Background
Our highly-networked world, where software pervades all aspects, is dominated by cyber-physical systems (CPS). The dividing line between electronic security, physical security and safety has blurred to the point of near-invisibility. Cyberattacks are a major threat to society; they can inflict physical damage to trillions of dollars in infrastructure and threaten the well-being (and lives) of millions. The correct and secure operation of software is required to protect this critical infrastructure. Recent reports to the National Academy of Sciences urge the adoption of software with “correctness certificates”. The Department of Defense (DoD) has developed a “System Assurance Strategy” that stresses security throughout a system’s lifecycle and requires DoD programs to account for vulnerabilities. The Food and Drug Administration has developed guidance for the security for medical systems and device software. The Institute of Electrical and Electronics Engineers released the report “Building Code for Medical Device Software Security” in response to mounting pressure to secure the medical infrastructure. K-State researchers have been key participants in many of these efforts, with a distinguished history of developing technologies for construction of safe and secure systems.

Description
The Center for Information & Systems Assurance (CISA) is a leader in cybersecurity research, teaching, and outreach. In 2010 CISA was designated as a National Center of Academic Excellence for Research in Cyber Security by the National Security Agency and Department of Homeland Security. For over 15 years CISA researchers have collaborated with partners such as Rockwell Collins, Boeing, HP, Microsoft, Honeywell, Galois, Adventium, and Idaho National Lab to design secure, mission-critical software systems. New collaborations in safety, security, and education research are being explored.

CISA also has contributed to securing the national infrastructure. DoD contractors integrate custom and off-the-shelf components from hundreds of suppliers to build complex distributed systems. Because current design, acquisition, and vulnerability assessment techniques are insufficient for this complexity, security flaws and cost overruns are common. CISA researchers have developed tools to design and assemble such software systems quickly and at low cost. CISA researchers have also developed tools that protect medical communication, reduce programming errors and simplify the integration of security into next-generation CPS. CISA members also have multiple prestigious awards, including five National Science Foundation (NSF) CAREER awards and over $1.25M in DoD funding to study the safety and security of dynamically composable CPS.

Additional funding will significantly enhance CISA capabilities to solve the challenges of next generation CPS. These challenges include faster, less costly design of “zero-failure” mission critical systems, tools to protect the nation’s critical infrastructure, and partnerships with corporate and local, state, and national agencies to educate the general population on ways to overcome cybersecurity challenges.

CISA is uniquely poised to tackle these issues. CISA will develop usable security solutions that seamlessly integrate with current verification and validation activities and produce secure systems by increasing uptake and reducing development costs. Enabling techniques include reasoning based on formal languages and type theory, code generation, and developer tools evaluated for usability. A shortage of cybersecurity engineers has been regularly cited as a potential threat to national security. CISA will continue to develop tools for security education in Manhattan, K-State Polytechnic, and Olathe and determine how to most effectively present security education material.

Relevance
CISA has a reputation of building secure software protocols and systems. Given existing collaborations with cybersecurity industry leaders and the anticipated arrival of the National Bio and Agro-defense Facility (NBAF), CISA will promote collaborations with cybersecurity and biosecurity companies and help establish a regional center to train the future cybersecurity workforce. CISA has also established CANSec, a semiannual workshop to present ongoing research and promote collaboration.

Agency Contact Information
National Science Foundation
Dr. Victor Piotrowski, 703-292-8670, vpiotrow@nsf.gov

National Science Foundation
Anita Nikolich, 703-292-4551, anikolic@nsf.gov

U.S. Army MRMC, TATRC HTIC
Betty Levine, 301-619-3199, betty.a.levine.civ@mail.mil

AFOSR
Dr. Kathleen Kaplan, MIT Fellow, 703-696-7312, kathleen.kaplan@us.af.mil
Summary: The safety of today’s critical infrastructures (e.g., transportation, communications, energy, etc.) depends on cybersecurity. Researchers at Kansas State University are working with industry and government to protect these infrastructures by developing new protocols and tools.

Opportunity: Cyber-physical systems (CPSs) pair computer control with physical machines, which requires electronic and physical security, and safety considerations. Because cyberattacks can inflict physical damage, safe and secure software is required to protect critical infrastructures, as noted recently by the National Academy of Sciences, Department of Defense, and the Food and Drug Administration.

Solution: Researchers at Kansas State University are developing secure, mission-critical software systems using improved vulnerability assessment techniques, protocols to protect medical communication, and software verification and validation tools to reduce programming errors and simplify integration of security into next-generation CPSs.

Impact: The Center for Information and Systems Assurance (CISA) is a designated National Center of Academic Excellence for Research in Cyber Security by the National Security Agency and Department of Homeland Defense. Center researchers collaborate extensively with cybersecurity industry leaders and foresee increased collaboration opportunities in critical infrastructure protection research with the anticipated arrival of the National Bio and Agro-defense Facility (NBAF) to Manhattan, Kansas. CISA will promote collaborations with cybersecurity and biosecurity companies and train the future cybersecurity workforce.

Equipment & Expertise: automatic code generation, automated analysis and verification, medical device interoperability, protocol design, model-based development, model checking, product-line engineering, risk management and hazard analysis, safety and security co-design, secure distributed system design, software and hardware co-design, system architecture modeling using modeling languages, verification and validation, usability design, user testing.