SERC Talks: "Secure Cyber Resilient Engineering for the Era of Competition"

June 15, 2022 | 1:00 PM ET

Ms. Melinda K. Reed, Director, Systems Security, Science and Technology Program Protection (STPP) Office in the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E))

CYBER RESILIENCE

- ❑ Today's session will be recorded.
- ❑ An archive of today's talk will be available at: www.sercuarc.org/serc-talks/ as well as on the SERC YouTube channel.
- ❑ Use the Q&A box to queue up questions, reserving the chat box for comments, and questions will be answered during the last 5-10 minutes of the session.
- ❑ If you are connected via the dial-in information only, please email questions or comments to SERCtalks@stevens.edu.
- ❑ Any issues? Use the chat feature for any technical difficulties or other comments, or email SERCtalks@stevens.edu.

SYSTEMS ENGINEERING RESEARCH CENTER

SERC TALKS

SERC Talks: "How Can We Model Cyber Attacks and Systems to Characterize Resilience of Critical Infrastructure Systems?"

Ms. Melinda K. Reed
Director, Systems Security, Science and Technology Program Protection (STPP) Office in the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E))

Dr. Peter Beling, SERC Research Council Member; Professor and Associate Director, Intelligent Systems Lab, Hume Center for National Security and Technology; Professor, Grado Department of Industrial and Systems Engineering at Virginia Tech

DISCLAIMER

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

Any views, opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense, OUSD (R&E), nor the SERC.

No Warranty. This SERC - Stevens Institute of Technology Material is furnished on an “as-is” basis. SERC and Stevens Institute of Technology makes no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose or merchantability, exclusivity, or results obtained from use of the material. SERC and Stevens Institute of Technology does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

This material has been approved for public release and unlimited distribution.

Secure Cyber Resilient Engineering In the Era of Competition

Engineering Cyber-Resilient Weapon System Workforce Development

Problem Statement:

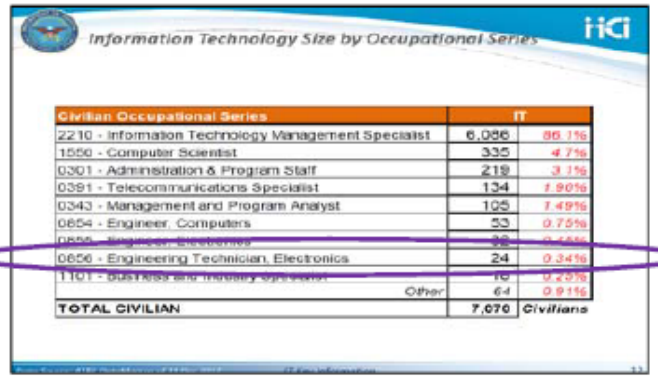
- *The evolving and complex nature of the challenges presented by critical systems operating in contested cyberspace environments requires unique skills beyond those addressed by information technology security education.*
- *DoD must develop the ability to engineer and assess the combined safety, security, and resilience in current and future systems in the presence of determined cyber adversaries.*

Workshop 6 (Jul 31– Aug 2 2018)
State of the Engineering Workforce; Cybersecurity Engineering

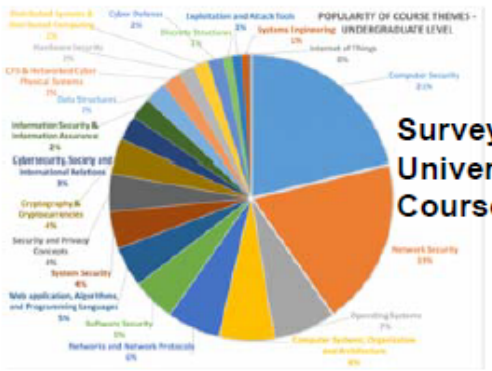
Goal: Identify skill sets and curriculum needs for our current and future engineering workforce

- **Understand engineering education gaps related to cybersecurity**
- **Develop Need's for today's engineering workforce**
- **Develop Need's for tomorrow's engineering workforce**

Sponsored by the SERC



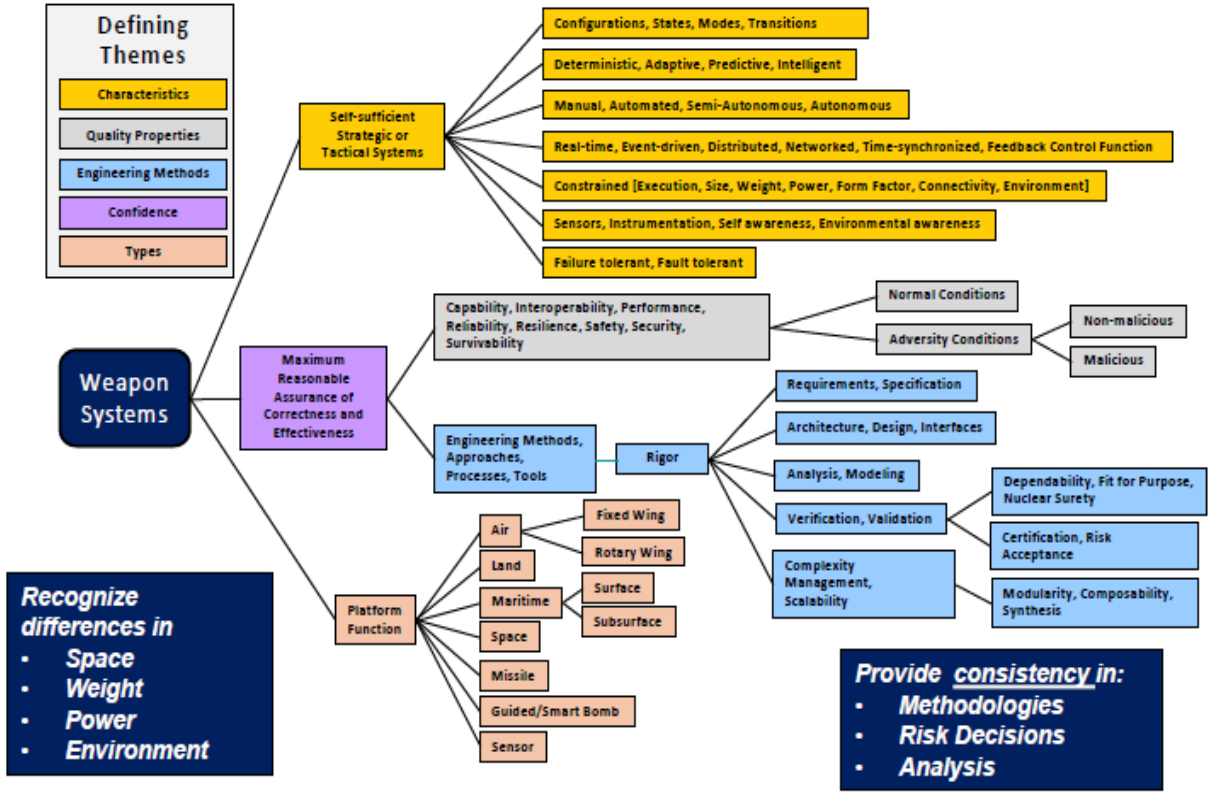
Civilian Occupational Series	IT	
2210 - Information Technology Management Specialist	6,086	86.1%
1550 - Computer Scientist	335	4.7%
0301 - Administration & Program Staff	219	3.1%
0391 - Telecommunications Specialist	134	1.90%
0343 - Management and Program Analyst	105	1.49%
0854 - Engineer, Computers	53	0.75%
0856 - Engineering Technician, Electronics	24	0.34%
Other	64	0.91%
TOTAL CIVILIAN	7,070	Civilians



Survey of 104 Universities by Course Themes

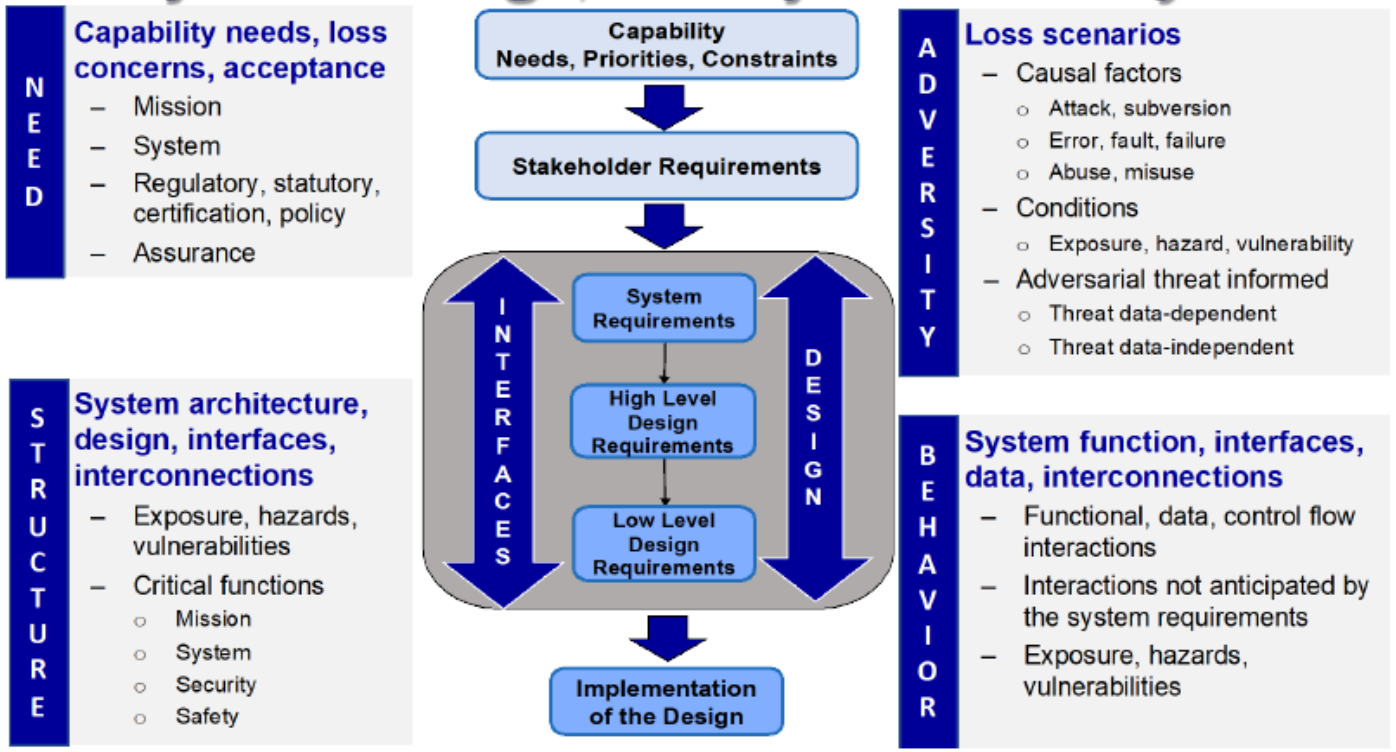
Secure Cyber Resilient Engineering Considerations

Weapon Systems Characteristics



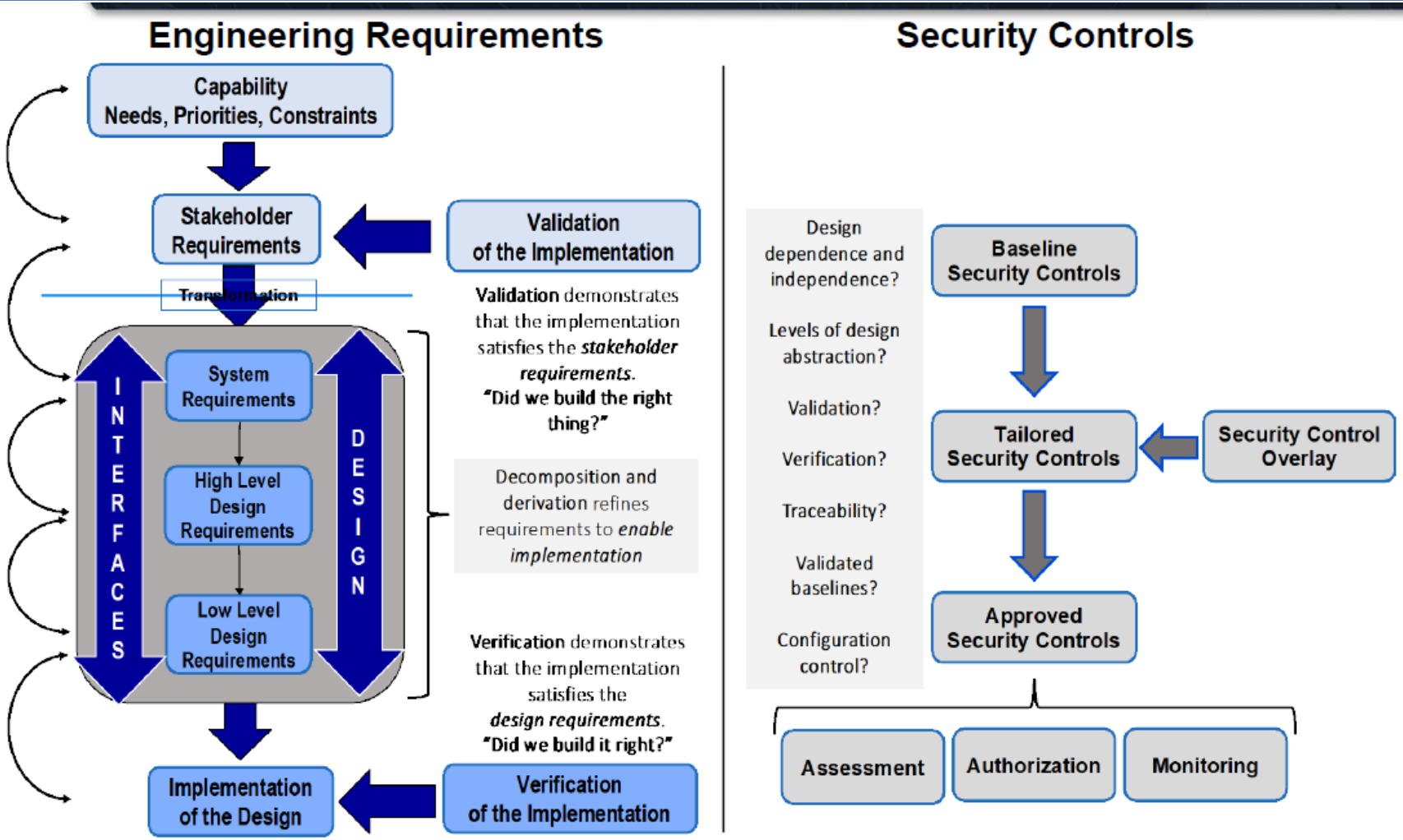
Secure Cyber Resilient Engineering Approach to Requirements Derivation

Requirements Derivation, System Design, and Systems Analysis



Applied with rigor necessary to achieve the targeted level of confidence

Secure Cyber Resilient Engineering
Security Considerations



Questions and Discussion

SERC TALKS

SYSTEMS ENGINEERING RESEARCH CENTER

THANK YOU FOR JOINING US!

Please check back on the SERC website for today's recording and future SERC Talks information.

www.sercuarc.org/contact-us/