TSP Symposium 2014

Going Beyond Methodology to Maximize Performance

November 3–6, 2014
Pittsburgh, PA

Graphical Recordings

TSP 2014 Keynote: Case Study of Toyota Unintended Acceleration and Software Safety

Philip Koopman
Carnegie Mellon University

TSP SYMPOSIUM 2014

November 4, Pittsburgh PA

"Back pain. The tie that binds"

TSP helping to lay the foundations of the next generation of software

It's a myth that quality costs more. In creating software, quality COSTS LESS.

James Over, Opening Remarks

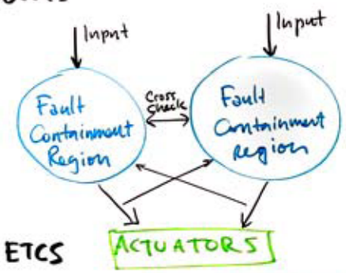
"What would Watts say?"

Keynote:

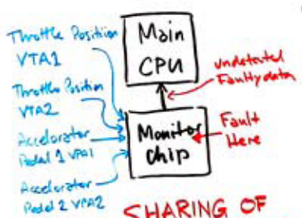
CASE STUDY OF TOYOTA UNINTENDED ACCELERATION AND SOFTWARE SAFETY

- Philip Koopman

Redundancy Required for Critical Systems

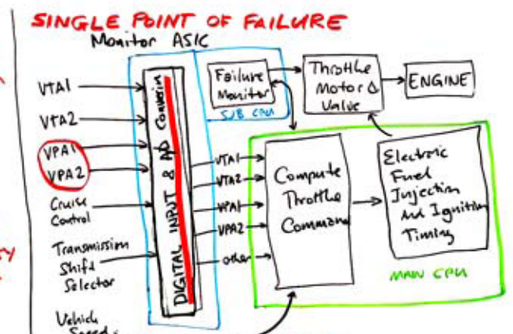


Toyota ETCS



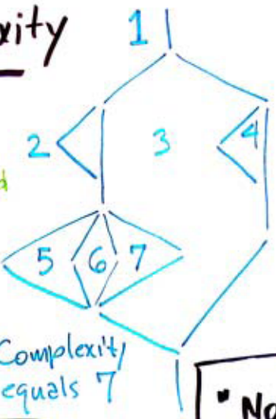
SHARING OF INPUTS PERMITS UNDETECTED FAULTY DATA TO REACH MAIN CPU.

SINGLE POINT OF FAILURE



Both copies of VPA go through the same input block on the same chip

Code Complexity



McCabe Cyclomatic Complexity Metric

Over 50 is considered "untestable"

ETCS Code Throttle Angle function complexity 146

Complexity equals 7

Global Variables are evil.

ETCS → ABOUT 10,000 global Variables

"No configuration management"

"No bug tracking system"

Concurrency Bugs Race Conditions

UPDATE FROM TASK2 GETS OVERWRITTEN BY TASK 1

ETCS Recursion

Recursion can keep putting copies of data onto stack, causing overflow

No mitigation for stack overflow

TSP 2014: The Rest of the Story: From Product Process to Process Analysis

Jeff Schwalb
NAVAIR

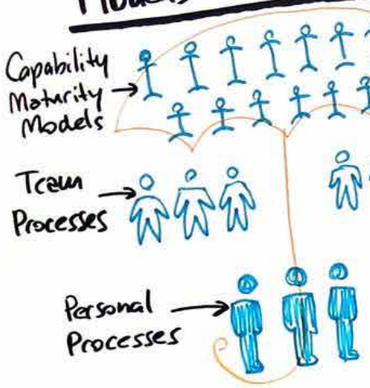
The Rest of the Story: From Product Process to Process Analysis

Jeff Schwalb, NAVAIR

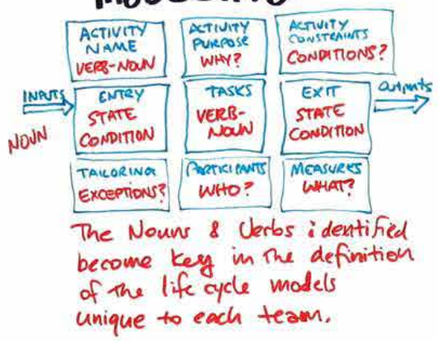
Learn a little, do a little.

- TPI is based on the application of good engineering in ALL technical areas, not just Software.
- Defining a team's process supports effective planning during launch.
- Effective post mortem analysis relies on well-defined workflows.

Models & Processes

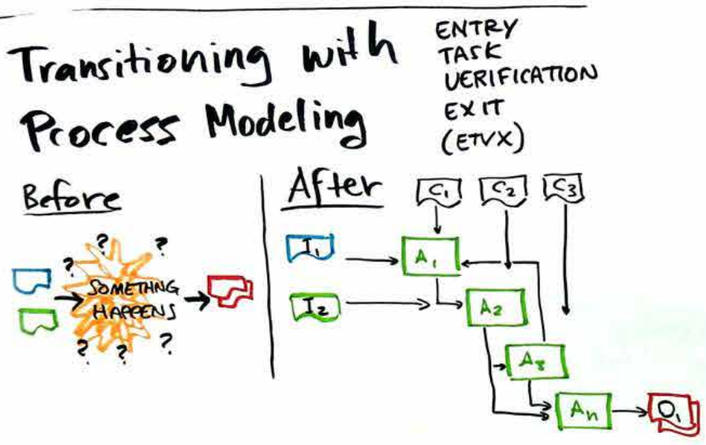


PROCESS MODELING



The Nouns & Verbs identified become keys in the definition of the life cycle models unique to each team.

Transitioning with Process Modeling

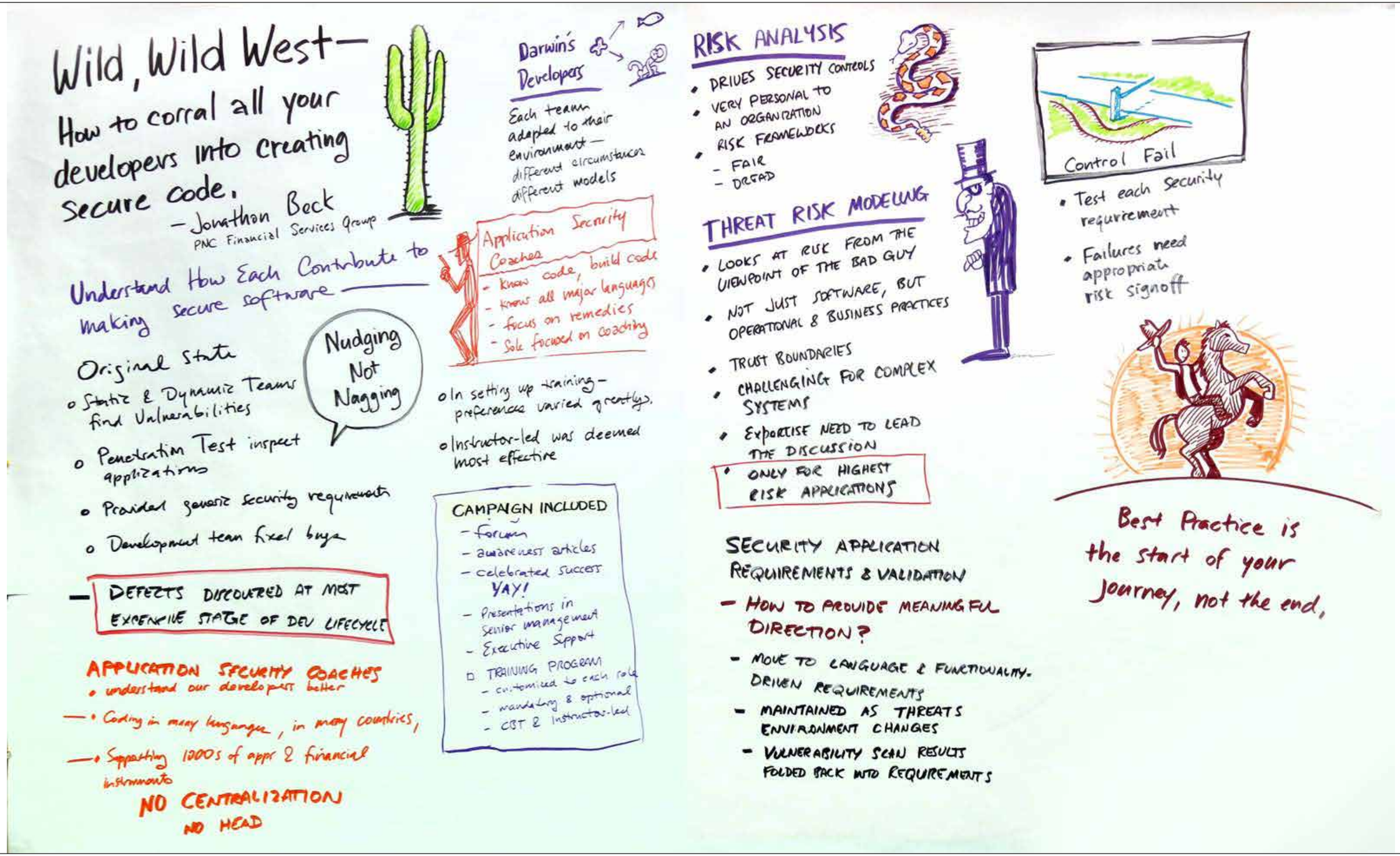


Post Mortem Analysis

- Considers artifacts applied during the project
- Looks at data collected throughout project
- Individual Experiences
- Data Mining through automated process tool

TSP 2014 Keynote: Wild, Wild West—How to Corral All Your Developers into Creating Secure Code

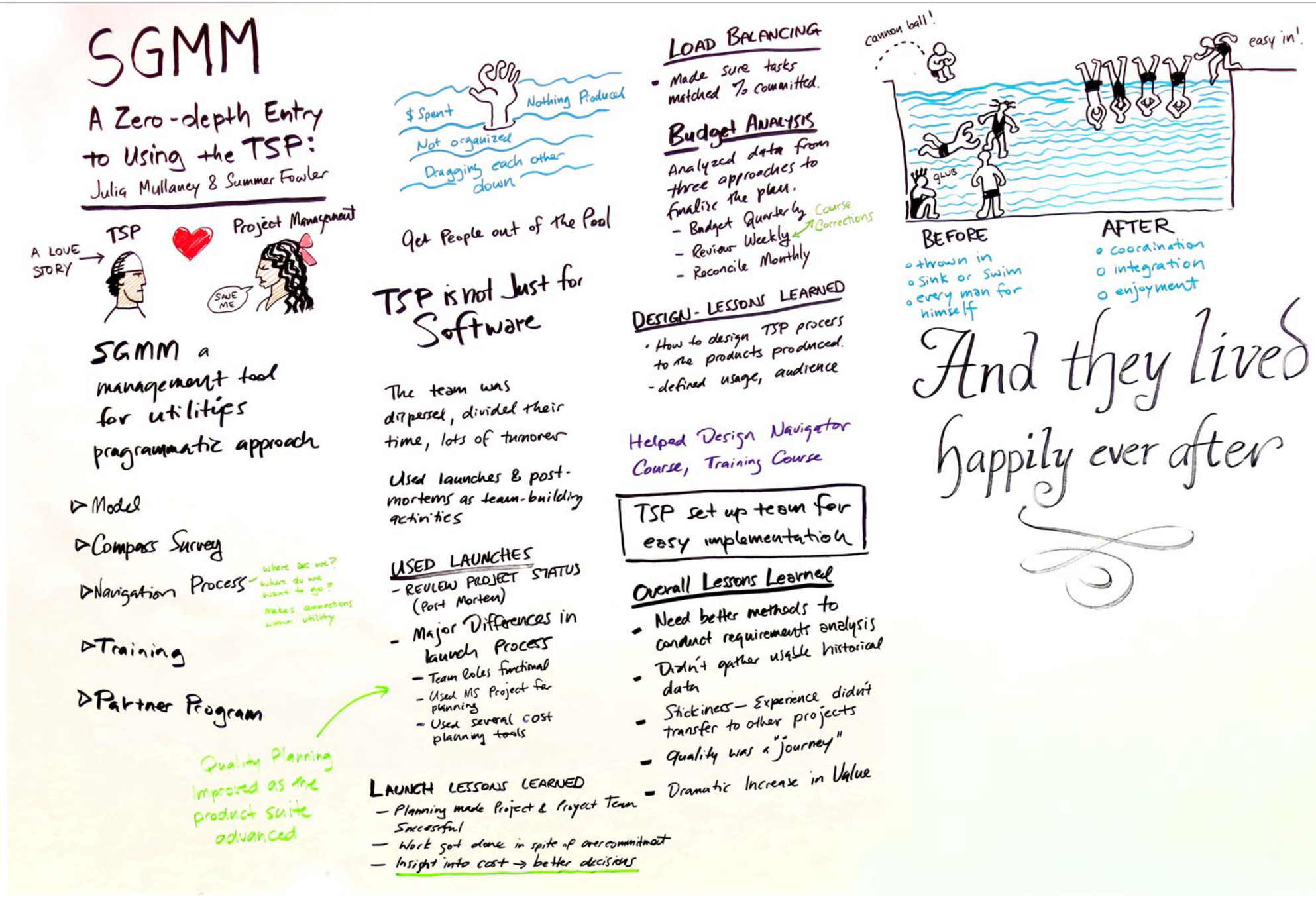
Jonathan Beck
Vice President and Director of Security Controls, PNC Financial Services Group



TSP 2014: A Zero-Depth Entry to Using TSP: How TSP Turned Around the Smart Grid Maturity Model Project

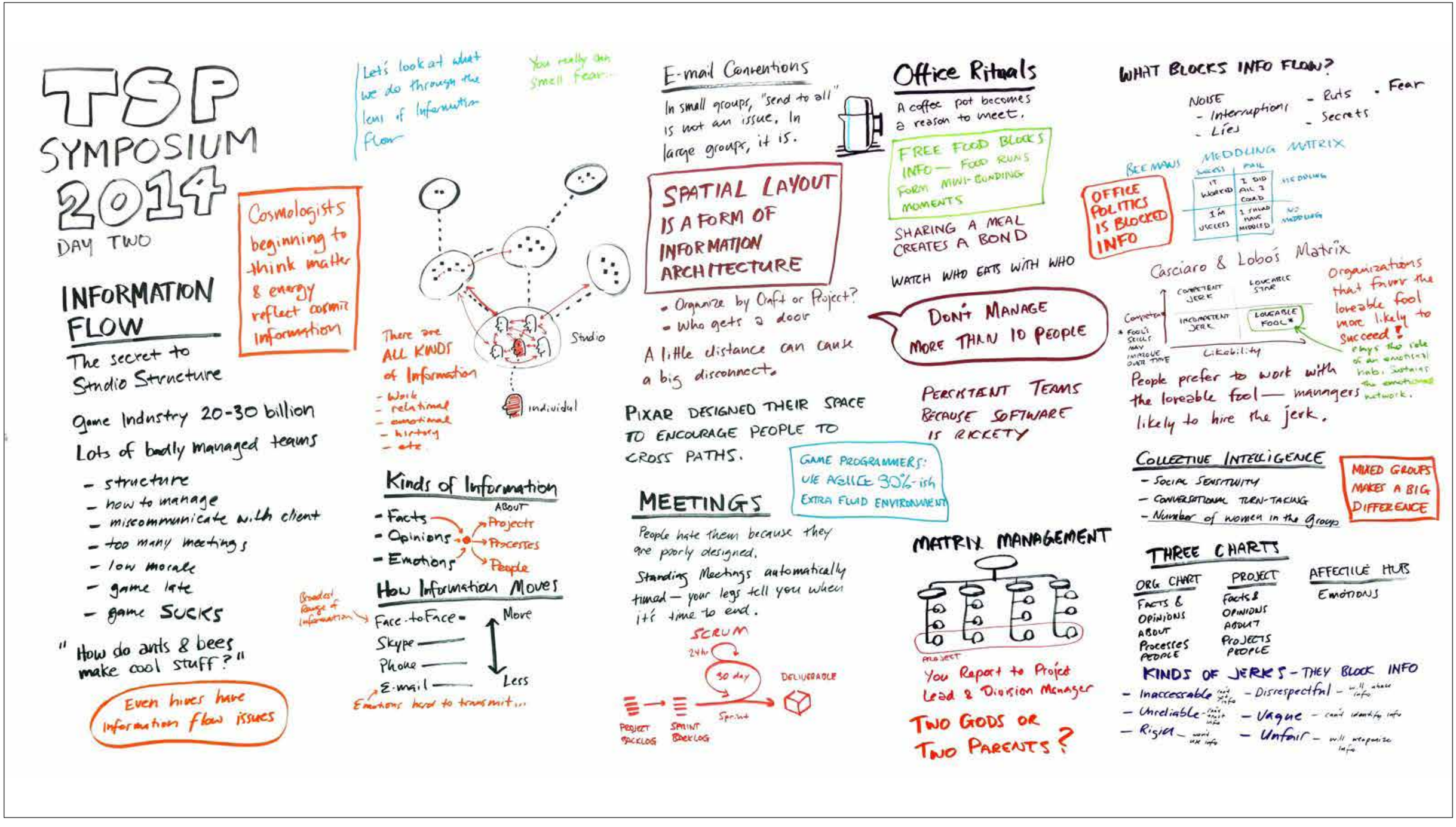
Summer Fowler, Carnegie Mellon Software Engineering Institute

Julia Mullaney, Carnegie Mellon Software Engineering Institute



TSP 2014 Keynote: Information Flow: The Secret to Successful Teamwork

Jesse Schell
CEO, Schell Games



TSP 2014: Insider Threats in the Software Development Life Cycle

Daniel Costa, Carnegie Mellon Software Engineering Institute

Randall Trzeciak, Carnegie Mellon Software Engineering Institute

TSP 2014: Under N: Acceptance to Delivery in N Hours

Umashankar Velusamy
Verizon Communications, Inc.

UNDER N:

Acceptance to Delivery in n hours

Umashankar Velusamy

= 9 Months to Delivery

= 2 Months to Delivery

Not All Deliveries Are Alike

Think of it as building an ER for software delivery

Under-N

Smart Delivery of pre-defined orchestrated software changes from acceptance to delivery in under "n" hours.

- Driven by business values
- Doesn't compromise quality
- Co-exists with other business delivery cycles
- Many teams already do it!

ER
- Create a framework
- Use templates
- Create Governance Process
- Enable a Medium to handle Requests
- Institute a support structure

Invoke the Framework for each Under-N Capability

FRAMEWORK:

Create a Template with key info associated with the Under-N capability, both the info needed & the info to be used.

- Ask the right questions to the IT teams

GOVERNANCE:

1. Capability Request
2. Define Capability
3. Team Assess & Approve
4. Define Template
5. Confirm Task Ownership
6. Ensure Process & standards
7. Launch

CAPABILITY INVOCATION:

1. Client invokes a defined Under-N capability
2. Validate Pre-requisites
3. Accept / Deny
4. POCs follow Template Steps
5. Confirm Delivery in N-hours
6. Measure Business Value

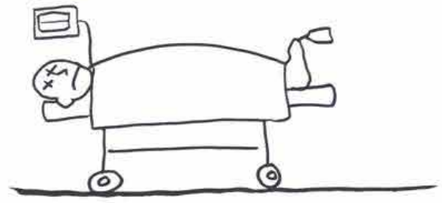
MEDIUM:

- Central Information Radiator Portal

SUPPORT STRUCTURE:

- Strong Executive Support
- Create Under-N fabric
- Celebrate Success
- Broadcast, Identify & Apply capabilities
- Challenge Teams to Self-Service

When does it fail?



- When used to bypass processes
- When cutting corners
- Wrong choice of tools or Architecture
- When trying to squeeze large Projects

TSP 2014 Keynote: When You Build It, They Will Come

Richard Pethia
Director of the CERT Program, Carnegie Mellon Software Engineering Institute

WHEN YOU BUILD IT, THEY WILL COME

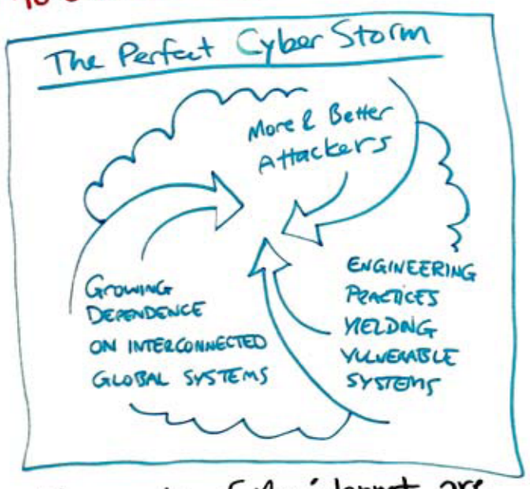
Rich Pethia

Our systems are under CONSTANT ATTACK

Credit Card Bad, Identity Theft harder on the individual

CYBER CRIME THE BIGGEST THREAT TO OUR DEFENSE, ECONOMY, & LIBERTY

The Perfect Cyber Storm



All aspects of the internet are growing dramatically—

1969: 4 hosts → Today: Over a billion

We are dependent on evolving cyber ecosystems...

... and that trend is going to continue

CYBER SECURITY IS ONLY GOING TO BECOME MORE CRITICAL

- SOFTWARE COMPLEXITY INCREASES VULNERABILITY TO ATTACKS
- Open source supply chain is vulnerable

75% of organizations rely on open source as the foundation of their applications

- Security skills haphazard among developers
- no provenance of code
- no process for updates
- transitive vulnerabilities

More than 81% development organizations do not coordinate their security practices accross the board

96% of attacks not difficult

97% of attacks were avoidable

A community of Adversaries

- Writers - Make & Sell Malware
- First Stage Abusers - Gather Information
- Middlemen - Collect & Process/sell blocks of info
- Second Stage Abusers - Do the real damage - ID Thieves, extortion

Organized Crime & Terrorist Networks Involved

The solution:

1. Better software engineering practices
2. Improved security & resilience practices
3. Larger skilled workforce

How to make secure software agilely and affordably?

Good software architecture leads to longevity & quality in a software-reliant systems

Design weaknesses drive vulnerabilities

76% of Most Dangerous Errors stem from Design Weaknesses

Malware samples are accumulating at more than a million a month

Static testing & Source code analysis improving—leading to better code

Government Systems moving away from check-the-box-checks and towards ongoing processes that increase/enhance security/resilience

There is a critical shortage of cyber security professionals.

The need is outpacing supply of trained people.

There's more to it than cryptography

TSP 2014: Scrum: Creating Great Products and Critical Systems – What to Worry About, What's Missing, and How to Fix it

Neil Potter
The Process Group