"If It Passes Test, It Must Be OK"

Common Misconceptions
And
The Immutable Laws of Software Development

ASQ Software SIG

January 27, 2015

Software Engineering's Persistent Problems - 1

Exponential rise in cybersecurity vulnerabilities due to **defective software**

Unacceptable cost, schedule, and quality performance of legacy systems **modernization** and Enterprise Resource Planning (**ERP**) projects

Software Engineering's Persistent Problems - 2

Cost of finding and fixing software bugs (i.e. **scrap and rework**) the number one cost driver in software projects

Arbitrary and **unrealistic schedules** leading to a culture of "**deliver now, fix later**"

Software Engineering's Persistent Problems - 3

Inability to scale software engineering methods even for medium size systems

Lack of understanding of the impact of **variation in individual productivity**

Absence of work place democracy and **joy in work**

The Appetite for Assured Software

The organizational appetite for assured software is driven by the net losses realized from compromised software

The consumer has been living with nearly 60 years of poorly developed and incompetent software.

Hundreds of millions of dollars are spent annually on post software compromise and incident recovery, lost opportunities and productivity (ask me).

Insecure software represents a pervasive kinetic threat to critical infrastructure and our way of life…..make no mistake about it.

The prudent approach is to take a proactive one. That is, software assurance measures must be a top integration priority in the enterprise cyber security risk management schema.

Source: Shaping Your Approach – the Executive's role in software Assurance, SWAMP Webinar, Jerry L. Davis, Chief Information Officer, NASA

By the Numbers

Feel my pain. Lack of a good software assurance program is a painful experience

At one time – 127 applications were tested and;

- 81 (64%) contained high vulnerabilities that facilitated exposure of sensitive data or system take over;
- 45 applications (36%) exposed Personally Identifiable Information (PII)
- At another time – 50 applications were tested and;
- 41 applications (82%) hosted OWASP top 10 defects
- 5 applications (10%) taken offline due to high risk
- 19 (38%) contained high vulnerabilities that facilitated exposure of sensitive data or system take over
- 12 applications (24%) exposed PII

Source: Shaping Your Approach – the Executive's role in software Assurance, SWAMP Webinar, Jerry L. Davis, Chief Information Officer, NASA

Emerging Cyber Threats Call for a Change in the 'Deliver Now, Fix Later' Culture of Software Development

By Girish Seshagiri, CEO of Advanced Information Services Inc. (AIS)

The demand for new and innovative technology solutions has created a software industry laser focused on speed to market, costs and product functionality. While this may help companies achieve a first-to-market advantage, it has also led to an environment where developers are more focused on meeting unrealistic schedule commitments than producing high-quality software.

necessary to permanently reduce the number of vulnerabilities found in their products."

Commit to Quality, Reduce Risk

Well-publicized software failures in recent times have been spectacular. We want these failures to become the exception instead of the norm. We want to encourage a thriving industry that easily enables quality work

"Well-publicized software failures in recent times have been spectacular. We want these failures to become the exception instead of the norm. We want to encourage a thriving industry that easily enables quality work to happen."

Growth Industries - 1

Information Assurance

Certification & Accreditation

PMP, ITIL, CMMI, Agile Scrum

Testing, Test Automation

Code Analyzers

The Application Security Industry

Is Now Bigger Than

The Applications Development Industry

Common Misconceptions -1

We must start with firm requirements

If it passes test, it must be OK

Software quality can't be measured

The problems are technical

We need better people

Software management is different

Source: *Managing the Software Process,* Watts Humphrey, Addison Wesley, 1989

Common Misconceptions – 2

Maturity level 3 is all that is needed

Higher maturity levels add to cost

Higher maturity levels are needed only for safety critical or business mission critical systems

If it is “agile” or “lean”, it is good

What we need are lean processes

Maturity levels guarantee results

Maturity level 5 is the end

The Real Question

Whose Process Is It?

Why? - 1

Why do development teams agree to **delivery schedule they know they can't meet?**

Why don't C-level executives realize that poor **quality performance is the root cause** of most software cost and schedule problems?

Why doesn't the government **hold contractors liable** for software defects and vulnerabilities?

Why? - 2

Why does the software applications development industry believe that **quality increases costs and schedule?**

Why do we continue to rely on **test as the principal defect removal** method?

Why do we continue to rely on monthly status reporting when we know that projects get to be **one year late one day at a time?**

Is Healthcare.Gov the Exception?

SAM.Gov?

USAJobs.Gov?

TSP.Gov?

Can you guarantee the cost, schedule, and quality outcomes of your current projects?

Have You Considered?

Quality work is more predictable

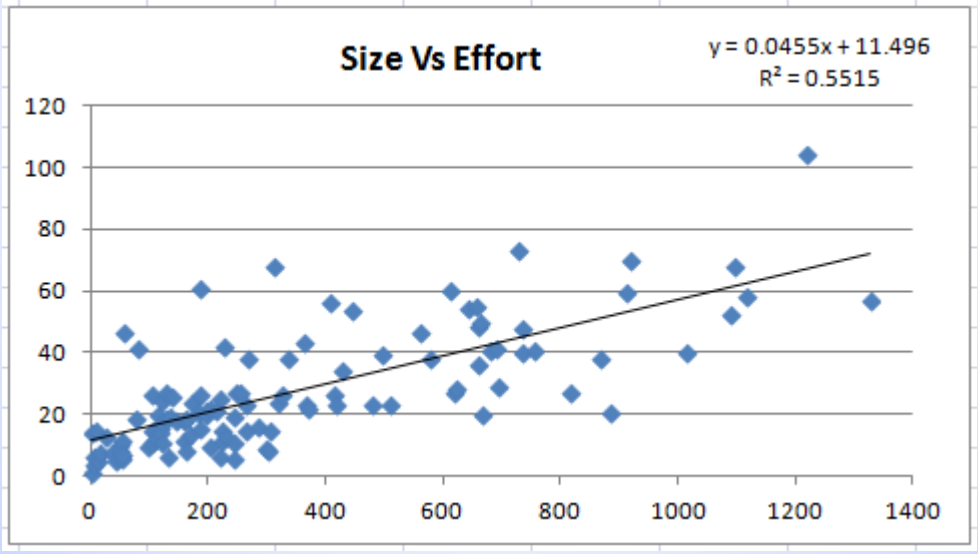
Unhappy people rarely do quality work

Without quality, agility is in name only

Quality without numbers is just talk

Immutable Laws of Software Development – 1

- The number of development hours will be directly proportional to the size of the software product



Immutable Laws of Software Development – 2

- When acquirers and vendors both "guess" as to how long a project should take, the acquirers' "guess" will always win
  - Customers' Dilemma
    - Want their product now at zero cost.
    - Due to time-to-market pressures, time frames are arbitrary and unrealistic for the software team to produce a product that works.
  - Developers' Choices
    - Try to "guess" what it would take to win the business.
    - Or make a commitment based on a plan and what the organization can do based on organization historic data.

Immutable Laws of Software Development – 3

- When management compresses schedule arbitrarily, the project will end up taking longer

Schedule/Quality Trade-off				
	Default	10% Compression	20% Compression	10% Extension
Duration Mths	25.9	23.3	20.7	28.5
Defect Count	1,033	1,316	1,715	849
% Change		27.4%	66.0%	-17.8%

Immutable Laws of Software Development – 4

- When poor quality impacts schedule, schedule problems will end up as quality disasters

Maryland officials were warned for a year of problems with online health-insurance site

"We didn't know it would be broken when we turned it on"

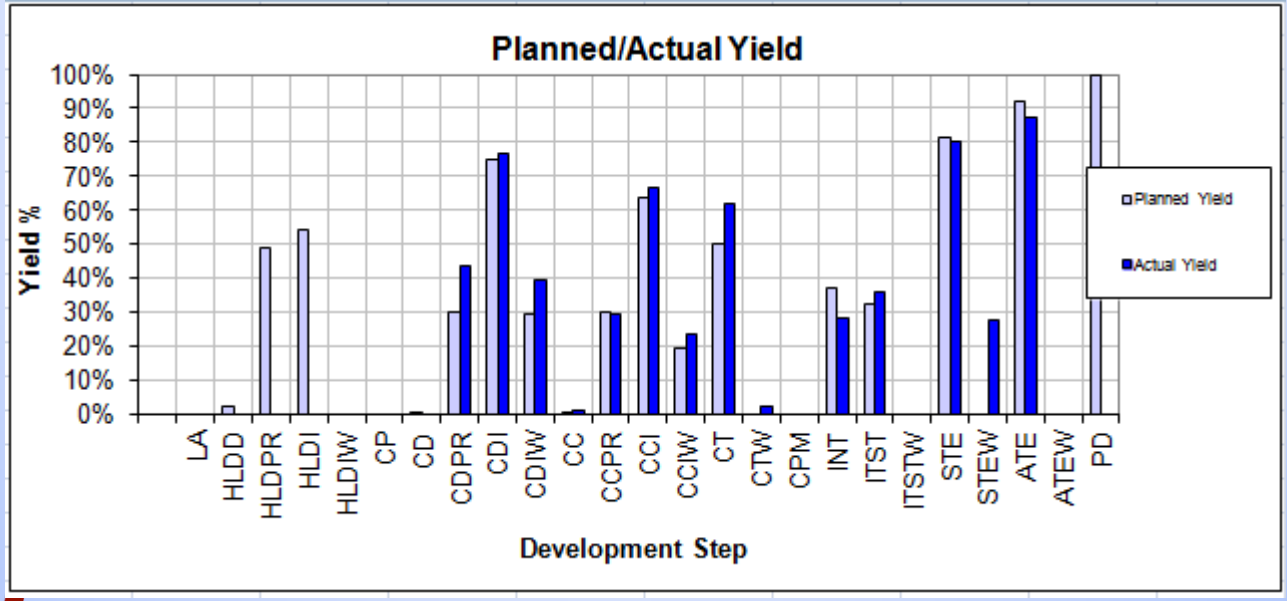
Immutable Laws of Software Development – 5

- The less you know about a project during development, the more you will be forced to know later

Data for week of	15-Aug-11	47	of 55		PROJECTED END DATE	Week Of	Week(s)	
					Avg EV Eff/Wk	19-Sep-11	5	
	Baseline Plan	Actual	Actual/Plan		Rem EV Effort & Avg EV Eff/Wk	12-Sep-11	4	
Project Hours	696.1	577.8	0.83		**Top 8 Avg EV Eff/Wk**	**12-Sep-11**	**4**	
Project Hours To-Date	26,311.3	26,712.9	1.02		Rem EV Effort and Estimating Accuracy	10-Oct-11	8	
Earned Value	1.70%	1.80%	1.06					
EV To-Date	86.40%	86.20%	1.00		To Date Hours Per EV (excl Blocked EV Eff)	221.3		
EV Effort		**413**	71.5%		**FOR ONTIME COMPLETION**			
					Avg EV / Week	**1.7**		
Avg EV Eff/Wk	761.3	425.8	**0.56**		Avg EV Effort / Week	**265.0**		
To Date Max EV Eff/Wk		675.9			Total EV Effort Required	**2,119.9**		
Top 8 Average EV Eff/Wk		609.0						
To-Date Hours for EV Tasks Closed	19228.5	19077.0	**0.99**			Actual	%	
To-Date Hours for Rework Tasks Closed	2860.9	2738.8	**0.96**		EV Tasks	20,010.7	74.91%	
Cost of Quality [(A+FR+PREV)/TOTAL EFFORT]		9072.4	**34.0%**		Travel Hours[TRVHRS]	86.5	0.32%	
Blocked EV Effort		**933.7**			Technical Meetings[TECHMTG]	2,394.0	8.96%	
					PM Ongoing Phase 3[PMONGOING3]	4,058.2	15.19%	
Cu. EV Effort	19833	20,010.7	1.01		SCOE Phase 3[SCOE3]	163.5	0.61%	
Cu. Non EV Effort	6478.3	6,702.2	1.03		Other Ongoing Tasks	-	0.00%	
Cu. Total Effort	26311.3	26712.9	1.02		**TOTAL**	26,712.9		

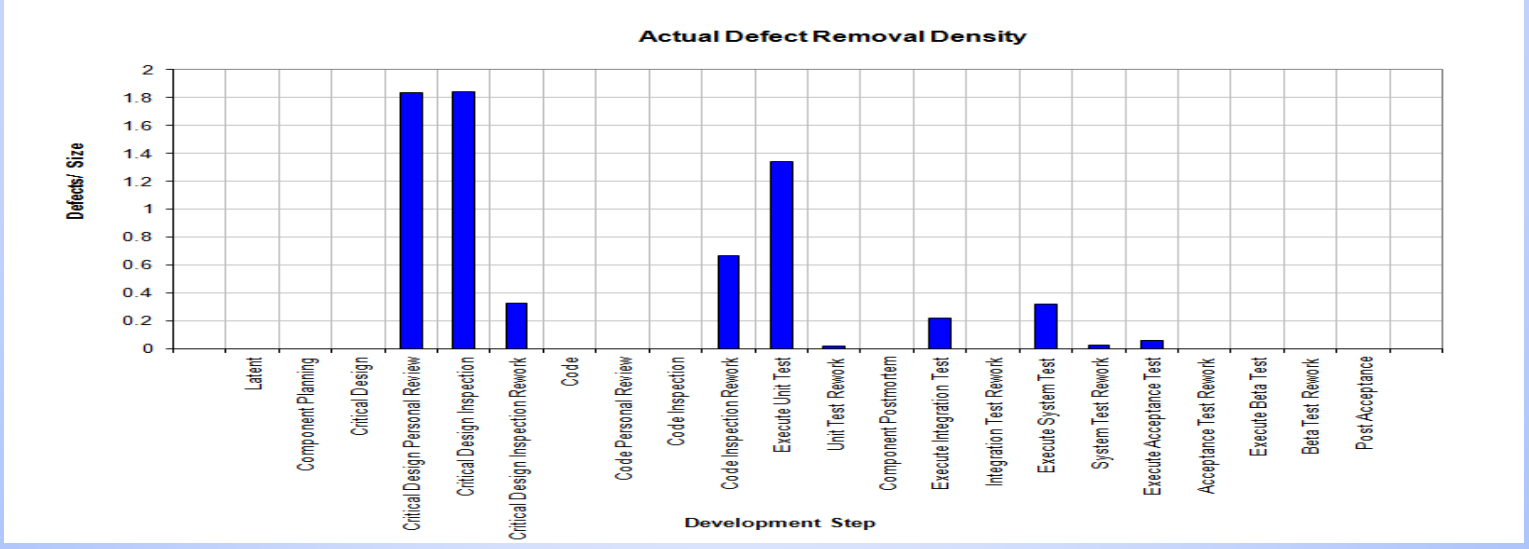
Immutable Laws of Software Development – 6

- When test is the principal defect removal method during development, corrective maintenance will account for the majority of the maintenance spend

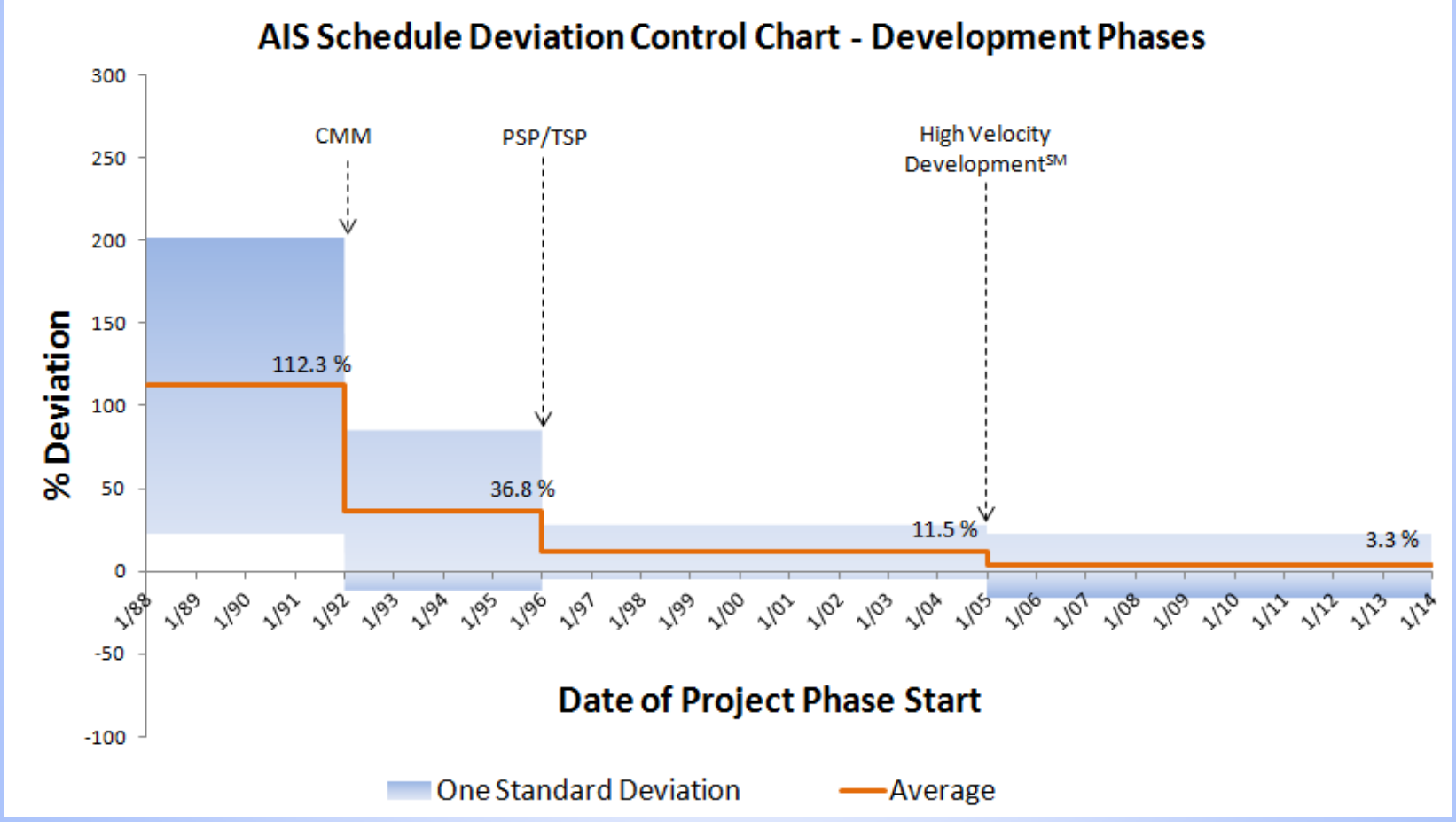


Immutable Laws of Software Development – 7

- The number of defects found in production use will be inversely proportional to the percent of defects removed prior to integration, system, and acceptance testing



Results
Organization History



Results
Recently Completed Project

- Component yield: 92.3%
  - Percent of defects introduced during development that were removed during development (before integration or system test)
- Cost of Quality: 34.9% [Industry average: >50%]
  - Effort in Appraisal, Failure and Prevention tasks
- Deliverable acceptance:
  - 1.3 Weeks per 100,000 SLOC/Day [Industry average: >16 Weeks]
  - 0.21 Defects/KLOC [Industry average: 4.73]
- Schedule deviation: 4 weeks ahead of schedule
  - 2.5% ahead [Industry average: 27% behind]

Results
New Team Member

43 Components

Size estimate error: 9%

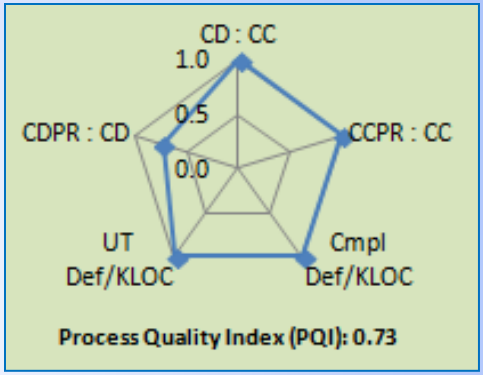
Effort estimate error: 13%

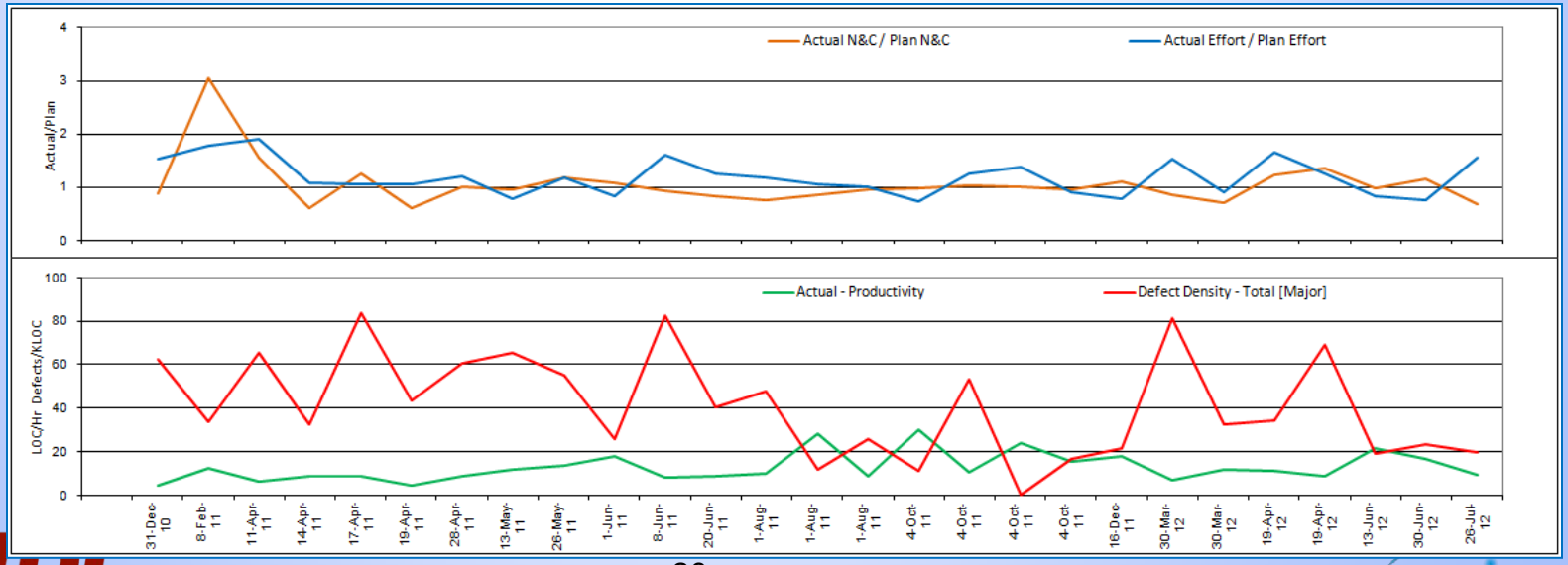
Process Quality Index (PQI): 0.73

- SEI data: PQI > 0.4 indicates high quality component

Component yield: 93.5%

- Percent of defects introduced during development that were removed during development (before integration or system test)





Regional Centers of Excellence for Secure Software

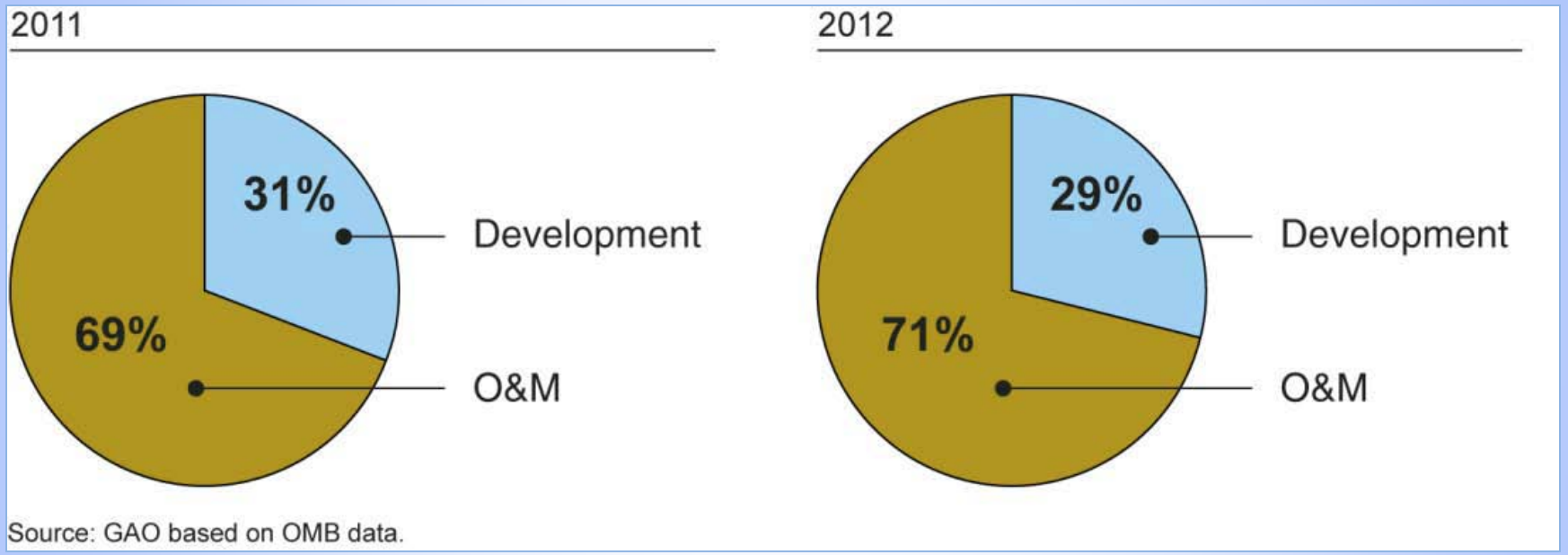
Central Illinois pilot

- An **industry-led** approach to training and skills formation for **secure software development**

Goals

- Using industry-defined competencies and requirements as well as a standardized curriculum to create highly-skilled, capable, and **readily employable** graduates.
- Creating a **registered apprenticeship program**, in which students receive competency based certification along with an associate degree and other accreditations.
- Connecting **education to a middle class job**, in which employers provide tuition reimbursement, school stipends, and an increasing hourly wage for the duration of the training and apprenticeship.

The $80 Billion IT Spend



Percentages of Total IT Spending for Fiscal Years 2011 and 2012 for 26 Key Federal Agencies

The $59.2 Billion Opportunity

Category	%	Spend	Waste	%	Annual Savings
Development	30.0	24.0	Scrap and Rework	60.0	14.4
O & M	70.0	56.0	Corrective Maintenance	80.0	44.8
Annual Spend	100.0	80.0			**59.2**

Joy in Work

"There is a square; there is an oblong. The players take the square and place it upon the oblong. They place it very accurately; they make a perfect dwelling place. Very little is left outside. The structure is now visible; what was inchoate is here stated; we are not so various or so mean; we have made oblongs and stood them upon squares. This is our triumph; this is our consolation."

The players in Virginia Woolf's *The Waves*

What does

“FUN ON THE JOB”

Mean to you?

Girish Seshagiri

girish.seshagiri@ishpi.net

703 426-2790