school of SYSTEMS and LOGISTICS
▶ education ▶ service ▶ research

Software Acquisition in the Age of Cyber Warfare

Maj Mark Reith, Ph.D.

Software Professional Development Program

Air Force Institute of Technology

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense or the United States Government.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
MAY 2011

2. REPORT TYPE

3. DATES COVERED
00-00-2011 to 00-00-2011

4. TITLE AND SUBTITLE
Software Acquisition in the Age of Cyber Warfare

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Institute of Technology,Software Professional Development Program,Wright Patterson AFB,OH,45433

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 23rd Systems and Software Technology Conference (SSTC), 16-19 May 2011, Salt Lake City, UT.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT
unclassified

b. ABSTRACT
unclassified

c. THIS PAGE
unclassified

17. LIMITATION OF ABSTRACT
Same as Report (SAR)

18. NUMBER OF PAGES
40

19a. NAME OF RESPONSIBLE PERSON

Overview

- AF Cyber Professional Roadmap
- Proposed framework establishing baseline education for cyber developers
- Identify systems and software characteristics necessary for employment in the cyber domain
- Identify future system and software challenges within the context of the cyber domain

AF Cyber Professional Roadmap

- Describes AF way ahead in developing cyberspace professionals
- Describes core and enabling cyber competencies
- Describes development of officer and enlisted AFSCs; outlines Reserve & civilian
- Describes training and education

The Air Force Roadmap for the Development of Cyberspace Professionals, 13 Aug 2010

Force Development Roles

- Cyber Operators
- Cyber Specialists
- Cyber Analysts
- Cyber Developers

Not limited to the 17D career field!

Cyber Developers

- “Design, develop and document solutions that can be tactically employed by cyberspace forces to meet combatant commander requirements.”
- “They have in-depth expertise with the software or hardware technologies to which they are assigned, appropriate computer programming experience and expertise, and sound problem solving skills.”

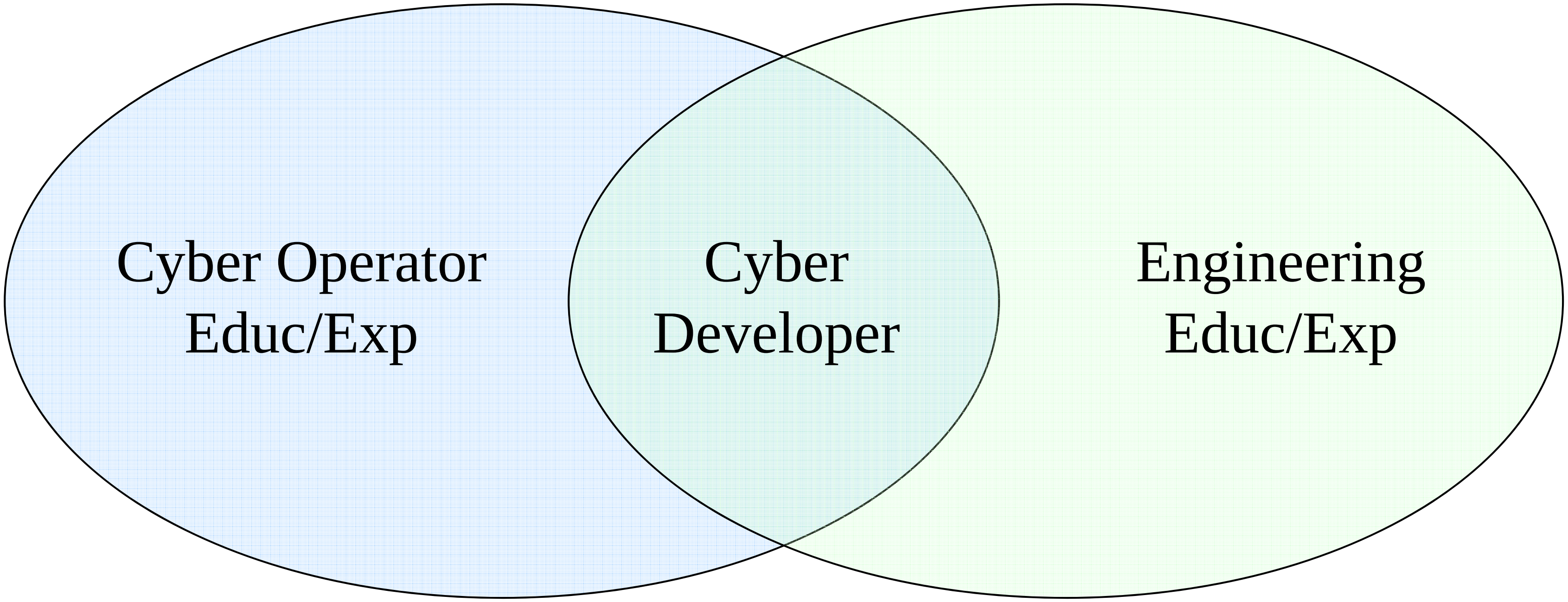
The Air Force Roadmap for the Development of Cyberspace Professionals, 13 Aug 2010

Cyber Developers

- “They apply current technologies, sound engineering techniques, and proven TTPs in their work.”
- “Developers for long-term projects should have experience in cyberspace operations and/or as cyberspace operators.”

The Air Force Roadmap for the Development of Cyberspace Professionals, 13 Aug 2010

Cyber Developers



Cyber Operator Educ/Exp

Cyber Developer

Engineering Educ/Exp

Cyber Developers

- **Skill Set:**
  - Design, engineer & problem-solving
  - Computer programming & development
  - Documentation
- **Experience:**
  - Cyberspace operations
  - Cyber TTPs
  - Engineering techniques
  - Current technologies

Two Questions:

1. Is this necessary and complete?
2. How do we get there?

Once upon a time…

- …in a combatant command far, far away…
  - Need for an enterprise network management tool
  - Suite of COTS tools integrated to provide a common operating picture of the network
  - Project managed by J6 Communications Directorate (NetOps, Engineering)
  - Versions 1 and 2 delivered with serious shortfalls
  - Version 3 in danger of repeating past mistakes

Plenty of mistakes…

- CONOPS focused on a specific solution rather than a needed set of capabilities
- No competition for contract
- Failure to include all stakeholders
- No requirements document
- No acceptance test plans
- Little documentation on implementation/integration
- No data rights
- Over budget, behind schedule
- No authorization to operate (ATO)

Analysis

- Clearly network management falls within cyber operations
- The command was developing tools to assist in the management of the cyber domain, so a cyber developer would be appropriate
- Given this case study, would the cyber developer, given the previous description, fare any better?

Analysis

- **Skill Set:**
  - Design, engineer & problem-solving
  - Computer programming & development
  - Documentation
- **Experience:**
  - Cyberspace operations
  - Cyber TTPs
  - Engineering techniques
  - Current technologies

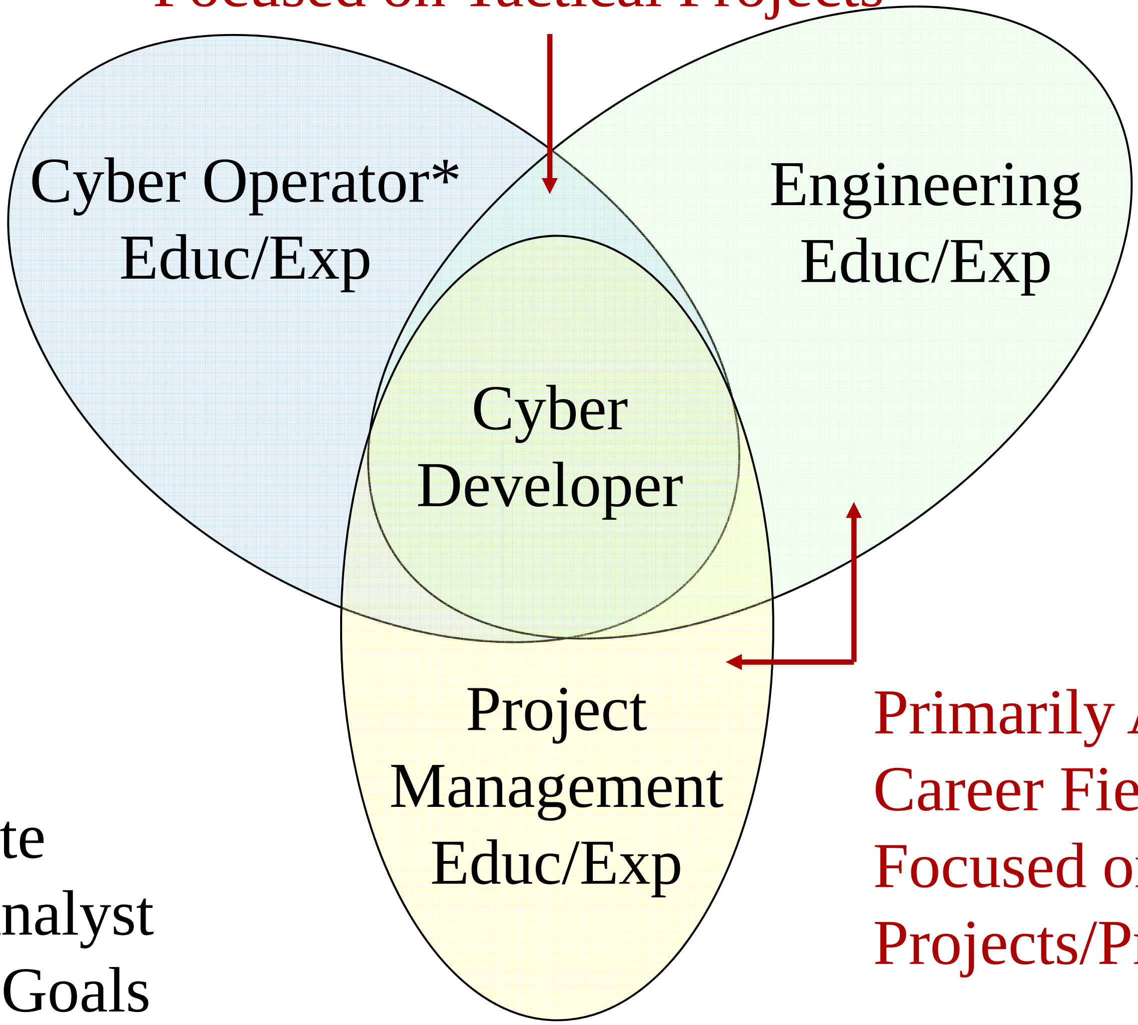
1. Is this necessary and complete?

Cyber Developer Educational Framework

- Blended Approach
  - Project Management
  - Engineering
  - Cyber Concepts

Cyber Developer Educational Framework

Identified by Cyber Roadmap;
Focused on Tactical Projects



Cyber Operator* Educ/Exp

Engineering Educ/Exp

Cyber Developer

Project Management Educ/Exp

Primarily Acquisition Career Field Domains;
Focused on Large Projects/Programs

*May Substitute Specialist or Analyst Depending on Goals

Cyber Concepts

- Relation between operations and technology
  - How operations depend on technology, vice versa
  - How technology exploits impact operations
- DoD and AF Enterprise Systems
  - System Integration Interfaces
  - Multi-Layered Defense
- Cyber Exploit/Defense Tools & Techniques
- Cyber Law & Policy

Operator-Centric

Why Cyber Concepts?

- Need to understand the environment
  - Understand how the tool hooks into environment
  - Understand the constraints, limitations, law
- Need to understand the operator
  - Accurately capture requirements
  - How will the tool be used?
- Need to understand impact on operations
  - What capabilities does the tool provide?
  - Can we save money, manpower, time?

Engineering

- Requirements Elicitation & Analysis
- Architect & Design
- Implement / Manufacture
- Test & Evaluate
- Deploy / Install
- Documentation / Technical Writing

System/Software Development Lifecycle-Centric

Why Engineering?

- Demonstrated best practices on maximizing quality while minimizing cost
  - Quality is really important here because tool failures may cost lives, treasure and reputation
  - We’re entering an era of fiscal constraint
- Need to demonstrate success before putting it on the network… too many people impacted

Cyber Engineering

- Understanding taxonomy of exploits
  - Buffer overflows
  - Race conditions
  - Virus replication, polymorphism
  - Data hiding
  - Authentication on untrusted client
  - Unsecure communications
  - Spoofing
  - Social engineering

Project Management

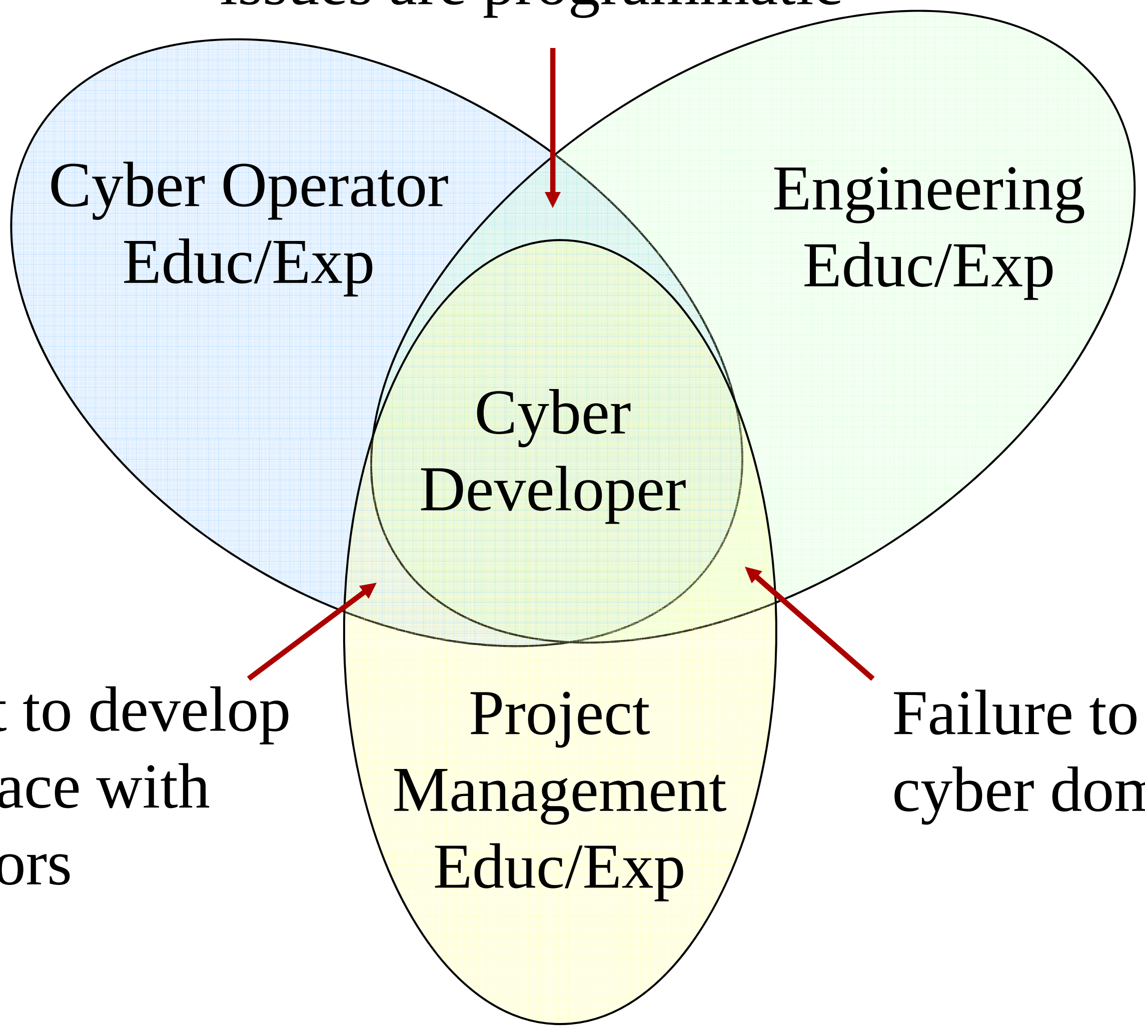
- Developing and tracking milestones
- Measuring projects against a set of metrics
- Tracking resources (funding, man-hours, etc)
- Monitoring & Controlling
- Documentation & Reporting
- Decision-Making Reviews

Acquisition Lifecycle-Centric

Why Project Management?

- Big or complex projects take time/resources
  - Need a means of deconstructing workload and tracking progress
  - Military cyber developers are by definition are transient; may not see to completion
- Need for not only technical metrics, but programmatic metrics
  - Metrics assist decision-making
  - How do we know that we’re successful?

Cyber Developer Educational Framework



Majority of “avoidable” issues are programmatic

Cyber Operator Educ/Exp

Engineering Educ/Exp

Cyber Developer

Project Management Educ/Exp

Difficult to develop or interface with contractors

Failure to understand cyber domain

Back to our story…

- CONOPS focused on a specific solution rather than a needed set of capabilities Cyber/PM issue
- No competition for contract PM issue
- Failure to include all stakeholders PM issue
- No requirements document Cyber/Engineering issue
- No acceptance test plans Engineering issue
- Little documentation Engineering issue
- No data rights PM issue
- Over budget, behind schedule PM issue
- No authorization to operate (ATO) PM issue

So how do we build them?

- **Or more appropriately, how get fully qualified cyber developers in the needed positions**
  - **Investment in people (Education & Experience)**
  - **Tracking and vectoring people**
  - **Retaining people**

- **If we're serious about supporting cyber operations, then we'll need cyber developers**

Education & Training Sources

- **Engineering**
  - **Undergraduate/Graduate Degree Programs**
  - **Industry Standard Professional Continuing Education (PCE) & Certification**
    - IEEE Certified Software Developer Professional
    - INCOSE Certified Systems Engineering Professional
  - **Department of Defense PCE**
    - Defense Acquisition University
    - Software Professional Development Program
  - **Vendor/Technology PCE & Certification**
    - Cisco Certified Network Associate/Professional
    - Microsoft Certified Systems Engineer

Most Desired Education Areas

Response	Personally	Score	Boss	Score	Coworker	Score
Team Management	205	0	401	2	159	0
Testing	261	1	126	0	315	2
Stakeholder Expectation	205	0	334	2	171	0
Architecture/Design	358	2	170	0	360	2
Requirements	401	3	331	2	419	3

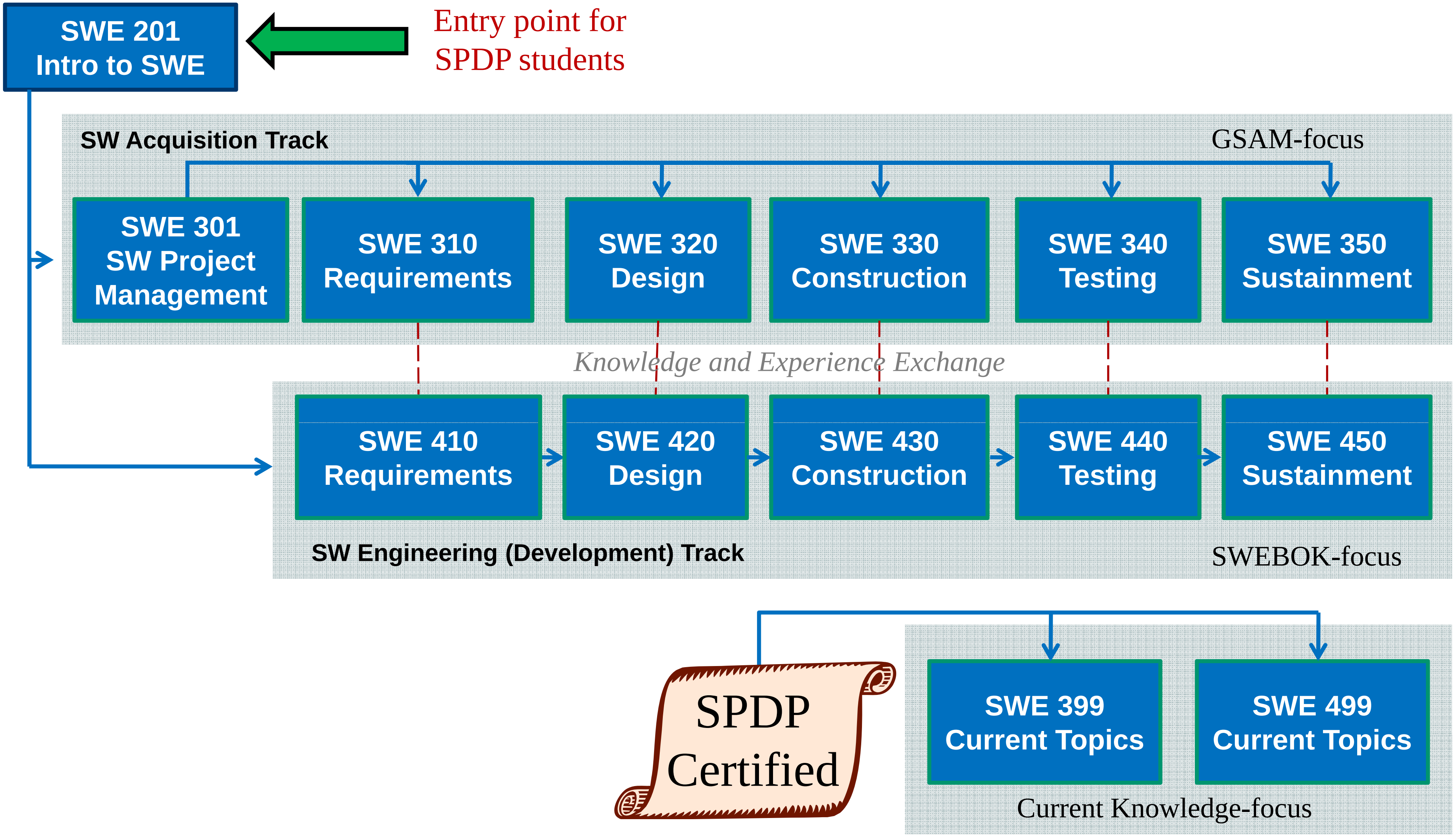
Score = # of standard deviations above mean

Respondents Were Asked to Choose Up to 5 Topics

Special Emphasis On…

- Requirements development
- Acceptance test development
- Technical writing and documentation
- Software maintenance
- Resources available for engineering software

SPDP



SWE 201
Intro to SWE

Entry point for
SPDP students

SW Acquisition Track

GSAM-focus

SWE 301
SW Project
Management

SWE 310
Requirements

SWE 320
Design

SWE 330
Construction

SWE 340
Testing

SWE 350
Sustainment

Knowledge and Experience Exchange

SWE 410
Requirements

SWE 420
Design

SWE 430
Construction

SWE 440
Testing

SWE 450
Sustainment

SW Engineering (Development) Track

SWEBOK-focus

SPDP
Certified

SWE 399
Current Topics

SWE 499
Current Topics

Current Knowledge-focus

SPDP (cont.)

- Partition management and engineering concerns across 2 tracks
- Manageable 3-week distance learning courses
  - 18-24 hrs per “track” course
  - 2-8 hrs for special topics
- AF Implementation of Industry Standards; Best Practices

Education & Training Sources

- **Project Management**
  - **Industry Standard PCE & Certification**
    - PMI Project Management Professional
  - **Department of Defense PCE**
    - Defense Acquisition University
    - AFIT School of Systems & Logistics

Organizational Attributes

Organizational Attribute (# Respondents)	Not Exhibited / Poorly	Satisfactorily / Exemplary
Establishing accurate performance, cost, and schedule baselines (821)	63%	37%
Educating stakeholders as to their role in software acquisition/development (811)	60%	40%
Capturing lessons learned (811)	56%	44%
Disseminate lessons learned to external organizations (810)	74%	26%

Special Emphasis On…

- CONOPS development
- How to schedule and allocate resources
- How to measure and analyze project progress metrics
- Working with stakeholders
- Resources available for managing software-intensive projects

External Certification

Certification	# Certified (All Career Fields)
Project Management Professional (PMP)	38
IEEE Certified Software Development Professional (CSDP)	6
IEEE Certified Software Development Associate (CSDA)	4
Engineering License w/ Software Engineering Specialization	10
ASQ Certified Software Quality Engineer	4
INCOSE Certified Systems Engineering Professional	5

At Best, Only 67 (7.8%) of Respondents Indicate Having External Certifications

Education & Training Sources

- Cyber Concepts
  - **Graduate Degree Programs**
  - **Industry Standard PCE & Certification**
    - Certified Information Systems Security Professional
    - Security+
  - **Department of Defense PCE**
    - AFIT Cyber 200/300 Courses
    - Cyber Warfare IDE Program

Special Emphasis On…

- Enterprise Integration (Active Directory, PKI)
- Security Integration (Firewall, IDS, Antivirus)
- Parallel Processing
- Networking and Bandwidth Sensitivity
- Service Oriented Architecture
- Digital Forensics
- Integrated COTS/GOTS

Consider these as system/software characteristics for operating in the cyber domain

So how do we build them?

- Or more appropriately, how get fully qualified cyber developers in the needed positions
  - Investment in people (Education & Experience)
  - Tracking and vectoring people
  - Retaining people

- If we're serious about supporting cyber operations, then we'll need cyber developers

Tracking & Vectoring

- Tracking
  - Acquisition Record
  - Cyber Record
  - Special Experience Identifiers (SEI) for Certs
- Vectoring
  - Code assignments providing or requiring development experience
  - Professional development and mentorship
  - Education with Industry program
  - Cyber assignments

So how do we build them?

- Or more appropriately, how get fully qualified cyber developers in the needed positions
  - Investment in people (Education & Experience)
  - Tracking and vectoring people
  - Retaining people

- If we’re serious about supporting cyber operations, then we’ll need cyber developers

Retaining People

- Some years a significant challenge!
- Build a solid community of cyber developers
  - Promote “Source Forge” type of portal and invite cyber developers to participate in projects
  - Introduce online TTP sites to promote development education for cyber developers and contractors
- Alternate assignments between cyber operations and development

Summary

- Cyber Developer Education Framework
- System/Software Characteristics for Cyber Domain
- Future Challenges

For more information:
mark.reith@afit.edu
SPDP@afit.edu

U.S. AIR FORCE