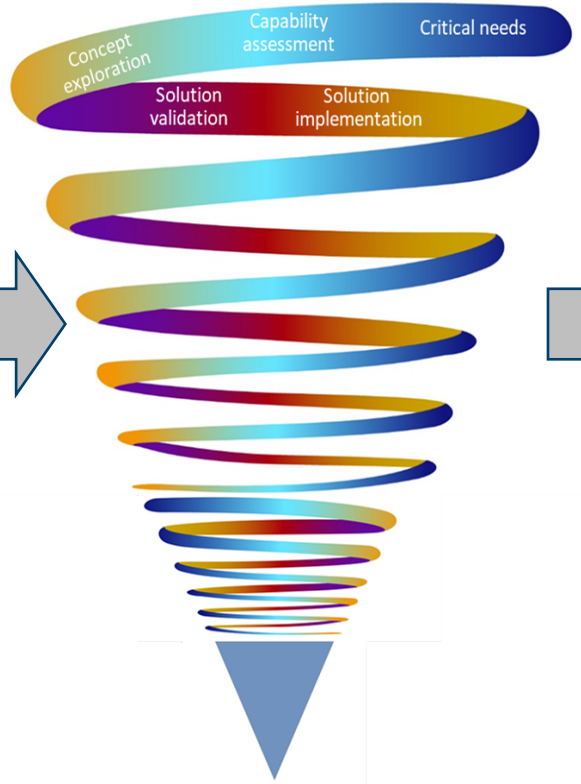
Coordinated spiral development of enabling technologies

Agile Incremental integration

Integration

Ensures risk reduction and allows for demonstration and design evaluation

Iterative Design Revision



Incorporates lessons learned while managing impact to linked components

Fabrication & Test of Final System

Increasing Component Maturity

An Example - Start with the End in Mind

What Does This Document Image Say?

Living with Insecurity

Security Dilemma: Healthcare Clinicians at Work

While healthcare organizations strive to increase control of network access, clinicians need unencumbered access to data. Clinicians make unconscious decisions daily to comply with security measures or to live with a certain level of insecurity to get their job done.

ROSA R. HECKLE
MITRE

In a crowded conference room, a group of system engineers, hospital clinicians, and various staff sat intently listening to a team of vendors extol the virtues of their single sign-on (SSO) technology. Each vendor promised to deliver an authentication system that would improve usability for multiple system users, increase compliance with policies and government mandates, and help curb maintenance costs. From a technical perspective, the technology was a good fit for the infrastructure and the purpose at hand. From a management perspective, it fit the security requirements and organizational policies.

However, the clinicians weren't so sure. They were reflecting on the last implementation to enhance security: an electronic medication administration record (MAR) system that used bar coding. Each hospital patient received a bar-coded identification bracelet. When administering medications, the protocol was for nurses to scan a patient's bracelet and then scan the medication being administered. However, on occasion, nurses had problems scanning the bracelet or the medication label. As a workaround, the nurses placed a copy of the patient's bar code on their clipboard. In tight times or when they [illegible] bracelet, they simply scanned [illegible] rather than [illegible] without the [illegible] mechanism. [illegible] poses wasting [illegible] apparent [illegible] structure, many [illegible] in other [illegible] culture, and critical work [illegible] individual accountability crucial. Although technology has become an important piece of a clinician's toolset, it's not the focus of his or her mindset. This is particularly true for security systems. Though the Health Insurance Portability and Accountability Act (HIPAA) mandates strict data security, a patient's well-being might depend on quick and easy access to information.[3] Clinicians understand the importance of security, but it plays second string to convenience. On a daily basis, they decide between doing what is necessary to comply with a security measure or living with a certain level of insecurity to get the job done. The unanticipated consequences of these decisions can lead to suboptimal outcomes.

To address this issue, some research strongly recommends taking a holistic sociotechnical perspective in security system design.[4] This is not a new idea, but exactly what does it mean?

A 15-month ethnographic field study I conducted of an SSO system implementation at a regional hospital sheds some light on the issue. Although my study focused on developing a deeper understanding of the technical design and implementation issues of an SSO mechanism, it also provided a firsthand view of how modern healthcare work is performed in an environment in which the clinicians must navigate between adhering to security protocols and quick accessibility.

Network-Level Authentication

Recent government regulations are pressuring healthcare organizations to increase IT usage and governance

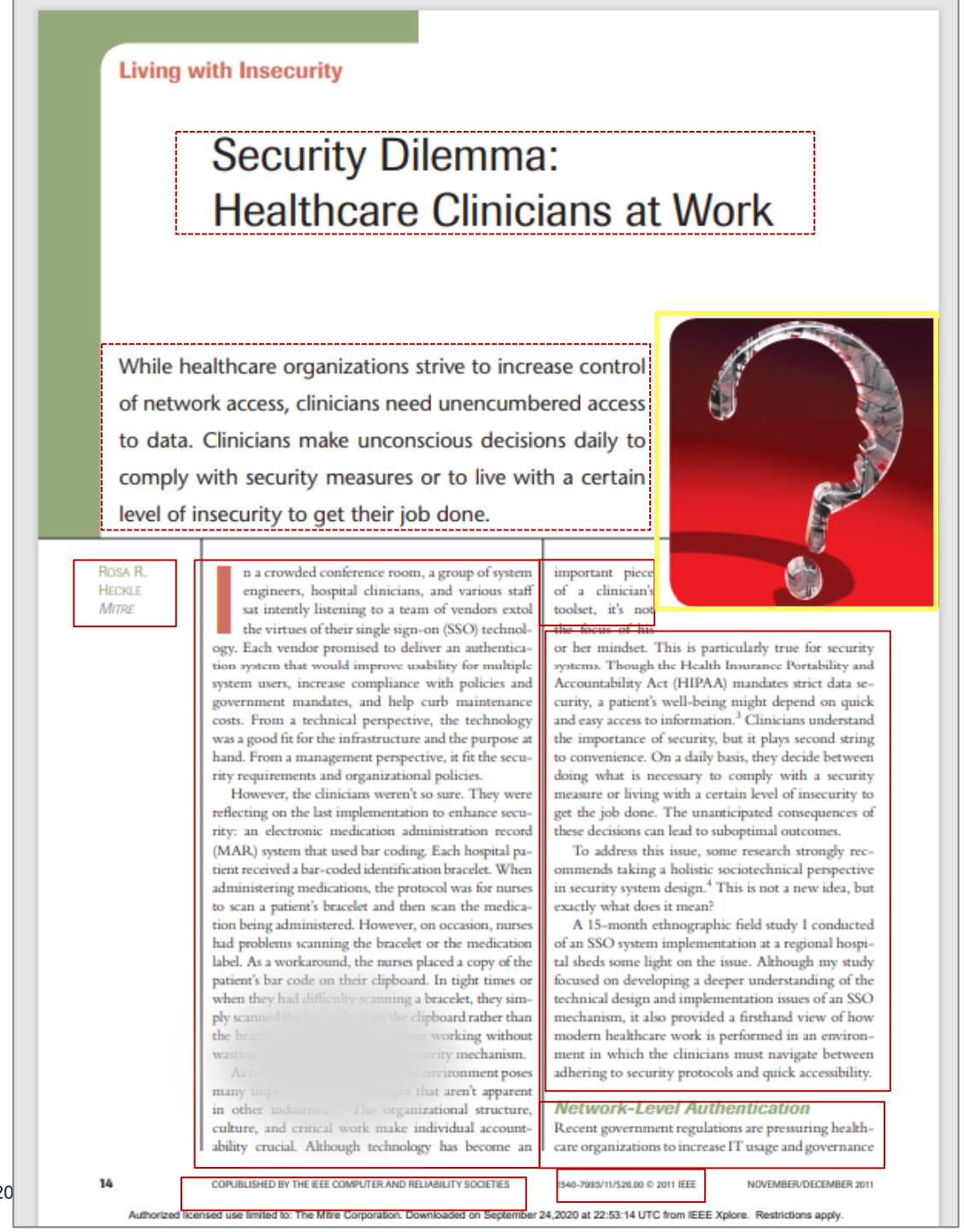
COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES 1540-7993/11/$26.00 © 2011 IEEE

Computer Vision

1. Adjust document rendering
2. Identify areas that need cleaning
3. Language = English
4. Identify layout (sentences, paragraphs, headings, footings, etc.)
5. Identify text only
6. Extract text characters

HLT

1. Read text – extract entities (people, places, things of interest).



Living with Insecurity

Security Dilemma: Healthcare Clinicians at Work

While healthcare organizations strive to increase control of network access, clinicians need unencumbered access to data. Clinicians make unconscious decisions daily to comply with security measures or to live with a certain level of insecurity to get their job done.

ROSA R. HECKLE
MITRE

In a crowded conference room, a group of system engineers, hospital clinicians, and various staff sat intently listening to a team of vendors extol the virtues of their single sign-on (SSO) technology. Each vendor promised to deliver an authentication system that would improve usability for multiple system users, increase compliance with policies and government mandates, and help curb maintenance costs. From a technical perspective, the technology was a good fit for the infrastructure and the purpose at hand. From a management perspective, it fit the security requirements and organizational policies.

However, the clinicians weren't so sure. They were reflecting on the last implementation to enhance security: an electronic medication administration record (MAR) system that used bar coding. Each hospital patient received a bar-coded identification bracelet. When administering medications, the protocol was for nurses to scan a patient's bracelet and then scan the medication being administered. However, on occasion, nurses had problems scanning the bracelet or the medication label. As a workaround, the nurses placed a copy of the patient's bar code on their clipboard. In tight times or when they had difficulty scanning a bracelet, they simply scanned the bar code from the clipboard rather than the bracelet [illegible] working without wasting [illegible] security mechanism.

As th[illegible] environment poses many implementation challenges that aren't apparent in other industries.[1,2] The organizational structure, culture, and critical work make individual accountability crucial. Although technology has become an important piece of a clinician's toolset, it's not the focus of his or her mindset. This is particularly true for security systems. Though the Health Insurance Portability and Accountability Act (HIPAA) mandates strict data security, a patient's well-being might depend on quick and easy access to information.[3] Clinicians understand the importance of security, but it plays second string to convenience. On a daily basis, they decide between doing what is necessary to comply with a security measure or living with a certain level of insecurity to get the job done. The unanticipated consequences of these decisions can lead to suboptimal outcomes.

To address this issue, some research strongly recommends taking a holistic sociotechnical perspective in security system design.[4] This is not a new idea, but exactly what does it mean?

A 15-month ethnographic field study I conducted of an SSO system implementation at a regional hospital sheds some light on the issue. Although my study focused on developing a deeper understanding of the technical design and implementation issues of an SSO mechanism, it also provided a firsthand view of how modern healthcare work is performed in an environment in which the clinicians must navigate between adhering to security protocols and quick accessibility.

Network-Level Authentication

Recent government regulations are pressuring healthcare organizations to increase IT usage and governance

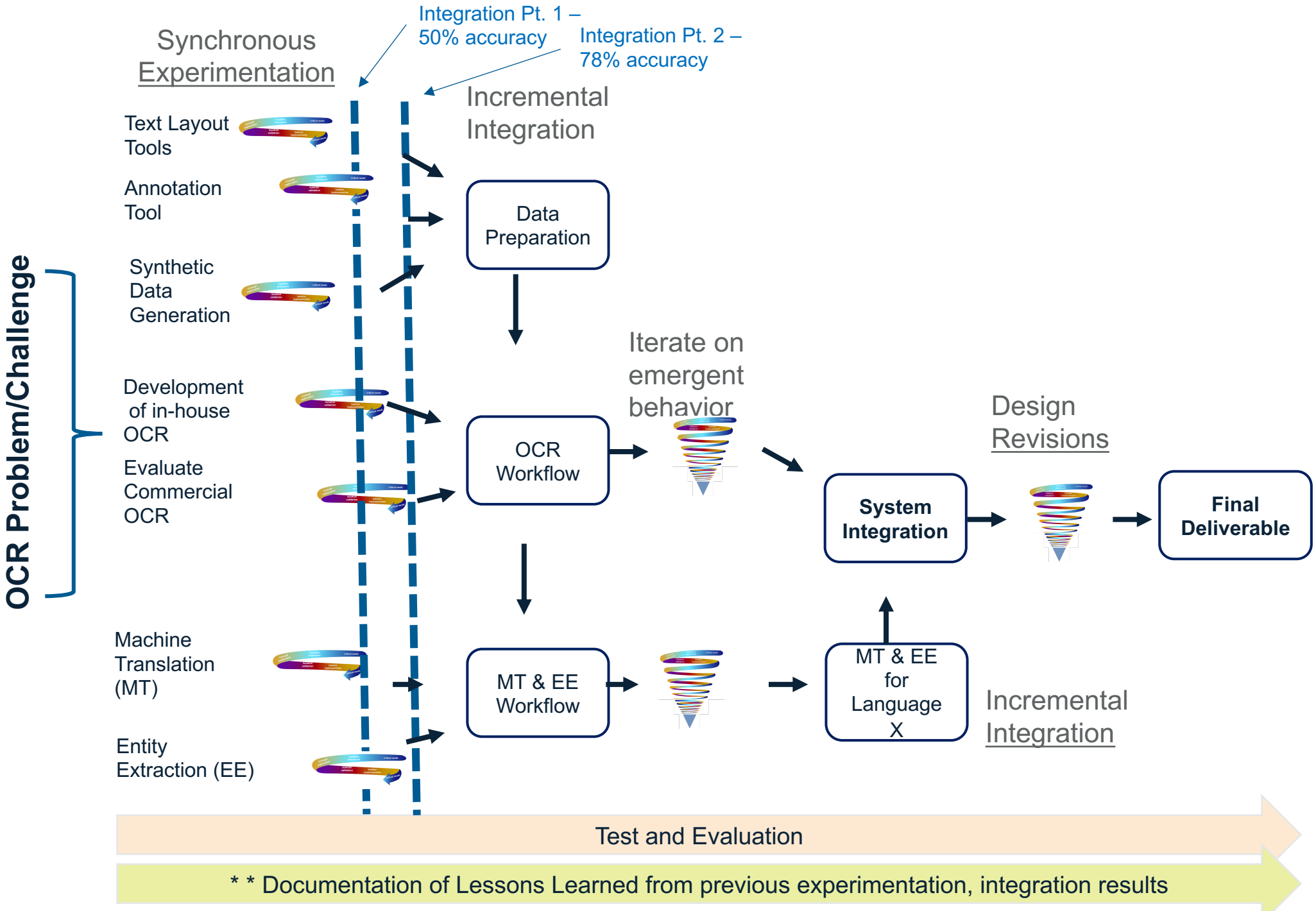
1540-7993/11/$26.00 © 2011 IEEE

Mix of Various Analytics To Do the Job

Computer Vision Analytics Workflow

What Does This Document Image Say?

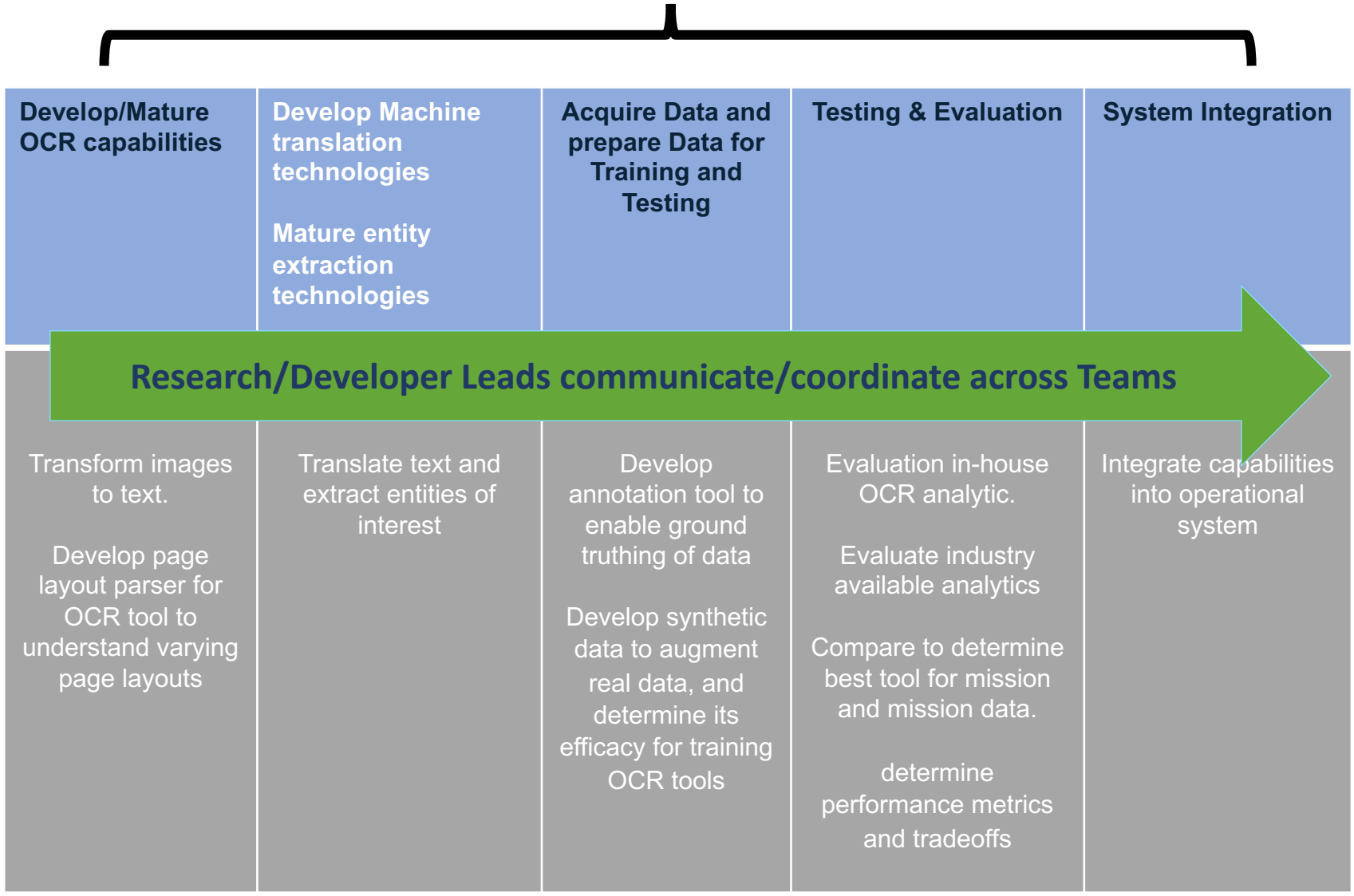
Human Language Technology Analytics Workflow


Integration Pt. 1 – 50% accuracy
Integration Pt. 2 – 78% accuracy
Synchronous Experimentation
Incremental Integration
Text Layout Tools
Annotation Tool
Synthetic Data Generation
Development of in-house OCR
Evaluate Commercial OCR
Machine Translation (MT)
Entity Extraction (EE)
OCR Problem/Challenge
Data Preparation
OCR Workflow
MT & EE Workflow
Iterate on emergent behavior
System Integration
Design Revisions
Final Deliverable
MT & EE for Language X
Incremental Integration
Test and Evaluation
* * Documentation of Lessons Learned from previous experimentation, integration results

Taking a Transdisciplinary Approach to Stakeholder Engagement

New **Roles and** ***New*** **Skillsets**

- Subject Matter Expert,
- Data Engineer,
- Developer,
- Machine Learning Engineer,
- Mathematicians,
- Data Scientist



Rosa R. Heckle

rheckle@mitre.org

linkedin.com/in/rosaheckle

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD™